PRIVACY NOTICE OF TELIA EESTI AS

Valid from 15 April 2025

We are Telia Eesti AS (*Mustamäe tee 3, 15033 Tallinn, Estonia with reg. code 10234957)* (hereinafter 'Telia') and, here's how we, as the controller of your personal data process and protect it.

Telia recognizes that the protection of personal data is important to our customers and other individuals whose personal data we are processing. Therefore, we protect the privacy of every data subject with responsibility and care.

When processing personal data, Telia shall comply with the General Data Protection Regulation (GDPR)[1], the Electronic Communications Act[2] and other directly applicable legal acts regulating the processing of personal data.

1. What is in this Privacy Notice?

This Privacy Notice applies to the processing of personal data of natural persons, regardless of whether you are a consumer, a user of the services we provide or business customer. In addition, Telia may have service-specific privacy notices, which describe the processing of personal data in the context of a specific service or domain. You can find them on our website: https://www.telia.ee/lepingud-ja-tingimused/.

This Privacy Notice sets out:

- how we collect personal data;
- what personal data we process;
- for what purposes and based on which legal grounds we process your personal data;
- for how long we process your personal data per purpose;
- how we protect and safeguard your personal data;
- to whom we disclose your personal data;
- what rights you have regarding the processing of your personal data and how you can execute them.

This Privacy Notice does not apply to the processing of your personal data by other companies when you are using their services or websites even if they were accessed through Telia's communications network or services. Those companies have their own privacy and cookie notices and they are responsible for processing your data.

2. How do we collect your personal data?

Telia offers a wide range of products and services. The information we collect about you depends on the products and (or) services you order and (or) use and the data you provide to us when you order products and (or) services or register on our websites, applications and other platforms.

You are not obliged to disclose any personal data to Telia, but please note that if you choose not to disclose your personal data, we will not necessarily be able to provide you with all our services or offer relevant products/solutions to you.

Telia collects and further processes your personal data from the following sources:

- **Directly from you**

  This data derives from you, when you do business with us, buy or subscribe to our services, or when you register with or log in to our services, visit our website, reply to our customer satisfaction survey or contact us by phone, email or chat.

- **Generated data**

  This data is generated when you use our communication networks or our services, i.e., when you are making phone calls, sending messages (SMS), browsing the Internet, using TV and entertainment services, visiting our websites and applications etc.

---

[1] 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 on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] https://www.riigiteataja.ee/akt/127022022003?leiaKehtiv

- **Derived data**

  This data is created based on your personal data, such as conclusions about your possible interests or consumption habits, made e.g., by means of analytics for marketing purposes.

- **Other source data**

  This data is obtained from other service providers, public authorities, or publicly available registers, such as state agencies (ie population register, e-business register), banks or credit bureaus (for credit-check and solvency assessment). We also process personal data received from other Telia companies in accordance with this Privacy Notice under the conditions laid down by law.

3. What is personal data and what kind of personal data do we process?

Personal data (hereinafter also data) is data that is directly or indirectly associated to you as a private individual (it can be the customer or a user using services under the customers contract, such as business customer employees, partners representatives or private customers family members, authorized persons).

For the sake of clarity, we group your personal data into the following data categories:

Basic personal data

Basic personal data is any information relating to an identified or identifiable natural person that does not fall under any other data type. For example: personal identification information (name, personal ID code, date of birth), contact information (address, e-mail), information related to ordering and provision incl contract information, information related to payments, credit and debt related information, consents and objections that you have provided; your communication with Telia, marketing data, images and videos captured by CCTV etc.

Traffic data

Traffic data is the data generated using communications services. It is necessary for the conveyance of a communication through the electronic communications network and for the billing thereof. This data reflects your activities when you are using communications services and communications network at a particular time and place. For example, the number A calls the number B at a specified time, at a specific location, and the call has a certain duration, time and format of SMS/MMS's sent to or from you, Internet usage data (incl. IP address, domains, amounts of data sent/received) etc.

Non-personal communication data is processed to provide services and to compile invoicing. This datatype refers to communication data obtained from the use of communications services in our network by roaming service clients, clients of other operators or internet service providers, i.e. individuals who have not been authenticated by Telia.

Location data

Location data refers to the geographical location of a person and (or) terminal equipment (e.g., GPS coordinates, base station location derived from the data received through use of services or applications). Location data other than traffic data may be processed for the purpose of the provision of value-added services and to the extent necessary for the provision of these services or based on your specific consent.

Location data does not refer to your place of residence, service provision or invoicing address, contact address, etc. That information is part of your basic personal data.

When location data is used for the purpose of the conveyance of communication on an electronic communications network or for billing purposes such it is defined as traffic data.

Content of communication while using services provided by Telia

Content of communication refers to information exchanged (communication) between two communicating parties using an electronic communications service, e.g., the content of phone calls and e-mails, SMS and MMS content when using Telia services.

It is important to specify that when you interact with another communication party by phone call, via email, or, for example, by sending text messages (SMS), we do not record or use this content. Telia is not the controller for the content of communication as we only convey the content through our networks.

In case Telia is a party to the communications, the data exchanged between the parties is not considered content of communication.

Special categories of personal data

Special categories of personal data include racial or ethnic origin, political views, religious or philosophical beliefs or trade union membership, genetic data, biometric data used to as a unique identifier of a natural person, health data or data on sex life and sexual orientation of a natural person.

We do not retain or collect such data, unless you have provided this information to us yourself or provided us with an explicit consent to process such personal data in which case you will be informed about the processing activities performed in more detail upon providing explicit consent.

Children's personal data

Telia processes children's personal data to the extent permitted by law, when appropriate in the case in question. Telia takes reasonable efforts to ensure and verify that the custodian of a child under the age of 13 has agreed to the processing of personal data, considering the available technology and the privacy risks related to the processing.

Device tracking data

Device tracking data consists of data collected by means of cookies and similar tracking technologies in connection with web or mobile browsing. For more information about the cookies used by Telia please see the cookie notice on our website.

Anonymous data

We may also process anonymous or aggregated data that is not associated with you as an individual. Such data is not personal data according to GDPR and the processing of it is thus not covered by this Privacy Notice.

4. How do we process your personal data?

We collect and process your personal data to the extent it is needed for specified and legitimate purposes and only if necessary to fulfil the purpose.

In this Privacy Notice we have grouped all purposes of processing into nine categories. You have different rights and opportunities to influence and make choices regarding the processing of your personal data that are described in this Privacy Notice.

4.1. The legal grounds for processing

Telia applies a legal ground for each processing activity. Telia processes your personal data based on your consent, in order to fulfil the contract between you and Telia, in order to fulfil a legal obligation derived by law or based on Telia's legitimate interest.

Data processing based on consent

With your consent, Telia may process your basic personal and/or traffic data. When requesting your consent, we will inform you of the purpose and how you can withdraw your consent at any time.

Performance of a contract

We process personal data on the legal ground performance of contract when it is strictly necessary. Such processing of personal data primarily manifests in allowing a certain result for our services and products and this cannot be achieved by avoiding the processing of personal data.

Compliance with an obligation arising from legislation

If data processing is necessary for the performance of an obligation arising from law, Telia cannot decide on the collection and further processing of such personal data, nor can you.

Processing based on legitimate interest

When we process personal data based on the legal ground legitimate interest we balance between your and our rights. We process personal data on this legal ground for improving and developing our communications network

and systems, usage statistics, etc. because we want to ensure our customers high quality of services, smooth products and service delivery and the best customer experience.

If we process personal data for marketing and profiling purposes on the legal ground legitimate interest, you always have the right to object to the processing via Telia's e-environment.

4.2. For what purposes do we process your data?

Customer administration

Telia processes basic personal data for the purposes of administering the customer relationship and to improve customer experience and customer care operations.

The maximum retention time for keeping personal data for customer administration purposes is 36 months after end of the customer relationship. Depending on data type, the personal data might be deleted also earlier during the customer relationship.

Purpose	Legal ground	Data category with examples of attributes	Retention time
Credit-check Processing necessary to assess if a customer or potential customer is considered suitable to receive services and/or equipment in credit but is not mandatory by law	Performance of contract	Basic personal data, i.e. name, address, contact information, services used, products purchased, credit information	5 years after end of relationship
Customer care Customer care operations aimed at better customer experience. For this purpose we have concluded that the processing is highly beneficial to provide customer care, to improve our customer care services, and to measure their efficiency at the same time as the customer will have an improved customer experience where their needs will be met faster and in a more efficient way	Legitimate interest	Basic personal data, i.e. name, address, customer ID	36 months after creation
Order management Issuing, managing and completing data subject orders for products and services or other	Performance of contract	Basic personal data, i.e. name, personal identification number, customer ID, address, e-mail address, phone number, images	36 months after creation; Call recordings to verify orders 2 years after call recording
Customer administration Customer relationship operations, i.e. establishing and terminating customer agreements, customer identification, updating customer data, dispute resolution	Performance of contract	Basic personal data, i.e. name, social security number, Telia ID, product description, contract number, address, e-mail address, phone number	36 months after end of relationship
Business reporting Processing necessary for statistics and analytics to detect trends and correlations. For this purpose we have concluded that the processing will support us in creating more relevant offerings and general recommendations that may benefit our customers	Legitimate interest	Basic personal data, i.e. products and services used, address, customer ID	36 months after creation

Delivery of products and services

Telia uses your personal data for delivering the services and products you have ordered from Telia.

The maximum retention time for personal data processing in relation to service and product delivery is 36 months after end of the customer relationship. Depending on data type, the personal data might be deleted also earlier during the customer relationship.

Purpose	Legal ground	Data category with examples of attributes	Retention time
Product and service delivery	Performance of contract	Basic personal data, i.e. contact details like name, address, phone nr and e-mail address, services/products purchased and ordered; Traffic data, i.e. caller/receiver and IP-address; location data	36 months after end of relationship; 12 months after creation for traffic data
Communications transmission necessary to achieve transmission of electronic communications	Performance of contract	Traffic data, i.e. caller/receiver and IP-address; location data	12 months after creation for traffic data
Service quality assurance, i.e., ensuring quality of services in accordance with contractual or legal obligations	Legal obligation or performance of contract	Basic personal data, i.e. name, social security number, Telia ID and product description; Traffic data, i.e. phone number of outgoing and incoming calls, timestamp of transmission, length of transmission, operator, IMEI, IMSI, data sent, geographical location of mobile device	36 months after end of relationship 12 months after creation for traffic data

Billing

Telia uses personal and traffic data for billing purposes and for revenue assurance purposes.

The maximum retention time for the processing for billing purposes is between 24 months and 7 years as from end of the customer relationship. Depending on data type, the personal data might be deleted also earlier during the customer relationship.

Purpose	Legal ground	Data category with examples of attributes	Retention time
Billing and payment Calculating payments, issuing invoices, collecting payments and debts	Performance of contract	Basic personal data, i.e. name, social security number, address, invoice number, invoice date, invoice amount, payment date, payment amount and payment category; traffic data and location data	24 months after end of relationship (12 months from creation for traffic data); 15 years as of debt in case of an outstanding debt in the absence of an ongoing recovery procedure and publishing in a payment default register
Accounting Complying with accounting legal obligations	Legal obligation	Basic personal data, i.e. name, social security number, Telia ID, phone number, service account number, invoice number, invoice	7 years after end of calendar year in which the

		date, payment date, payment amount payment category, invoice amount; contract data, e-enviroment transaction logs	accounting year was closed
Revenue assurance, identifying and detecting unbooked or lost revenue For this purpose we have concluded that the processing is of fundamental importance to ensure Telia's revenues and that's this processing is in the interest of our customers and our owners	Legitimate interest	Basic personal data, i.e. name, personal identification number, order amounts	24 months after creation

Security

Telia processes personal and traffic data to monitor the security of telecommunication networks and are bound by contractual obligations to maintain and restore the security of the networks and systems used for service provisioning, including incident management. The maximum retention time for personal data for security purposes is between 0 and 36 months depending on the specific purpose. Depending on data type, the personal data might be deleted also earlier during the customer relationship.

Purpose	Legal ground	Data category with examples of attributes	Retention time
Network and information security Maintaining and restoring security of electronic communications networks and services, ensuring information, asset, customer and personnel security	Performance of contract	Basic personal data; Traffic data, i.e. E-mail address, caller's and receiver's telephone number	24 months after creation; 12 months after creation for traffic data
Network and information security Maintaining and restoring security of electronic communications networks and services, ensuring information, asset, customer and personnel security. For this processing we have concluded that the processing benefits Telia and our customers, the economy and society at large	Legitimate interest	Basic personal data, i.e. name, personal identification number, order information	24 months after creation
Incident management Resolving incidents and issues related to services, detection of technical faults and errors in transmission of electronic communications	Performance of contract	Basic personal data, i.e. customer notification information and information related to the incident	24 months after resolving
Fraud detection purposes, e.g., identifying misuse, fraud prevention in sales, and identifying customers. For this purpose, we have concluded that this processing has benefits for Telia, our customers, users, the economy, and society at large, when avoiding damages.	Legitimate interest	Basic personal data, i.e. name, personal identification code, contact information; video recordings; personal QR codes, access logs to Telia' facilities	36 months after resolving

See also privacy notice for video surveillance in Telia' facilities			
Mandatory monitoring Security, privacy and network monitoring required by law, e.g., supplier audits, DPO audits and testing, network-based security measures such as firewalls, IDS, AV and monitoring the network for illegal traffic or patterns	Legal obligation	Basic personal data e.g. traffic data, phone number, title, category, source, date, start and end time for streaming, outgoing and incoming phone number, timestamp for transmission, length of transmission, operator, IMEI, IMSI, data sent, geographic location for mobile device	Deleted after resolving of the matter.

Development

Telia processes your personal and traffic data in order to develop new products and services and improve the products and services offered by us. Telia processes data to develop and maintain our systems and networks in order to provide you with up-to-date products and services based on cutting edge technology.

The maximum retention time for data processed for development purposes is up to 36 months or until consent has been withdrawn depending on the purpose. Depending on data type, the personal data might be deleted also earlier during the customer relationship.

Purpose	Legal ground	Data category with examples of attributes	Retention time
Service and product improvement Development, innovation and improvement of services and products. For this purpose, we have concluded that this processing is needed for Telia to provide services from a business and security perspective	Legitimate interest	Basic personal data, i.e. name, address, customer ID, products and services used, phone recordings and Telia' chat content; Traffic data, i.e. service usage data	24 months after end of relationship (for basic data). 12 months as from creation (for traffic data). 24 months as from creation for phone/voice recordings. 36 months for chat history
Development and maintenance purposes of our systems and networks For this purpose, we have concluded that this processing is generally expected to receive the provided services	Legitimate interest	Basic personal data, i.e. name, address, products and services used	36 months after creation

Marketing

Telia processes your personal and traffic data for marketing purposes.

The maximum retention time for the processing of personal and traffic data for marketing purposes is 5 years after marketing activity during customer relationship and not more than 2 years after end of the customer relationship. Depending on data type, the personal data might be deleted also earlier during the customer relationship.

Purpose	Legal ground	Data category with examples of attributes	Retention time
Direct marketing to electronic contact information Contacting the data subject for marketing purposes via e-mail and SMS	Consent for a private customer; legitimate interest for a business customer	Basic personal data, i.e. name, contact information	24 months after customer relationship; upon withdrawal of consent or opting out of direct marketing
Marketing messages in other marketing channels, i.e. reaching out to customers in online channels, like Telia webpage, chatbot, Telia apps or other channels with marketing messages	Legitimate interest	Basic personal data, i.e. name, contact information	24 months after end of relationship, but no more than or 5 years after marketing activity
Basic marketing and basic profiling This means that we create a general profile of you to better understand you as a customer and tailor the services and content accordingly. For basic marketing and basic profiling purposes, we have concluded that by providing customers with targeted and tailored marketing, our customers will receive more relevant marketing communication, incl. media planning activities and that individuals may have an interest in receiving tailored marketing	Legitimate interest	Basic personal data, i.e. name, contact information, services and products purchased, order history	24 months after end of relationship, but no more than or 5 years after marketing activity
Metadata marketing Processing of traffic data for marketing profiling, follow-up of marketing campaigns, tracing sales and similar	Consent	Traffic, i.e., outgoing and incoming phone number, timestamp for transmission, length of transmission, operator, IMEI, IMSI, data sent, geographic location for mobile device	Consent is deleted 12 months after the end of relationship; upon withdrawal of consent; 12 months after creation for traffic data
Extensive profiling, evaluating, analyzing, or predicting behavior, interests, location, incl. using cookies and similar trackers etc. When processing your data for such a purpose, Telia will give you more specific information about the processing activity while asking for your consent	Consent	Basic personal data, i.e. IP address, unique identifiers; Traffic data, i.e. device data; location data, i.e. IP location	24 months after the end of relationship; upon withdrawal of consent; 12 months after creation for traffic data

What is meant by profiling for marketing purposes?

Profiling for marketing purposes refers to data processing where we process your data using statistical, mathematical or predictive analysis methods for creating various links, probabilities, correlations, patterns, models, marketing profiles, etc. As a result, we can predict or derive your expectations, preferences and needs regarding the consumption of goods and services offered by us.

Profiling always includes some margin of error because the correlations are based on mathematical and statistical procedures. This is an inherent characteristic of profiling, and, at the same time, the main

source of risk to individuals' privacy, namely because of the possibility of occurrence of two kinds of error: a) wrongly assigning a person to a category; b) excluding from a category those that in fact belong to it.

How do we use marketing profiling in Telia?

- We create and assign customer types or profiles to data subjects

We analyze customers' demographical data (age, gender), service usage data and other aggregated data by using several different, internationally recognized statistical analysis methods to conduct profile analysis, to develop different customer segments, types, or profiles. Based on the identification data and probability assessment used in the profile analysis, we can determine the specific customer segment, type, or profile (e.g., technology savvy customer) and use this assessment for different marketing decisions (for example displaying personalized content and advertising in the e-environments).

- We assess behavior and interest based on the customer's journey

In this case we can analyze and use customers' data related to the use of services, website visits and other data concerning purchasing behavior and consumption, as well as various methods of statistical analysis and profile analysis, to derive customers behavior patterns, models, and customer types. As a result, we are provided with a probability assessment on how interested a specific customer would be in ordering and using a specific service.

We are careful when performing profiling in order to avoid irrelevant offers or other unwanted marketing communications towards you. You have the right to object, at any time, concerning the processing for marketing purposes.

Processing to fulfil legal obligations

We are to fulfil applicable legal obligations, including obligations related to personal data processing. Such processing includes retaining data for and answering law enforcement requests and enquiries and complying with court orders. We are also obliged to process personal data for regulatory reporting to national regulatory authorities and for fulfilling obligations set for significant market players by the national regulatory authority.

We are subject to certain laws and regulations related to providing financing services, such as fulfilling the know your customer obligations, mandatory customer identification and credit-check obligations to fulfil the responsible lending requirements. In addition, we need to process personal data to fulfil anti-money laundering obligations.

The maximum retention time for data processed for development purposes is 10 years. Depending on data type, the personal data might be deleted also earlier during the customer relationship.

Purpose	Legal ground	Data category with examples of attributes	Retention time
Mandatory retention for law enforcement and emergency services	Legal obligation deriving from Electronic Communications Act	Basic personal data, i.e. name, user credentials; Traffic data, i.e. outgoing and incoming phone number, timestamp for transmission, length of transmission, operator, IMEI, IMSI, data sent, geographic location for mobile device	12 months after creation
Court orders, i.e. an order that requires us to provide certain data	Legal obligation	As stated in the specific court order	12 months after complying with the court order
Significant market player obligations, (telecommunication operators are required to share data with other operators)	Legal obligation	Basic personal data, i.e. number portability related data; Traffic data, case specific	Case specific

Authority and individual reporting, i.e. providing data subjects rights of access report or reporting personal data breaches	Legal obligation (i.e. GDPR, ESS, IKS etc)	Basic personal data, Traffic data upon request	24 months after resolving
Mandatory customer identification, e.g. AML, mobile ID etc	Legal obligation based on Anti-Money Laundering and Counter Terrorism Act	Basic personal data, i.e. name, personal identification code, contact information and data specified in the legal acts.	Minimum 5 years after end of relationship; in the case of Mobile ID, 10 years from the expiration of the certificate
Mandatory credit-check Requirement for responsible lending. Assessment of a consumer's creditworthiness and for the verification of the data submitted, keeping of credit file	Legal obligation (Creditors and Credit Intermediaries Act)		Minimum 36 months after end of agreement
Know your customer (KYC) Financial legislation such as anti-money laundering and counter-terrorist financing legislation obliges all financial companies to have an in depth knowledge of their customers	Legal obligation (Anti-Money Laundering and Terrorist Financing Act)	Basic personal data i.e. name, personal identification code, contact information	Minimum 5 years after end of relationship
AML retention	Legal obligation (Anti-Money Laundering and Terrorist Financing Act)	Basic personal data	Minimum 5 years after end of relationship
AML retention of criminal activities	Legal obligation (Anti-Money Laundering and Terrorist Financing Act)	Basic personal data	Minimum 10 years after end of relationship
Speak-up-line reporting suspected violations of laws and regulations, or company policies	The Act on the Protection of Whistleblowers from Professional Violations	Basic personal data, i.e. name, contact details, position	3 months after resolving

Supplier relations

To conduct business responsibly, Telia chooses its suppliers very carefully to determine whether the supplier meets Telia's responsible business criteria. Such research about suppliers may also include personal data processing of individuals related to specific suppliers.

Purpose	Legal ground	Data category with examples of attributes	Retention time
Supplier relationship Supplier due diligence, offers management containing personal data	Legitimate interest	Basic personal data, i.e. name, contact details, position in the supplier company	12 months after end of relationship

5. Automated decision making

Automated decision making is a means of processing your personal data where decisions are made by technological means without human involvement. An automated decision can be based on different processing activities, for example, profiling, and these processing activities need to have appropriate legal grounds in place. If there is any human intervention involved, the processing is not considered being automated (e.g., if a person reviews a credit-check prior to the decision).

Telia uses the legal grounds performance of contract and a legal obligation arising from law when processing personal data within the scope of automated decision making.

In case you are not satisfied with the automated decision made by Telia regarding you, you have the right to

- ask Telia for a human intervention instead of the automated decision making,
- express your point of view and
- to contest the decision.

5.1. Credit limit

Credit limits are indicative financial limits applicable to the customer, in excess of which Telia is not obligated to provide the customer Telia contractual services for credit. The final amount and conditions of the credit offered to the customer will become clear after the submission of the respective application by the customer and after having assessed the customer's creditworthiness.

5.2. Credit rating

A credit rating is an assessment of the probability of insolvency of a private customer based on the relevant customer's payment behaviour, background information obtained from Telia's internal information systems and Creditinfo. Creditinfo's external risk assessments are risk parameters calculated on the basis of data available from public sources for the assessment of credit risk related to a private person. Different information is used to calculate the credit rating; this includes information from the Creditinfo credit register, the business activity of the specific individual, as well as the experience and activity of the private person in the credit market. The higher the score obtained, the higher the credit risk associated with that private person. More information about this can be found on the website of Creditinfo Eesti AS.

The credit rating results 'new' and 'negative' result in the non-receipt of credit, and while signing up for a service, Telia may require the customer to provide additional collateral (e.g. surety, guarantee, deposit), as well as make an advance payment (e.g. the credit limit is exceeded or the customer's creditworthiness assessment is insufficient).

The results 'satisfactory' and 'positive' will generally result in automatic permission for subscribing to a service if the customer has no current debt. While determining credit terms, we collect relevant information about the customer's payment behaviour and background:

- from Telia's information systems (e.g. length of the customer relationship, payment behaviour in relation to Telia: data on debts and payment of invoices), incl. companies related to the customer;
- from public databases (official announcements, information provided by enforcement agents and other official registers, such as the business register, population register);
- from the database and external credit risk assessments of Creditinfo Eesti AS (Credit Register of Creditinfo: the dates of occurrence and termination of the default of both the customer and the companies related to the customer; debt amounts and the sector of origin of the debt; Creditinfo's private scores and credit assessments of customer -related companies);
- from other reliable sources (e.g. background information from private registries for compliance with due diligence requirements pursuant to money-laundering regulations, court decisions, etc.), if necessary.

5.3. Debt management

If the customer does not pay the debt despite the debt notifications, the communications services will be automatically restricted and the customer will not be able to use the service to the normal extent. If it is a mobile or telephone service, only outgoing calls will be restricted, and the customer will be able to continue to receive

6. For how long do we store your personal data?

We will store your personal data for the period required to attain the purposes stated in the privacy notice or until the legal obligation stipulates that we do so as stated above in section 4.2.

It should be considered that in certain cases, exceptions apply to maturities. For example, some automatic maturities do not apply in case of debts or in cases where Telia needs to retain your personal data in order to defend itself in legal disputes and claims in which case we store the data until it is necessary to defend Telia in any proceedings against us have ceased. Neither do these rules apply to the storing of anonymous data, as in such case, we are no longer dealing with personal data.

7. To whom do we disclose your personal data?

Below you can find different recipients to whom we provide your personal data.

- **Companies of the Telia Company Group**

  We share data within Telia companies to get an overview of our customers commitments with all Telia companies. At an aggregate level, i.e., when personal data is merged with other customers' data, that information is used for analytics, including following up on the distribution of customers between different companies within our group. In addition, we share customers data across our Telia Company Group in order to make company management and administrative decisions.

- **Our partners working for us,** who will process your data on behalf of Telia.

  These partners may process personal data only in accordance with Telia's instructions and to the extent necessary for the proper performance of their obligations under the contract with Telia. For example, IT service providers, equipment servicing partners, and marketing offices performing marketing efforts on our behalf.

  Please see the list of our approved contractual partners on our website. In this list we have the data processors we use and partners with who we have co-liability when processing personal data.

- **Other telecommunication network operators or service providers** who provide services or are employed to provide you services, such as invoicing or troubleshooting and eliminating errors.

  When you leave our communications network and use mobile roaming services in other operators' networks (e.g. on a trip abroad), these operators can collect and process your personal data and also receive data from Telia.

  When you, for example, subscribe to Spotify through us, the service provision may require disclosure of your data to the service provider in question. If you send your device to us for servicing, the warranty procedure may require disclosure of your data to the manufacturer.

  Your data may also be disclosed in association with electronic identification or electronic signing to identification broker services or service providers whose services you access or log in by means of Telia's identification service or identification device (such as Mobile ID) to verify your identity or to sign electronically.

  If you use the payment feature of your mobile subscription, i.e. you purchase a ticket to be paid on your phone bill, Telia may process the personal data needed to execute the payment transaction and also disclose the subscription number to the service provider from whom you purchase the service using the payment feature.

- **Competent state authorities and other public authorities**
  We disclose personal, traffic and/or location data to security and surveillance authorities, including the police, prosecutors, courts, emergency centre (112) etc. if the corresponding obligation arises from the legislation. For example, for the purpose of preventing, investigating, detecting criminal activities, to provide the emergency service, etc., to the extent required by the law and in accordance with a predefined procedure.
- **Other third parties**
  Companies managing joint debtors' data files.

Telia has the right to provide debtors' (meaning data subjects who have failed to meet their financial obligations to Telia in a timely and proper manner) data to companies managing joint debtors' data files maintain and then provide data to third parties for the purposes of creditworthiness and debt management. Debtor's data shall only be provided according to the conditions laid down by law, after the data subject has been given a notice about failure to fulfil their financial obligations.
Companies which take over (purchasing) the right to claim.
In accordance with the Law of Obligations Act, Telia (the creditor) has the right to assign the right of claim on the debt portfolio to other the person who may take over the claim. Such a transfer does not require the consent of the debtor and the debtor can be notified either by the old, or the new creditor.
Debt collection companies, to the extent necessary to initiate and enforce debt collection.
Providers of legal, auditing and other professional services, bailiffs, etc.
In connection with **mergers and acquisitions** and various business transactions and transfers.

8. Is your data transferred outside the European Union or European Economic Area?

Our partners who process Personal data on our behalf are sometimes located outside the European Union (EU) or the European Economic Area (EEA). When transferring Personal data outside the EU or EEA, we ensure by means of agreements (e.g. by the use of the EU Commission's standard contractual clauses) or otherwise (an adequacy decision by the European Commission) that the transfers are implemented as required by law. In addition, we ensure that Personal data remains protected regardless of whether they are transferred outside of the EEA.

We assess risk factors related to the transfer to or access to personal data from outside EU/EEA by conducting a transfer impact assessment (TIA). Telia uses TIAs to verify, on a case-by-case basis, whether the law of the third country ensures adequate protection of personal data when transferred. We collaborate with our sub-processors to gather sufficient information to perform and complete TIAs. Based on the law or practices of the country the data is transferred and the effectiveness of the appropriate safeguards we review whether and which supplementary measures should be implemented. In determining which supplementary measures are most appropriate, we assess the effectiveness of such measures in the context of the transfer or other applicable scenario, the third country law and practices and the transfer tool used.

The European Commission's list of countries outside of the EU that offer an adequate level of data protection can be found on European Commission's website.

The European Commission's standard contractual clauses can be found on European Commission's website.

9. How do we safeguard your personal data?

9.1. How we safeguard your data?

Safeguarding your personal data is of the utmost importance to us why we implement necessary organisational and technical security measures to ensure the integrity, availability and confidentiality of the data. These measures include the protection of employees, information, IT infrastructure, internal and public networks, as well as office buildings and technical equipment.

The purpose of information security activities is to implement the appropriate level of protection of information, risk mitigation and risk prevention. We ensure the security of the communication network and the confidentiality of the message contents and form of messages sent by you, as well as the time and method of sending them, in accordance with terms and conditions that apply to Telia services and with legislation. The measures required for this are implemented by Telia's internal security regulations.

Our employees are subject to data confidentiality and protection requirements. Personal data protection training is provided to them, and employees are liable for fulfilling their obligations. Also, our partners are required to ensure that their employees comply with the same rules as we do, and their employees are liable for meeting the requirements for the use of personal data.

Learn more about Telia's information security policies in general on Telia Company's website.

9.2. How you can safeguard your data?

Prior to disclosing your personal data to a third party or entering it somewhere, consider who will receive the data and how securely it will be stored. In the case of communication and internet services, it must be considered that by enabling access to your data (e.g., on our self-service), either due to your own negligence or any other reason, you will be providing access to call logs, service details, invoicing information and data of associated persons.

If you suspect that your personal data has been processed contrary to our privacy notice or that your information has been disclosed to strangers, be sure to inform us as soon as possible by contacting us using the below described methods. This way we can solve the situation as quickly as possible and help minimize potential losses. You can always check and change your data using the below presented methods.

10. Your privacy choices and rights

Your rights and options depend on the purposes of the processing and on the situation.

The right of access

You have the right to access your personal data that Telia has, at any time. Additionally, you have the right to be informed of the purposes of data processing, categories of personal data, the recipients, or categories of recipients to whom the personal data has been or will be disclosed and retention times of the data.

To request access to your data you can submit an application when logged in. In case it is not possible to log in, a request can be sent via e-mail to privacy@telia.ee. You need to properly authenticate yourself. If less than six months have passed since your previous request, Telia has the right to charge you for the request.

The right to withdraw your consent

If the processing of Personal data is based on consent, you have the right to withdraw consent at any time. This can be done by logging in to self-service portal. Upon receipt of the data subjects consent withdrawal, Telia will start to implement changes immediately, but it may take up to 2 working days for the change to take effect. It is worth noting that application or withdrawal of consent does not have a retroactive effect.

The right to rectification

You have the right to request Telia to rectify incorrect or inaccurate personal data concerning you and to supplement incomplete personal data. If, while reviewing your data, you have discovered that the data is incorrect or if your personal data has changed, you can always change them yourself in the self-service.

In the event that you want to rectify data that you are unable to change in the self-service, send us a request. The request form will become available when you **log in**.

The right to object to processing

You have the right to object to the processing of your personal data when your data is being processed based on the legal ground legitimate interest. If we agree to your objection, we will stop processing your data for that purpose unless we can give strong and legitimate reasons to continue processing your data despite your objection.

You have an absolute right to object to Telia processing your data for direct marketing and we will stop processing the data if you object. This right cannot be used in a situation where we are required to compile, submit, or defend a legal claim (e.g., we believe that a person has breached the contract and therefore have to turn to a court or other law enforcement agency to protect our rights).

If you wish to object to the processing of your data, please send us a request. The request form will be available when you **log in**. You can exercise your right to object also logging in through www.telia.ee or by opting out from direct marketing according to the information provided in the marketing communication.

The right to erasure ("right to be forgotten")

You are entitled to erase your data in certain circumstances, for example, if

- the processing of personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- you initially consented to the use of your data but have now withdrawn your consent and there is no other legal ground for the processing;
- you have objected to the processing and there is no overriding legitimate ground for the processing (your interests outweigh our interests);
- it was identified that your data have been unlawfully collected and (or) further processed;
- Telia has a legal obligation to erase the data;
- the data was collected from you as a child for an online service.

If you wish to demand the deletion of your data, please send us a request. The request form will be available when you **log in**.

The right to restrict the processing of your personal data

In certain cases, you have the right to request the **restriction to the processing of your personal data**. You should take into account that this right requires a very precise wording of the purpose, and may in some cases lead to the temporary suspension of services.

You can request the restriction to the processing of your personal data in the following cases:

- to verify the accuracy of personal data if you have challenged the accuracy thereof;
- to establish unlawful processing of data;
- you need personal data to prepare, file, or defend a legal claim;
- you are objecting for the assessment of a legitimate interest and wish to restrict the processing in question until a decision has been made.

If you wish to restrict the processing of your data, please send us a request. The request form will become available when you **log in**.

The right to data portability

You have the right to receive your personal data that you have provided to Telia and that are processed with your consent or for the performance of a contract.

Telia gives you access to your personal data in a structured, common, and machine-readable format, or enables to have it transferred directly to another service provider or controller, provided that the other service provider has the capacity to receive the data in that format.

If you wish to transfer your data, please send us a request**.** The request form will become available when you **log in**.

The right to lodge a complaint

If you believe that your personal data is being processed in violation of current regulations, you should report it to Telia as soon as possible by contacting us at privacy@telia.ee.

You are always entitled to contact us, the Data Protection Inspectorate or the court to protect your privacy rights and personal data. The Data Protection Inspectorate is a public institution that can be contacted or consulted on issues related to personal data protection.

The right to damages

If you have suffered damage because of Personal data being processed in violation of applicable laws or regulations, you may be entitled to damages. Damages claims can be brought forward to Telia or to a court.

A damage claim request brought forward to Telia must be made in writing and must contain the following information:

- full name,
- social security number and
- any subscription number.

The request is then sent to info@telia.ee.

11. How can you exercise your right and contact us?

You can exercise all the above-mentioned rights by contacting Telia and verifying your identity in any convenient manner:

- https://andmed.telia.ee/privaatsusvalikud-ja-oigused;
- by e-mail to our DPO at privacy@telia.ee;
- by calling customer care (+372) 639 7130 or sending an email to info@telia.ee.

Once we have identified you properly, we will promptly register and process your request. We will provide you with information on the action taken on your request no later within one month of receipt of the request.

In case we are not able to find a solution together and you remain dissatisfied, you have the right to contact and make a complaint to the Data Protection Inspectorate (www.aki.ee), which is responsible for the supervision and control of personal data protection legislation.

Telia is committed to conducting responsible and sustainable business. If you suspect that Telia has acted contrary to the legislation or the Privacy Notice, you can also report the matter confidentially through Telia Company's Speak Up Line (so-called whistleblowing system).

If you have any questions or you want to discuss how Telia Company protects your privacy, please contact our Group Data Protection Officer at DPO-TC@teliacompany.com.

Learn more about privacy in Telia Company on Telia Company's website.

Learn more about security at Telia Company on Telia Company's website.

12. Changes to this Privacy Notice

Just as modern communications services, devices and solutions are evolving at a fast pace, so are the data processing activities necessary to provide those. We will do our best to keep the Privacy Notice up-to-date and available to you on the Telia website www.telia.ee. For this reason, we encourage you to periodically visit our website, where you will always find the most current version of this Privacy Notice. We may also notify you of the most significant changes in the Privacy Notice on our website, by email or in any other reasonable manner.