CORPORATE CUSTOMER

PRIVACY POLICY

This privacy policy applies when Telia Sverige AB (Telia) supplies products and services to a corporate customer (the customer) and where Telia is the personal data controller.

The policy describes Telia's processing of data and the rights that a data subject, that is, an employee or a contractor of the customer (the user), may exercise over data concerning the data subject.

The data subject to the privacy policy is a part of the information we process in order to supply products and services to customers.

The privacy policy also applies for Telia websites for customers in Sweden, but does not apply to websites or services from other companies, even if it is possible to access them from Telia’s network or services.

Telia's processing of personal data on behalf of the customer is not subject to this privacy policy.

telia.se/foretagintegritet

Data and how we process data

What type of data we collect

We process two types of personal data – user data and traffic data.

User data is information about a user, e.g.their telephone number, email, user ID, password and other information we process to supply products and services to the customer.

Traffic data is data which is generated when certain of our products or services are used. Traffic data is processed for the purpose of transmitting an electronic message via an electronic communications network, e.g. when a telephone call is made or an email is sent. The data is also used for billing such messages or for interconnection traffic. Examples of this are who has communicated with whom, the times when the communication began and ended, the total time it lasted and the network used. Traffic data is also information on where a person is geographivcally when that person is making a call or is connected to a network.

How we collect data

Depending on which product or service we are providing, we collect and process data that:

- the customer provides when the customer enters into a contract with Telia and communicates with us – e.g. by contacting us for information or subscribing to newsletters.
- is created when the user uses certain of our services – e.g. by making a call or sending a text message or email.
- is collected from other sources – e.g. company information from the companies' register as well as from other operators and service providers.
- is generated through our web-sites' use of cookies that collect information on and from the users' browsers.

What we use data for

The processing of data must be permitted under law, so-called legal basis - eg. *the Electronic Communications Act* and the *General Data Protection Regulation* .

This means that data may be processed if it is necessary (1) for performance of contract or (2) for compliance witha legal obligation. Data may also be processed (3) for the purpose of legitimate interest or (4) after consent has been given for that specific processing.

Provision of services

We process data in order to manage and deliver on orders in accordance with agreements and to provide services. We also process data to obtain payment for services, to manage billing and payments, to correct errors and address other incidents, and to handle complaints and customer claims.

Lawful basis: performance of contract.

Communication in relation to the services
We also process data in connection with communication with the customer, such as when we send information and contact the customer concerning questions about the services. When the user calls our customer support the call may be recorded. When the user contacts our customer support online using the chat-functionality, the messages may be analysed. We do this to train our employees and improve our ways of working.

Lawful basis: legitimate interest.

Development of services
We process data to manage and develop our business operations, our services and networks as well as our processes. For this purpose, we may also compile statistics for analysis.

Lawful basis: customer consent (traffic data) and legitimate interest (user data).

Marketing
We process different types of data in order to market our products and services. For this purpose, we may also compile statistics for analysis. Marketing may be communicated via e.g. letters, calls, text messages and email.

Lawful basis: customer consent (traffic data) and balancing of interests (user data).

Information security and the prevention of abuse of our services
We process data in order to ensure the security of our services and communications networks, to detect and prevent use of the services that is in violation of law or the terms and conditions for the service. We also process data to prevent abuse of the network and services, and to detect and prevent fraud, virus attacks etc.

Lawful basis: performance of contract (user data) and legal obligation (traffic data).

Compliance with law
We process data in order to meet our obligations under law, for example the Swedish Bookkeeping Act.

Lawful basis: legal obligation.

How long we keep data

We do not keep data longer than we need to. Certain data is deleted immediately while other data is kept for longer periods of time depending on the purpose for which the data is processed and our legal obligations.

- User data is kept as long as the customer remains a customer and for a maximum of 24 months after the the contractual relationship has terminated. Exceptions apply for documentation which under law must be kept for longer periods of time, e.g. the Swedish Bookkeeping Act.
- Traffic data is kept for billing purposes. In case of outstanding invoices, the data is kept until the debt has been settled. Once the invoice has been settled, the data is kept for another 6 months, except for data which under law must be kept for longer periods of time, e.g. the Swedish Bookkeeping Act.
- We also keep traffic data so that we can assist the customer if there is a problem with the services we provide. In order to continuously offer enhanced services based on our customers' needs, we also keep statistics that are based on data. These are kept for 6-24 months.
- In order to provide attractive market offerings based on the customer's needs, we keep certain data, e.g. the amount of text messages, MMS messages and calls, as well as information on the customer's data usage. We keep this data for 36 months.
- We process information about the websites that the user browses and the IP addresses associated with them. This is done to detect and prevent faults in the service. The data is kept for a maximum of 30 days. We do not keep information on the specific pages visited or their content.
- We keep IP addresses in order to investigate, block and delete addresses and messages for the purpose of protecting against internet fraud and limit damages.,. This way we are able to prevent the spread of viruses, spam and trojans. Dynamic IP addresses in the fixed network are kept for 6 months and dynamic IP addresses in the mobile network are kept for 100 days.
- Calls recorded by customer support are kept for 14-28 days.
- Chat conversations with customer support are kept for 60 days.

To whom we release data

We may provide data to:

Other companies within the Telia Company group and subcontractors who process data on our behalf

We use companies in the Telia Company group and in some cases also subcontractors in order to deliver services. This means that we may provide data to them. However, these companies may not use such data for any other purpose than to fulfil the agreement with Telia.

Transfer to third countries
Some subcontractors may have operations in countries outside Sweden or in so called “third countries”, i.e. countries outside the EU/EEA. If Telia, in order to provide products and services, transfers data to a subcontractor in a third country, we always take appropriate safeguard measures to ensure that the data which is transferred is processed in accordance with the Genral Data Protection Legislation and other applicable legislation as the case may be. Telia’s agreements with such subcontractors, state that the suncontractor must comply with the clauses approved by the European Commission regarding the protection of personal privacy. There are also countries that the European Commission has deemed meet the required level of protection of personal privacy .

The European Commission’s list of approved third countries can be viewed here.
The European Commission’s standard clauses can be viewed here.
The Swedish Data Protection Authority's page on data transfer to third countries can be viewed here.

Authorities
Telia is required by law to comply with decisions from authorities regarding the release of data, for example to the police.

Emergency services
Location data is released in connection with emergency calls made to SOS Alarm (the operator responsible for the 112 emergency number in Sweden).

Operators or service providers providing or contributing to the provision of services to the customer
When a customer uses our services to make a call to a person in another operator's network, e.g. international roaming, certain data may need to be disclosed to the operator in order to provide the service.

Rights-holders under copyright law (Ipred)
Ipred, which entered into force in Sweden in 2009, gives rights holders who suspect that illegal sharing of their intellectual property – e.g. a film or music – is taking place to initiate court proceedings to obtain information about what individual an IP-adress is linked to. If the court decides in favour of the rights-holder, Telia has toprovide information on who is using a particular IP address.
Read more here

Directory enquiry services
Telia will disclose the name, address and telephone numbers attributable to the Customer to companies providing directory inquiry services. The directory inquiry services company is then responsible for the processing of this data after the said disclosure has taken place. The customer may oppose such disclosure by providing written notice to Telia.

Other
If the customer, or in some cases the user, has given consent, Telia may provide data to companies, organisations or persons ifor other purposes than those mentioned above.

How we protect data

We work diligently to protect our customers' privacy. Our security work includes protection of persons, information, IT infrastructure, internal and public networks, office premises and technology facilities.

Particular attention is devoted to information security to prevent, deter and detect the dissemination of data to third parties and the loss of data. Access to data is provided only to those who need it to perform their duties. Data processing is logged and checked systematically. Encryption of data is done with reknown and secure encryption methods. We work continuously to fight the occurrence spam and viruses in our networks.

User rights

A user may exercise individual rights in relation to the data we process in our capacity of personal data controller. It is important to ensure that the individual (the specific user) whose data we process, is the same person as the person requesting to exercise individual rights. We therefore request that the customer assists us in identifying the specific user, specifying the right that the user wishes to exercise, as well as providing additional information necessary for us to handle the request and ensure the exercise of the user's rights.

Right of access

The user may, free of charge, request a transcript of the data about the user that we process. We will reply to the user's request without undue delay and in any case within one month from having identiffied the user. If for any reason we cannot fulfil the user's request, we will provide the reason for this.

Right to rectification

If the user discovers an error in their data, the user may request that the error be corrected.

When the incorrect data has been rectified, we will inform the parties to whom we have disclosed the data that the rectification has taken place, unless this proves impossible or would entail an excessive effort. At the user's request, we will provide information to the user about the parties that have been informed of the rectification.

Right to erasure

The user may request the erasure of data if any of the following conditions apply:

- If the data is no longer needed for the purposes for which they were processed previously.
- If the processing is based solely on consent that was provided by the user and that the user has now revoked.
- If the processing takes place for the purpose of direct marketing to the user and the user has objected to the processing of his or her data for this purpose.
- If the user objects to processing when, after a balancing of interests, it is deemed that and there are no legitimate grounds that override the user's interests of integrity.
- If data has not been processed in accordance with the General Data Protection Regulation.
- If erasure is required to fulfil a legal obligation.

If data is erased, we will notify those to whom we have provided such data that this erasure has taken place, unless this proves impossible or would entail excessive effort. At the user's request, Wwe maywill provide also information to the user about of whichthe parties that have been informed of the rectification.

Right to object

The user may object to such data processing that we perform on the basis of legitimate interest. The user must specify which processing he or she objects to. If we consider that such processing should continue despite this, we must show that there are reasons that out-weigh the user's interest of integrity.

If data are processed for direct marketing, the user has the right to object to the processing at any time.

Right to restrict processing

The user has the right to request a temporary restriction of data processing. Processing may be restricted in the following situations:

- When the user considers that the data is inaccurate and the user has therefore requested that we rectify the data that we hold. The user may then request that processing of such data be restricted while the investigation is ongoing.
- When the data processing is unlawful but the user opposes the erasure of the data and instead requests that the processing of this data be restricted.
- When the user needs data to establish, enforce or defend legal claims, even if Telia no longer needs such data for the purposes for which we process them.

When the user has objected to the processing of data, we are permitted to continue to process the data for the duration of the investigation. If the processing of data is temporarily restricted, we will inform those to whom we have provided it that this temporary restriction is in effect unless this proves impossible or would entail excessive effort.

Right to data portability

The user's right to data portability is applicable to the extent that it does not adversely affect the rights of another, e.g. the subscriber.

Notification of violation (complaint)

If the user considers that data is being processed in violation of current regulations, the user should notify Telia immediately. The user may also file a complaint with the Swedish Data Protection Authority.

Compensation

If a user has suffered damage due to data being processed in violation of applicable law, the user may be entitled to compensation. Such a request must be made in writing to Telia, or the user may bring an action for compensation in court.

Cookies

Cookies are used on our websites. They are small text files stored on the device, e.g. a mobile telephone or computer, used to visit a website. Cookies are used improve the experience of our websites for the user or to provide us with statistics on the use of a site.

Most browsers enable the user to block cookies. Go to telia.se/cookiepolicy for more information on how we handle cookies.

We protect children

To counteract the circulation of child sexual abuse imagery, we collaborate with the police to block visits to websites that they inform us contain such material.

Contact information

Personal Data Controller Telia Sverige AB

Telia Sverige AB (company registration no. 556430-0142)
Stjärntorget 1
SE-169 94 Solna,
Sweden

Telephone: 90 400

Personal Data Officer Telia Sverige AB

Telia has appointed a personal data officer to ensure that Telia process personal data correctly and in compliance with law. The personal data officer's contact details are provided to the Swedish Data Protection Authority.

Contact for the exercise of the user's individual rights

Requests to exercise one or more individual rights are to be submitted to Telia in writing at the address below.

Telia Sverige AB

Mina rättigheter - Företag

Svarspost 108317743

978 00 Luleå

Other

The privacy policy may be updated and we will notify you of this at telia.seforetagintegritet. We keep earlier versions here.