Contents

How we protect your privacy

SpareBank 1 takes your privacy seriously and constantly works to ensure that your personal data is safe with us. You can read more about how we process your personal data in this privacy policy.

The privacy policy was updated 29th of August 2023.

Who is responsible for your personal data?

Terms

This privacy policy is aimed at you as a customer, potential customers and other users of SpareBank 1's services and websites. SpareBank 1 is made up of several banks and companies. Where we write 'SpareBank 1' or 'we' in this privacy policy, we mean the banks and companies that make up SpareBank 1.

Controller

The bank and/or the companies within SpareBank 1 with whom you have a customer relationship are the 'controllers' responsible for processing your personal data. If you need to get in touch with us about privacy/data protection, please email the bank's or company's data protection officer.

Download the privacy policy

You can download the privacy policy in PDF format here.

Find out how we protect your privacy. Download our privacy policy (PDF in English).

Other companies within SpareBank 1

General insurance and personal insurance policies are provided by Fremtind Forsikring. Read more about Fremtind's processing of personal data.

Pension savings are handled by SpareBank 1 Forsikring. Read more about SpareBank 1 Forsikring's processing om personal data.

SpareBank 1 also has a cooperation agreement with LOfavør AS that allows us to offer certain benefits to members of unions affiliated to the Norwegian Federation of Trade Unions, which is also a customer of SpareBank 1.

Joint controllers

In some circumstances, certain companies within the SpareBank 1 alliance will cooperate in deciding how your personal data will be processed. In these circumstances there will be a so-called joint controllership between these parties. Joint controllership means that the companies decide together which of your information is to be collected and how your personal data will be processed.

Regardless of the joint controllership, you will be able to enforce your privacy rights by contacting the bank or the company you are affiliated with.

Your rights

Below you will find information on your rights when we process personal data about you.

Right to access

You have the right to request access to the personal data we process about you, and you have the right to receive a copy of this information. You also have the right to information about how we process your data. Information about this can be found mainly in this privacy policy.
Information about your products, agreements, contact information and transaction history are available in your online bank. If you cannot find the information you are looking for, please send us a request for access. We may ask you to clarify to what information or processing activities you want to access. If you do not have an online bank or cannot read digital documents for some other reason, we can send you the information on paper.
There are exceptions to the right of access in certain circumstances. This typically applies when we are legally bound to secrecy or when we have to keep the information confidential for the prevention, investigation, detection and prosecution of criminal acts. Another exception is when the information is contained only in documents prepared for internal case processing and exemption from access is necessary to ensure proper processing.

Right to rectify

It is important that the information we have about you is correct. SpareBank 1 checks its data against the Norwegian Population Register and other sources. In addition, we ask you at regular intervals in online banking and mobile banking to confirm that the information we have registered about you is correct. If you believe that the information we about you is incorrect or incomplete, you have the right to request that the information be corrected or updated.

Right to erasure

You have the right to request that your personal data be deleted if:

- You withdraw your consent to the processing and there is no other justified reason for the processing.
- You object to the processing and there is no justified reason to continue processing.
- You object to processing for the purpose of direct marketing.

- The processing is illegal.
- The personal data has been collected in connection with offering information society services (e.g. social media) to a child.

Right to restrict processing

You may demand that SpareBank 1 restrict the processing of your personal data in certain situations, for example, if:

- You believe that the personal data is incorrect or that the processing is not lawful.
- SpareBank 1 wants to delete data, but you need the information because of a legal requirement.
- You have lodged an objection to the processing and it is based on a balance of interests.

We will still store the relevant information, but all other processing of the personal data will be temporarily suspended. SpareBank 1 may begin processing your personal data again in connection with legal requirements or to protect another person's rights.

Protecting your personal data

If you have the right to require that only a limited number of employees be able to access your personal data, we will facilitate this.
For further terms and conditions and information on shielding personal data, please email the bank's data protection officer.

Right to data portability (the right to receive your data in a machine-readable format)

You have the right to receive a copy of the personal data you have given us in a machine-readable format. Unlike to the right of access, this right applies only to personal data that you have personally provided to us and that is processed based on your consent or agreement.
If you want to retrieve your information, you can log in to online banking and download your data under 'Settings'.
If you want information about your insurance policies, you can fill out a simple form using BankID, and Fremtind Forsikring will make it available to you within 30 days.

Right to object

You have the right to demand that SpareBank 1 stop processing personal data about you based on its legitimate interests, unless there are compelling legitimate grounds that override your interests, or the processing is for the establishment, exercise or defence of legal claims. You may also demand that SpareBank 1 stop processing your personal data for direct marketing purposes, including profiling related to such purposes.
If you wish to opt out of direct marketing, please contact Customer Service.

How to exercise your rights

If you wish to exercise your rights, please email the bank's or company's data protection officer.
Email is not considered as a secure channel, so please do not send us confidential information via email. We will answer you as quickly as possible and no later than within 30 days. If we see that the processing time will be longer than 30 days, we will let you know.
If you have given us your consent to use information about you, you can withdraw or modify this at any time via your mobile bank or online bank.
You can also contact us to withdraw or modify your consent.

The personal data we collect

Personal data includes information and assessments that can be linked directly or indirectly to you as an individual. The various banks and companies in SpareBank 1 process different types of personal data about you depending on your relationship with them and the products and services you have purchased.

The types of personal data we collect

- Identification and personal information such as name, national identity number, nationality, other identification numbers issued by the government and copies of identification documents.
- Contact details such as phone number, address and email address.
- Financial information such as customer and product agreements, credit history, revenue information, payment card number and transaction data.

- Information required to fulfil regulatory obligations such as tax country, foreign tax registration number, information in connection with financial advice, information related to anti-money laundering work and reporting to public authorities.
- Specific categories of personal data such as health information and trade-union membership when you buy insurance cover or enter into an agreement with LOfavør AS.
- Information on income, debt, place of work and employment, education, marital status, family relations and dependent responsibilities.
- Photos and video recordings taken in connection with our customer and sponsorship events.

Where do we collect personal data about you from?

From you

As a general rule, the personal data and information we register about you will be obtained directly from you as a customer, for example when you create an account, apply for a loan or when we talk to you via digital channels and chat services. If a guardian has been appointed for you, we will also collect information about your guardian.

From third parties

We collect information about you from others in order to provide services to you, to comply with legal requirements and to quality assure information you have provided to us. Examples of information collected from third parties such as publicly available sources/registers or private business sources can include:

- Identity information, family relationships, demographic information and mortgage data from the Norwegian Population Register, Property Register or Register of Motor Vehicles. When you apply for a loan as a customer, we collect credit and debt information about you from the debt registers and the credit reference agency Dun & Bradstreet.
- When executing payment transactions, we collect information from senders (payers or recipients), shops, banks, payment service providers (such as Vipps and PayPal), invoice issuers (such as TietoEvry and Nets) and others.
- In order to carry out customer checks pursuant to the money laundering and financial contract regulations, we collect information from public authorities such as the tax authorities, Brønnøysund Register Centre and police. We also collect

information from sanctions lists published by the Norwegian authorities and international organisations such as the EU, the UN and the Office of Foreign Assets Control (OFAC).

- In connection with the registration of customer relationships for self-employed individuals, banks are required by law to collect information about the key people and beneficial owners of a company. The information is collected from the Brønnøysund Register Centre and commercial information services that provide information about, for example, beneficial owners and politically exposed persons.
- With your consent, your bank can, in line with the Payment Services Directive, share account and transaction information with other banks or financial institutions. This means, for example, that you can view your accounts with other banks in our mobile bank and vice versa, and that you make payments from these.

From cookies

We collect information about your use of our websites, platforms and digital apps such as traffic data, location data and other communications data. Read more about our use of cookies here.

Mobile applications and access rights

Our mobile apps sometimes need access to functions and information on your phone. The apps only ask for the access required to enable them to work. We cannot view the data on your phone. You can read more about the access rights the apps request in the various apps.
Our apps in the App store
Our apps in Google Play

Legal basis for the use of your personal data

We always need a valid legal basis in order to process your personal data. SpareBank 1 can have several different legal bases for processing your personal data and information.

Agreement with you

Your personal data is mainly processed for the purposes of customer management, financial advice, billing and the performance of banking, insurance and financial services in line with the agreements we have entered into with you. When new agreements are entered into with you, you will always be made aware of the terms and conditions that apply in relation to the agreement.

Legal obligations

We also process your personal data to fulfil our obligations in compliance with statutes, regulations or governmental decisions.
Examples of processing based on legal obligations:

- Prevention and detection of criminal acts such as money laundering, terrorist financing and fraud
- Sanctions monitoring
- Accounting requirements
- Reporting to tax authorities, law enforcement agencies, enforcement and supervisory authorities
- Risk classification related to risk management such as credit development, credit quality, capital adequacy and insurance risk
- Requirements and obligations related to payment services
- Other obligations related to service or product-specific legislation such as securities, funds, pledged collateral, insurance or mortgages.

Legitimate interest

We may use your personal data if this is necessary to address a legitimate interest that overrides your right to privacy. The legitimate interest must be legal, pre-defined, genuine and objectively justified in relation to our business activities.

- Examples of processing based on a legitimate interest:
- Marketing, product and customer analytics. The analyses provide the basis for marketing, process, business and systems development. The purpose is both to improve our solutions and to provide the best possible offers, products and services to our customers.
- Profiling, for example, when we conduct customer analyses for marketing purposes or monitor transactions to detect fraud and other criminal acts.

- Transaction classification of your expenses and earnings into categories to provide you with a better overview and understanding of your personal finances.
- Automatic transfer to your SpareBank 1 bank when you log into your mobile bank, so you do not have to specify your bank affiliation every time you log in.
- The development of machine learning models in order to better identify suspicious transactions in connection with banks' statutory anti-money laundering work.
- Identifying your subscriptions or other recurring expenses that we can help you cancel.

When we process personal data about you on the basis of our legitimate interests, you can object to the processing. Read more about your right to object under *Your rights*.

Consent

In some circumstances, we will ask for your consent to process personal data. Any consent given by you as a customer must be voluntary, explicit and informed. Consent provides one of the bases for processing if we need to process special categories of personal data (e.g. health information and trade union information).

If you have provided consents to Sparebank 1, you can withdraw them at any time. If you withdraw your consent, the processing will stop, and the personal data related to the consent will be deleted.

You can turn your consents on and off in your mobile bank or online bank.

Consents related to cookies can be modified here.
To withdraw other consents, please email the bank's or company's data protection officer.

What we use personal data for

Your information is primarily processed for customer management purposes and to fulfil our obligations to you. We also process your personal data to provide you with information and offers, as well as to fulfil our legal obligations.

Products and service delivery

We will process your personal data to fulfil the obligations we have assumed in relation to the performance of assignments and service agreements entered into with you. In order to, for example, send you invoices, execute payment transactions on your accounts and respond to inquiries from you, we need to process your personal data.
Basis for processing: Agreement. Legal obligations.

Customer service

We want to be available to our customers both digitally and in person. Therefore, you can contact us via chat, email, letter, phone and other channels. We can also conduct digital meetings with you when you have agreed this with one of our customer advisers.

If you start a chat from the bank's website without being logged in to online banking, the call is anonymous. The chat is archived for the purposes of statistics and evaluating customer service, but it cannot be linked to you as a customer. Chats are retained for a period of one year.

If during a chat you choose to talk to an adviser, the chat conversation will be made available to that adviser. The purpose is to enable them to familiarise themselves with your enquiry before the chat continues.

If you start a chat when you are logged in to your online bank, it will be saved and linked to you as a customer. We do this in order to provide you with the best possible customer service when you are in subsequent contact with the bank, and as documentation in the event a dispute should arise.

If you contact us via social media (e.g. Facebook), one of our customer advisers will be able to contact you. However, if you need to share personal information, please still use one of the secure channels on our website (link).
Basis for processing: Legitimate interest, agreement.

Investment services

When we provide investment services, we are required by law to make audio recordings and retain calls, meetings and other customer communications. In the case of in-person advice

meetings, we must keep minutes of the meetings. Such documentation is retained for at least five years to document the investment services we provide.

Audio recordings of phone calls

We may occasionally record phone calls made to and from our call centre. You will be informed about this before the call starts, so that you can opt out of being recorded. The recording will be used only if you or we need to document the content of the conversation. To document notification of lost cards, we make audio recordings when the loss is reported over the phone. The audio recording is retained for 18 months.
In some cases, we want to record phone calls for training purposes. Before the call starts, you will be notified of this and be given the option of opting out of being recorded.
You can request access to audio recordings by contacting the bank. You must specify at what time the call took place and from what phone number when you request access.
Basis for processing: Legitimate interest, legal obligation.

Marketing of our products and services

SpareBank 1 wants to provide our customers with information about products within the product categories for which there is already a contractual relationship with the bank and/or the individual company. In these circumstances, the bank/company will use neutral personal data such as your name, contact details, date of birth and the services or products for which the customer has already entered into an agreement.

Our products are divided into the following categories:

- Payment services
- Savings and deposit products
- Loans and other credits
- Pension insurance
- Non-life insurance
- Personal insurance

With the aid of personal data and interest and user group profiles, we personalise communication, advice and offers so that they are relevant and useful. The information about you may also be used in analyses and customer surveys to develop and improve products and services and enhance customer service. Analyses for marketing purposes that

include transaction data will only be performed if you have explicitly consented to this in your mobile bank or online bank.

You may also see ads from us on social media and other web pages when we buy ad space through various media.

Digital customer service and marketing channels

Web pages: Homepage/online bank, News Centre, Insurance Talk, Exchange Weekend.
Apps: Apps in, app store,Apps in Google Play
Social media: Facebook, Instagram, YouTube, Twitter, LinkedIn, Snapchat.
Other channels: Newsletters, email and customer surveys
If you have opted out of marketing in the Reservation Register in Brønnøysund, we will of course respect this decision.

Facebook Pixel

By using Facebook image pixel on SpareBank 1's website, we can deliver personalised content from SpareBank 1 in Facebook's channels. This content will be more targeted and relevant to the user. Facebook Pixel collects information about your activity.

Adform script

We use Adform to keep track of the ads that should be displayed, to count the number of views, clicks etc. This is done on an anonymous basis and cannot be traced back to individuals. This is the system in which our marketing materials are located, and the information we collect is used to deliver personalised content and provide relevant ads on external websites, such as online newspapers.

Google Ads and Adobe Advertising Cloud Search

In Google Ads and through Adobe Advertising Cloud Search, we keep track of the ads that are to be displayed, count the number of displays and clicks, and see if any action is taken based on your ads. The information we collect is used to deliver personalised content and to provide relevant ads. We cannot link customer data to the ad placement.

Appnexus script, programmatic buying

Programmatic media advertising is automated buying and selling of online ads through an ad exchange. The online newspapers put ad slots (displays) up for sale on the ad exchange, and

as an advertiser, we place bids for what we want to pay. Using the script, we can set criteria to be used in the bidding and optimise the advertisements.

Basis for processing: Legitimate interest, consent.

Social media

Sparebank 1 uses various social media sites such as Facebook, Instagram, YouTube, Twitter, LinkedIn and Snapchat in order to be available to our customers. In these channels, we share useful information and relevant stories and updates about SpareBank 1 in local communities.

If you have a profile on one of the various social media sites, you must also comply with their terms and conditions and privacy policy. We encourage you to review their terms and conditions.
We also process and use aggregated data about visits and activity on our social media pages for statistical and analysis purposes. This data cannot be linked back to individuals.

None of the information you provide to us via social media, such as reactions and comments on our posts, is stored by us. It is stored by the social media site of which our page is a part. You can delete information you have provided at any time, for example if you delete comments you have posted. Please note that the information will not be deleted if you simply stop following our page.

Basis for processing: Legitimate interest.

Customer and market research

We process personal data in connection with market and customer satisfaction surveys. For example, after you have been in touch with us, we ask you to tell us how you experienced the contact. Your feedback helps us to provide you with even better products and services. We can also measure the effectiveness of improvement measures and look at the link between customer satisfaction and customer behaviour over time.
If you do not want to share this type of information with us, you can decide not to respond to the survey we sent you.

Basis for processing: Legitimate interest.

Risk classification of customers and credit portfolios

We use personal data to assess risk in connection with the sale of products and services. This provides you, the customer, with the confidence that your assets will be well taken care of. In accordance with the provisions of the Financial Institutions Act, the Securities Trading Act and the CRR/CRD IV Regulations, we will process credit information, application information and other information about you in order to calculate our capital requirements for credit risk. Such processing is also carried out in connection with the establishment of your customer relationship and when ascertaining which services and products are suitable for you.

Calculations are made using our own models, procedures and decision-making processes for lending, credit management and control mechanisms, IT systems, and internal policies related to classifying and quantifying the institution's credit risk and other relevant risks. In connection with this, personal data may be collected from credit reference agencies. Information can also be retrieved from Norwegian debt registers for the purpose of developing models for risk assessments and formulating individual credit policy rules.

Rules pursuant to the Financial Institutions Act, the Securities Trading Act and the CRR/CRD IV Regulations mean that institutions must share customer information in order to fulfil the institution's governance, control and reporting requirements. This particularly applies in the case of information related exposures in default.

Basis for processing: Legal obligations

Prevention and detection of criminal acts

We process personal data to prevent, detect, clear up and deal with fraud and other criminal acts against you, other customers or us.

We will also process personal data to prevent and detect transactions related to proceeds from criminal acts or in conjunction with terrorist financing. We do this because we are required to investigate and report suspicious transactions under the Anti-Money Laundering Act, as well as to carry out identification checks on all our customers.

Under the Anti-Money Laundering Act, we are also required to report suspicious information and transactions to the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) and the Financial Intelligence Unit Norway (EFE). The information will be retrieved from, and may be disclosed to, other banks and financial institutions, the police and other public authorities.

Basis for processing: Legitimate interest, legal obligation.

Security

SpareBank 1 implements technical and organisational security measures to protect your personal data. SpareBank 1 constantly works to ensure that your personal data is protected from loss, misuse, inadvertent access, disclosure, alteration or destruction. This is done through access management, logging, encryption, firewalls, access control and CCTV monitoring, as well as other measures that support your security and security at SpareBank 1. We have a dedicated management system for information security, access control, nonconformance management and training.

CCTV surveillance

Sparebank 1 has CCTV surveillance and in our premises and for our ATMs. Recordings are deleted after 90 days unless they are turned over to the police or the bank has the right to use the recordings for other purposes.

Basis for processing: Legal obligation. Legitimate interest

Logging

Your activity in your online bank and mobile bank is logged in order to track what changes have been made and by whom, for example, if there is a systems error or a breach of security occurs. Similar logging takes place in our internal systems where we process your personal data. Sparebank 1 has a legitimate interest in logging this traffic in order to identify or prevent potential unwanted activity in or against the bank. The scope of such logging is limited to the minimum amount strictly necessary and proportionate to ensure online and information security.

You can also enhance the security of your personal data in a few simple steps. Read about Secure Online Banking and Mobile Banking, How to protect your card and 10 tips on preventing ID theft. (Add links)

Basis for processing: Legitimate interest, agreement and legal obligation.

Logging in to your online bank and mobile bank

When you use Sparebank 1's online services, we can identify the computer or mobile device you use to carry out banking services and register user behaviour and the user environment, the status of your computer/device, etc. Sparebank 1 uses this information to verify that it is the right person using the relevant service. How your personal data is processed when you use BankID is described in *the terms and conditions for BankID (PDF) and in BankID's privacy policy*.

SpareBank 1 neither stores nor processes biometric information such as fingerprint and facial recognition data on your phone if you choose to use these to log in to our services. This data is only stored locally on your mobile phone and is not sent to Sparebank 1. The processing of biometric data on your phone is performed by the manufacturer (Apple, Google, Huawei, Samsung, etc.). For more information on the processing and storage of biometric data, please refer to the manufacturer's privacy policy.
It is your responsibility as a customer to choose the log in solution (PIN code or biometrics) that you want to use.

Basis for processing: Legitimate interest, agreement and legal obligation.

Testing and development purposes

SpareBank 1 is constantly working to improve its systems, services and products. To address personal data security and ensure that our solutions are working properly, we need to be able to use data for testing and development purposes. The general rule is that only fictitious or anonymised data should be used, although sometimes we need to use real customer data to ensure functionality and security.

Basis for processing: To offer our customers good solutions, we need to be able to develop and test new solutions before they are put into production. We consider this processing to

be very closely related to our original purpose of delivering products and service to our customers. We have documented this via a so-called compatibility assessment.

Statistics for public enterprises and private companies

Sparebank 1 processes personal data to provide statistics for public enterprises and private companies. The statistics we share with these enterprises and companies will be aggregated data that cannot be linked to you as an individual (anonymised). For example, the statistics will be based on demographic information, product information and transaction information. The enterprises and companies can only use the statistics to improve goods, services, communication and offers for consumers.

Examples of statistics can include what times most people visit supermarkets, how many customers live in a detached house or what average citizens in a municipality spend on electricity, phone subscriptions or food.

Basis for processing: Legitimate interest.

Automated decisions and profiling

Automated decisions

In some cases, we use automated decisions to assess whether we should enter into or perform an agreement with you, such as when you buy loan products or receive advice via the bank's website.

Automated decisions are decisions made exclusively by computer programmes without human intervention or influence. If automated decisions will have legal implications for you or otherwise significantly affect you, we may use them only if:

- It is necessary to enter into or perform an agreement with you.
- You have consented to it.

We will tell you if an automated decision has been made. You can also ask to have an automated decision reviewed by an account officer, ask for a decision to be explained or contest a decision.

Basis for processing: Legitimate interest

Profiling

Profiling is a form of automated processing of your personal data. We use profiling and data modelling to, for example, provide you with specific services and products that match your preferences, to prevent money laundering, to set prices for certain services and products, to uncover fraud and risk of fraud, to assess the likelihood of default, to estimate the value of assets, and to serve marketing purposes. You have the right to object to such profiling.

Basis for processing: Legitimate interest

Disclosure of personal information

Sometimes we share information about you with others who have the right to use it, such as government agencies, payment service providers, or companies in the SpareBank 1 Alliance. This may be done to fulfil our agreement with you, to meet legal obligations or to protect our legitimate interests. Before sharing personal data, we always ensure that we comply with the relevant confidentiality provisions applicable in SpareBank 1 as a financial institution.

Internally in SpareBank 1

The banks and companies in SpareBank 1 have a duty of confidentiality regarding customer information. As a general rule, this duty of confidentiality also applies between the companies in SpareBank 1. Nevertheless, companies in SpareBank 1 may disclose certain personal data to each other where permitted by law. This could be:

- Your contact details
- Your date of birth

Information about the SpareBank 1 company in which you are a customer and the services and products you have entered into an agreement to receive.
If you would like more relevant advice and offers from us, you can consent to the companies in SpareBank 1 sharing more information about you. The consents can be found in your online bank and mobile bank.

To public authorities

In many instances, SpareBank 1 has a statutory duty to disclose personal data to public authorities. Examples of this may include disclosures to tax authorities, the Norwegian

Labour and Welfare Administration (NAV), the courts, the police, supervisory authorities, the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) and public tribunals. Registered personal data will only be disclosed to public authorities and other third parties when this is required by a statutory duty of disclosure or right to disclose.

To private companies

Pursuant to the law, personal data may be disclosed to other banks, insurance companies, financial institutions and partners. Examples of this might be if you want to view account information in one bank via a different bank or if you want to view your insurance cover from Fremtind in your mobile bank.

In the event of payments to or from abroad, we will provide pertinent personal data to the foreign bank. The laws of the recipient country determine the extent to which the information is disclosed to government agencies or regulatory bodies. This might be done to comply with the recipient country's tax laws, measures against money laundering or terrorist financing.

If you default on your credit agreements, the information may be disclosed to a debt collection company for the purpose of collecting the defaulted claim on behalf of the creditor. The claim may also be sold to a debt collection company which then takes over as creditor for the claim.

About foreign tax liabilities

Norway has entered into agreements with several countries on mutual tax reporting to combat tax evasion and international tax crime. The agreements are often referred to as the Common Reporting Standard (CRS) and the Foreign Account Tax Compliance Act (FACTA). Under the agreement, Norwegian financial institutions are required to identify and report persons, companies and other entities that reside or are domiciled abroad to the Norwegian tax authorities. For more information about CRS and FATCA, consult the Norwegian Tax Administration.

Use of processors

Sparebank 1 uses third parties to deliver services to you as a customer. If these third parties process your personal data, they are acting as our processors. For example, SpareBank 1 uses a number of cloud services to deliver well-functioning services to you as a customer. SpareBank 1 enters into data processing agreements with all of the companies that process personal data on our behalf. These agreements govern how a data processor can use the personal data to which they gain access. SpareBank 1 will only use processors that guarantee they will comply with the Personal Data Act and GDPR.

SpareBank 1 currently uses different types of processors, such as:

- SpareBank 1 Utvikling – our own IT and development company, which provides services to the entire SpareBank 1 Alliance.
- Amazon (AWS) – a platform we use to build the digital bank, the financial platform, etc.
- TietoEvry – one of SpareBank 1's largest third-party providers of core banking and other payment systems
- Microsoft—for example, for Teams meetings with you or general email correspondence

Transfer out of the EU/EEA

SpareBank 1 primarily wants to use processors based in the EU/EEA. If SpareBank 1 uses providers outside the EU/EEA, we will ensure that the following conditions are met to ensure that the privacy and rights of our customers are properly protected:

- There is an approved transfer basis for the delivery of personal data to a third country, such as the use of standard contracts (EU standard clauses) approved by the European Commission, the data processor has valid, binding corporate rules (BCR) or the European Commission has decided that there is an adequate level of protection in the relevant country.
- The level of protection for the processing of personal data in a third country has been assessed as equivalent to the level of protection in the EU/EEA, as a result of specified technical and/or organisational measures.

How long do we retain your personal data?

We retain your personal data for as long as it is necessary for the purposes for which it was collected and processed, unless statutes or regulations require us to retain it for longer.

For as long as it is necessary

This means that, as a general rule, we retain your personal data for as long as it is necessary to fulfil an agreement you have entered into with us, or in compliance with the requirements for retention time in laws and regulations. After that, it is deleted or anonymised.

In cases where the retention of your personal data is based solely on your consent, and you withdraw your consent, we will delete the data as soon as possible.

Examples of retention times

- Offer: up to six months after the customer has received the offer
- Documentation collected and prepared to prevent and detect money laundering and terrorist financing: 10 years after transaction has been completed or the customer relationship terminated
- Information we are required to keep under the Bookkeeping Act and Bookkeeping Regulation: up to 10 years
- Audio recordings of investment services: at least five years, and, if deemed necessary, up to 13 years.
- Information collected for calculating regulatory capital requirements for credit risk (so-called internal rating-based approach): Up to 50 years (the information is stored separately with strict access controls).
- Documentation and history related to the execution of an agreement: up to 13 years after the end of customer relationship (this corresponds to the period during which you may, on specific terms, make claims against us under your agreement, the so-called ‘period of limitation’).
- Information collected from you in connection with a conversation about cancelling cards or your need for emergency funds if, for example, your wallet has been stolen: three years

- Backups of logs: Retained for as long as it is appropriate for the individual service (backup logs are stored separately with strict access controls).
- Your data/information: Is available to customer advisers for two years after your customer relationship has ended. You have the right to object to this.

How we use cookies and analysis tools

It is important to us that you feel safe when you visit our website, and at the same time confident that we are doing our best to provide you with what you need.

What are cookies?

We use cookies in our digital channels: websites, online bank and mobile bank.

Cookies are small data files that are stored on your computer or your mobile phone by the browser or app you are using. A cookie belongs to a particular website and therefore cannot be read by other websites.

If you use our website without identifying yourself, the cookie consent will only apply to the device (e.g. mobile phone or PC) you are using at the time. When you log in to your online bank or mobile bank, you can choose to allow whether the response for device should also apply to your entire customer relationship.

You can choose which categories of cookies we can use.

Web analysis tools and statistics make us better

We use various analysis tools, based on what you have consented to. Various analysis tools are used, for example, to:

- Collect statistics about your usage patterns.
- Systematise statistics and build segments for relevant content in our digital channels, such as websites, apps, social media and via ads.
- Test and present relevant content to you.
- We also use tools to manage and process data, such as Microsoft CRM Dynamics.

Product development and analyses

Sparebanken 1 may collect information about you that is used to analyse how you as a customer use Sparebank 1's services via digital channels and other communication channels. This information is also used to identify potential demand for new products and services, and to improve the functionality of existing products and services.
The following are examples of how we apply analysis:

- To determine price levels
- To assess and monitor credit risk
- To personally adapt our web pages
- To prevent and detect fraud
- To analyse website traffic and use of email and text messaging
- To personally adapt information and relevant ads

Read more about how we use cookies here.

Basis for processing: Legitimate interest.

Cookies, pixels and scripts we use

Technical cookies

We need to use technical cookies to make the websites work. Therefore, these cannot be turned off.

Functional cookies

We use functional cookies so you do not have to make the same choices every time you are on our websites. These store information about your use of the websites and the settings you have selected in order to personalise the functionality for you.

Cookies that archive statistics

We use cookies that store statistics to make the websites better and easier to use. This information helps us understand how the websites are used, which in turn enables us to improve.

Cookies for targeted marketing

For you to obtain content that is tailored to you, we use cookies that collect information about your usage pattern and your interests. This means that we can provide you with more relevant and targeted marketing, both from us and our partners. We do this in several channels, for example on our websites and in social media.

Cookie overview

In addition to cookies, we use pixels and scripts from third parties. These are snippets of code that allow us to analyse your usage across social media and our channels, and we use this to provide you with more relevant marketing.
You can choose which categories of cookies we can use.
Turn cookies on and off

Questions and complaints

If you think we are breaching the privacy policy or you are unhappy with how an enquiry has been handled, please contact us so that we can provide answers and clear up any misunderstandings.

Contact information

If you have any questions about this privacy policy or our processing of your personal data, please email the bank's or company's data protection officer.

Complaining to the Norwegian Data Protection Authority

You also have the right to complain to the Norwegian Data Protection Authority. You can find information about how to complain on the Norwegian Data Protection Authority's website.

Changes to the privacy policy

We need to update the privacy policy at regular intervals to provide you with the correct information about how we process your personal data.

Overview of changes

An overview of the changes made to the privacy policy is provided below.

Changes	Date
Necessary adjustments and clarifications in the section on cookies.	17 June 2022
Necessary adjustments and clarifications in line with the development of our services, products and websites.	8 March 2021
Necessary adjustments and clarifications in line with the development of our services, products and websites.	31 March 2023
Necessary adjustments and clarifications in line with the development of our services, products and website, as well as judicial changes in privacy.	28 August 2023