Contents

Safeguarding your privacy

At SpareBank 1, we take your privacy seriously and always strive to ensure that your personal data is secure with us. You can read more about how we process your personal data in this privacy policy.

The privacy policy was updated 16.05.2024.

Who is responsible for your personal data?

Terms

This privacy policy is aimed at customers, potential customers and other users of SpareBank 1's services and websites. SpareBank 1 is made up of a number of banks and companies. Where we write "SpareBank 1" or "we", we mean banks and companies in SpareBank 1.

Controller

It is the bank and/or companies you have a customer relationship with in SpareBank 1 that are responsible for processing your personal data. If you need to contact us in relation to privacy, please email the data protection officer at the bank or company.

Download our privacy policy

You can download our privacy policy as a PDF here.

Safeguarding your privacy. Download our privacy policy (PDF in English).

Other companies in SpareBank 1

Non-life and personal insurance policies are provided by Fremtind Forsikring. You can read more about how Fremtind processes personal data here.

Pension savings are provided by SpareBank 1 Forsikring. You can read more about how SpareBank 1 Forsikring processes personal data here.

SpareBank 1 also has a cooperation agreement with LOfavør AS that offers a number of benefits to SpareBank 1 customers who are also members of unions affiliated with the Norwegian Confederation of Trade Unions (LO).

Joint processing responsibility

In some cases, companies in the SpareBank 1 Alliance cooperate on how your personal data is processed. In these circumstances, they have so-called joint processing responsibility. Joint processing responsibility means that the companies jointly decide what your data will be collected for and how it will be used.

You can still contact just the bank or company you have a customer relationship with to exercise your rights.

Your rights

Your rights when we process your personal data are described below.

Right of 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 mainly be found in this privacy policy.
Information about, for example, 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 what information or processing activities you want to access. In those circumstances where your online bank is not available or you cannot read electronic documents for some other reason, we can send you the information on paper.

There are some exemptions to the right of access. These include when we have a legal duty of non-disclosure or we have to keep information confidential for the prevention, investigation, detection and prosecution of criminal acts. Another exemption exists regarding information that is solely contained in documents prepared for internal use and an exemption from access is necessary to ensure proper processing.

Right to rectification

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. At regular intervals, we also ask you in your online or mobile bank to confirm that the information we hold about you is correct. If you believe that the information we hold 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 no other legitimate basis for the processing exists.
- If you exercise your right to object to the use of your personal data and there are no compelling grounds for the processing.
- You object to the use of your personal data for direct marketing purposes.
- The processing is illegal.
- The personal data processing concerns minors, if the data was collected in connection with providing information society services.

In many circumstances, we have to retain information about you, even though you want the information deleted. This may be true both while you are a customer of ours and for a period after the agreement with us has ended. In practice, this means that you may not always be able to require us to delete your data. This may be because we have a legal duty to retain it or because we must safeguard our legitimate interests. Similarly, we may need to retain your information to establish, exercise or defend a legal claim.

Right to restrict processing

You can require 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 the data, but you need the information due to a legal claim.

You have objected to the processing and we need to assess whether we have a legitimate interest in continuing to process it. We will keep the relevant data stored, 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 are entitled to require that only a limited number of employees may and are able to access your personal data, we will facilitate this.
For further terms and conditions and information on protecting personal data, email the bank's data protection officer.

Right to data portability

You have the right to obtain a copy of the personal data you have given us in a machine-readable format. Unlike the right of access, this right only applies to personal data that you have provided to us and that is processed on the basis of consent or agreement.
If you want to obtain a copy of the information, you can log in to your online bank and download your data under “Settings”.
If you would like details pertaining to your insurance cover, you can fill out a simple form with your BankID, and Fremtind Forsikring will make them available to you within 30 days.

Right to object

You have the right to require SpareBank 1 to stop processing your personal data if the processing is based on legitimate interests, unless there are grounds that take priority over your interests or serve to establish, enforce or defend legal claims. You may also require SpareBank 1 to stop using your personal data for direct marketing sent directly to you, including profiling for such purposes.
If you wish to opt out of direct marketing, please contact customer services.

Exercising your rights

If you wish to exercise your rights, please email the data protection officer at the bank or institution.
Email is considered an unsecure channel. We recommend that you do not send us confidential information via email. We will respond as quickly as possible and within no more than 30 days. If it is clear to us that the matter will take longer than 30 days to process, we will let you know.
If you have consented to us using information about you, you can change your mind about this at any time in your online or mobile bank.
You can also contact us to change your consent.

Personal data collected

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.

Types of personal data collected

- Identification and personal information such as name, national identity number, citizenship, other identification numbers issued by the government and copies of proof of identity.
- Contact details such as phone number, address and email address.
- Financial information such as customer and product agreements, credit history, account numbers, balances, payment card numbers and transaction data.
- Messages and communication with the bank, annual statements, bank statements
- Information required by law 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.
- Special categories of personal data such as information about health and trade union membership in connection with the purchase of personal insurance or the conclusion of agreements with LOfavør AS.
- Information on income, assets, 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.
- Audio recordings may also be made when you talk to us on the phone. You can choose to refuse this when you call customer services. We are required by law to make audio recordings when you receive investment advice from us.
- Our premises and ATMs have camera surveillance for security purposes.
- If you have consented to this in your cookie settings for our websites, data is collected on your use of our websites and online and mobile banks.

Where do we get your personal data?

From you

As a rule, the personal data we hold about you was provided directly by you as a customer, for example, when you opened an account, applied for a loan or contacted us via digital channels and chat. If a legal guardian has been appointed for you, we will also collect information about the guardian.

From third parties

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

- Identity information, family relationships, demographic information and information about collateral from the Norwegian Population Register, Eiendomsverdi AS, Norwegian Property Register or Register of Motor Vehicles.
- When you apply for a loan as a customer, we collect credit information and debt information about you from, for example, the debt registers and credit information agencies.
- 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.
- We collect information from other public authorities such as the tax administration, Brønnøysund Register Centre and the police to conduct customer checks pursuant to anti-money laundering and financial contract legislation We also collect information from sanction lists published by Norwegian authorities and international organisations such as the UN, EU and Office of Foreign Assets Control (OFAC).
- In connection with the registration of customer relationships for self-employed individuals, we are required by law to collect information about the key persons and beneficial owners of the company. The information is collected from the Brønnøysund Register Centre and commercial information services that provide information about matters that include rightful owners and politically exposed persons.

- If you consent to it, we can, in line with the payment services directive, exchange account and transaction information with other banks or financial companies. This means, for example, that you can see accounts from other banks in our mobile bank and vice versa, and that you make payments from them. Publicly available information, for example from social media or search engines.

From cookies

We collect information about how you 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 apps and access rights

Our mobile apps sometimes need access to functions and information on your phone. The apps only ask for the access rights 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.

Ours apps in the App Store

Our apps in Google Play

Legal basis for using your personal data

We must always have a legal basis for using your personal data. There are several different legal bases for using personal data in SpareBank 1.

Agreement with you

The main purposes behind processing your personal data are customer management, financial advice, billing and the implementation of banking, insurance and financial services as they are described in agreements we have entered into with you. All of the agreements we have with you, or will enter into with you, describe their terms and conditions clearly such that it is easy to understand what the agreement includes.

Legal obligations

We also process your personal data in order to meet our legal obligations, such as:

- Preventing and detecting criminal acts such as money laundering, terrorist financing and fraud
- Monitoring sanctions
- 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
- Credit rating
- Requirements and obligations related to payment services
- Other obligations related to service or product-specific legislation such as securities, funds, collateral security, insurance or home loan mortgages

Legitimate interest

We may use your personal data if this is required to safeguard a legitimate interest that outweighs considerations concerning your privacy. The legitimate interest must be legal, pre-defined, real and factually rooted in our business activities.

Examples of basing our processing on legitimate interest include:

- Marketing, product and customer analyses that help us improve our solutions and provide our customers with the best possible services, products and offers.
- Checks, reporting and analyses that help us develop our business and systems, as well as ensure that our operations are properly managed.
- Profiling, for example when conducting customer analyses for marketing purposes or monitoring transactions to detect fraud and other criminal acts.
- Transaction classification of your income and expenses to provide you with a better overview and understanding of your personal finances.
- Automatic transfer to your SpareBank 1 bank when you log in to your mobile bank, so you do not have to disclose your bank affiliation every time you log in.

- Developing and using machine learning models to identify suspicious transactions in connection with statutory anti-money laundering work.
- Using machine learning and artificial intelligence to classify your transaction details, including in order to provide you with a better overview of where your money goes.
- Identifying your subscriptions or other regular expenses that we can help you terminate.

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

Consent

In some cases, we will ask for your consent to process personal data. Any consent given by you must be voluntary, unconditional and informed. Consent is one of the bases for processing if we need to process special categories of personal data (e.g. information about health and trade union membership).

We also use your consents to, for example, collect information about your activities on our websites (via cookies) and send you more personalised marketing based on data we hold about you.

If you have given us consents concerning cookies or marketing, you can withdraw these at any time in the online and mobile banks. If you withdraw your consent, the processing will stop and the personal data associated with the consent will be deleted. You can also read more about what your consents are used for in the overview provided in the online and mobile banks.
Consents regarding cookies can also be changed here .

To withdraw other consents, email the data protection officer at the bank or institution.

What we use personal data for

The purpose of using your information is primarily customer management and to fulfil our obligations to you. We also use personal data to provide you with information, offers and to fulfil our legal obligations.

Delivering products and services

We will process your personal data to fulfil the obligations we have assumed concerning the performance of transactions and services for you. For example, we will need to process your personal data to send you invoices, execute payment transactions on your accounts and respond to your enquiries.
Basis for processing: Agreement, legal obligation.

Customer services

We want to be accessible for our customers both digitally and in-person. For that reason, you can contact us by email, chat, letter, phone and other channels. We can also organise 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 the online bank, the chat will be anonymous. The chat will be archived for use in statistics and evaluating customer services, but cannot be linked to you as a customer.

If during the chat you choose to speak to an adviser, the adviser will be given access to the chat. This is done so that they can familiarise themselves with your enquiry before continuing the chat.

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. This is done to provide you with the best possible customer service when you contact the bank again later on, and as documentation in the event of a dispute arising.

If you contact us via social media (e.g. Facebook), one of our customer advisers will be able to follow up your enquiry with you. If you need to share personal information, we continue to recommend that you use the secure channels on our websites (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 physical counselling meetings, we must write minutes of the meetings. Such documentation is retained for at least 5 years in order to document the investment services we provide.

Audio recording 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 reports of lost cards, we make audio recordings when a lost card 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 opportunity to opt out of being recorded.
You can request access to audio recordings by contacting the bank. You must specify the time of the call and which phone number it was made from when you request access.
Basis for processing: Legitimate interest, legal obligation.

Marketing of our products and services

We want to provide you with information about products within the product categories where you already have an agreement with the bank and/or the individual institution. In these circumstances, the bank/institution will use personal data such as name, contact details, date of birth and the services or products for which the customer already has an agreement.

Our products are distributed across the following categories:

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

Using personal data, interests and user group profiles, we personalise communication, ads, advice and offers to ensure 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. We will only analyse your transaction data for marketing purposes if you have consented to this.

You may also see ads from us on social media, external news sites and other websites when we buy ad space through various media.

Digital customer service and marketing channels

Websites: Homepage/online bank, News centre, Swap weekends.
Apps: Apps in App store, Apps in Google Play
Social media: Facebook, Instagram, YouTube, Twitter, LinkedIn, Snapchat.
Other channels: email, news media.
If you have opted out of receiving marketing communications in the Reservation Register in Brønnøysund, we will of course respect this.

Basis for processing: Consent, legitimate interest.

We use various social media sites such as Facebook, Instagram, YouTube, Twitter, LinkedIn and Snapchat to make ourselves available to our customers. In these channels, we share useful information and relevant content 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 these terms and conditions.
We also use aggregated information about visits and activity on our social media pages for statistics and analyses. This information cannot be traced back to individuals.

Any information you provide us with via social media, such as reactions and comments on our posts, is not held by us. It is held by the social media site to which our site is linked. You can delete the information about yourself at any time, for example if you delete comments you have posted. Please note that the data will not be deleted if you just unfollow our page.

Basis for processing: Legitimate interest

Analysis and statistics

We use various analytical tools based on what you have consented to. For example, various analytical tools are used to:

- Collect statistics concerning your usage patterns
- Systemise statistics and build segments for relevant content in our digital channels, for example, websites, apps, on social media and via ads.
- Test and present relevant content to you.

We may collect information about you that is used to analyse how you as a customer use Sparebank 1's services in digital channels and in 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

Basis for processing: Consent and 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 improvements and look at the link between customer satisfaction and customer behaviour over time.
Responding to such surveys is voluntary.

Basis for processing: Legitimate interest

Risk classification of customers and credit portfolios

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

The calculations are conducted using our own models, work processes, decision-making processes, control mechanisms and internal guidelines. This applies to the classification and quantification of credit risk and other risks. In other words, the risk associated with credit and other financial factors is assessed. In conjunction with this, personal data may be collected from credit information agencies. Information may also be collected from the Norwegian Debt Register to develop risk assessment models and to draw up individual credit policy rules.

The Financial Institutions Act, Securities Trading Act and CRR/CRD IV Regulations require companies in the Group to exchange customer information in order to fulfil the institution's governance, control and reporting requirements. This particularly applies to information regarding defaults on commitments.

Basis for processing: Legal obligation

Preventing and detecting 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 gains derived from criminal acts or in conjunction with terrorist financing. This is done because we are required to investigate and report suspicious transactions under the Anti-Money Laundering Act, as well as to verify the identities of all of our customers.

The Anti-Money Laundering Act requires us to report suspicious information and transactions to the Financial Intelligence Unit (EFE) of the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim). The information will be collected from, and may be disclosed to, other banks and financial companies, the police and other public authorities.

Basis for processing: Legal obligation, legitimate interest

Security

We always strive to ensure that your personal data is secure. This is done through access management, logging, encryption, firewalls, access control and camera surveillance, as well as other measures that safeguard your security and the security of SpareBank 1. We have a management system for information security, nonconformance management and training.

Camera surveillance

SpareBank 1 has installed camera surveillance for our premises and 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 the online and mobile banks is logged in order to trace what changes have been made and by whom in case of, for example, a system error or a breach of security. Corresponding logging takes place in our internal systems where we process your personal data. In order to identify or prevent potential undesired activities in or in relation to the bank, Sparebank 1 has a legitimate interest in logging this traffic. Such logging takes place to the extent that is strictly required and proportionate to ensure good information security.
With a few simple steps, you can also increase the security of your own personal data. Read more about Secure online and mobile banking, Safeguarding your cards and 10 tips for preventing ID theft.

Basis for processing: Agreement, legal obligation, legitimate interest

Online and mobile bank login

When you use Sparebank 1's digital services, we can identify the computer or mobile device you use to perform the banking service, record user behaviour and the user environment, the state of the computer/device, etc. Sparebank 1 will use this information to verify that the right person is using the 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 does not store or process biometric information such as fingerprint and facial recognition data on your phone if you choose to use this to log in to our services. This information is only stored locally on your mobile phone and will not be sent to Sparebank 1. The biometric data on your phone is processed by the manufacturers (Apple, Google, Huawei, Samsung, etc.). For further information on the use and storage of biometric data, please refer to the manufacturer's privacy policy. It is up to you as the customer to choose the login solution (PIN code or biometrics) you want to use.

Basis for processing: Agreement, legal obligation, legitimate interest

Testing and development purposes

We are always striving to improve and enhance our systems, services and products. We depend on being able to use data for testing and development purposes in order to safeguard personal data security and ensure that our solutions work properly. The general rule is that fictitious or anonymised data must be used, although sometimes we need to use real customer data to ensure functionality and security.

Basis for processing: We rely on developing and testing new solutions before they are put into production in order to ensure our customers are offered good solutions. In our opinion, such processing is very close to our original purpose of delivering products and services to our customers. We have documented this via a so-called compatibility assessment.

Corporate governance, reporting and analysis

We also use personal data to ensure that the bank is well managed and to gain insights into customers. Information about your customer relationship will therefore be included as part of the basis for managing and supervising the bank. Furthermore, we use personal data to organise ourselves according to our customers' needs and expectations, as well as to provide a basis for making decisions on new customer concepts, delivery models, organisational changes and adjustments to capacity or competence.

Basis for processing: The basis for processing is a compatibility assessment, as the processing is very close to our original purpose of delivering products and services to our customers.

Statistics

We also process personal data to produce statistics for our own purposes and to share with public and private organisations. The statistics will be aggregated data that cannot be linked to you as a person. For example, the statistics will be based on demographic information, product information and transaction information. Both we

and public and private organisations can only use the statistics to improve goods, services, communication and services for consumers.

Examples of statistics include the most popular time of day for people to visit grocery stores, how many customers live in a detached house, sustainability reporting or what average citizens in a municipality pay for electricity, phone subscriptions, food consumption, etc.

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 execute 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 programs 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 execute an agreement with you.
- You have consented to it.

We will inform you if a decision was an automated decision. You can also request that an automated decision be reviewed by a case officer, request an explanation of the decision made or contest the decision.

Basis for processing: Legitimate interest

Profiling

Profiling is a form of automated processing of your personal data. We use profiling and data modelling, among other things, to provide you with specific services and products that are in line with 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 institutions in the SpareBank 1 Alliance. Before sharing personal data, we always ensure that we follow 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. The duty of confidentiality also applies between the companies within SpareBank 1. There are some exemptions where the companies in SpareBank 1 may in some circumstances share some personal data with each other where this is allowed. 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.

A typical case where information will be shared is, for example, between your bank and SpareBank 1 Forsikring to see whether you need any of the products or services that can be delivered. Information about customers will never be shared between the banks in the Alliance.

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. You will find the consent options in your online and mobile banks.

To public authorities

In many cases, SpareBank 1 is required by law to disclose personal data to public authorities. Examples of these include disclosing information to tax authorities, the Norwegian Labour and Welfare Administration (NAV), the courts, the police,

supervisory authorities, Økokrim and public committees. Registered personal data will only be disclosed to public authorities and other third parties when this is required by statutory disclosure obligations or disclosure rights.

To private organisations

If we are permitted to do so by law, personal data may be disclosed to other banks, insurance companies, financial companies and partners. One example where this might happen could be if you want to see your account information in another bank, or if you want to see your insurance from Fremtind in your mobile bank.

For 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 CRS (Common Reporting Standard) and The Foreign Account Tax Compliance Act (FACTA). Under the agreement, Norwegian financial companies are required to identify and report persons, companies and other entities that reside or are domiciled abroad to the Norwegian tax authorities. You can get more information about CRS and FATCA from the Norwegian Tax Administration.

Use of data processors

SpareBank 1 uses third parties to deliver services to you as a customer. If these third parties process your personal data, they will be our data processors.

SpareBank 1 enters into data processing agreements with all providers that process personal data on our behalf. Such agreements regulate how a data processor can use personal data to which it gains access. SpareBank 1 will only use data processors that guarantee they will comply with the Norwegian Personal Data Act and GDPR. SpareBank 1 currently uses various types of data processors, for example:

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

Transfers out of the EU/EEA

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

- 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 corresponding 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 information?

We retain your personal data for as long as necessary for the purposes for which they were collected and processed, unless statutes or regulations require us to store them longer.

For as long as necessary

As a rule, we retain your personal data for as long as 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, they are deleted or anonymised.

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

Examples of retention times

- Offer of product or service: up to 6 months after you received the offer
- Documentation collected and produced in order to prevent and detect money laundering and terrorist financing: 10 years after completion of the transaction or the end of the customer relationship
- Information we are required to keep under the Bookkeeping Act and bookkeeping regulations: up to 10 years
- Audio recordings of investment services: at least 5 years, and if deemed necessary up to 13 years
- Data collected for calculating capital requirements for credit risk: up to 50 years
- Documentation and history related to the performance of an agreement with you: up to 13 years after the end of customer relationship (this corresponds to the period during which you may, on a specific terms, make claims against us under your agreement, so-called period of limitation)
- Information collected from you in conjunction with a conversation about blocking cards or the need for emergency capital in the event of a stolen wallet: 3 years

Log backup: retained for as long as appropriate for the individual service

How we use cookies

It is important to us that you feel secure when you visit our website, and at the same time 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 pieces of data that are stored on your computer or your mobile phone by the browser or app you are using. A cookie belongs to a specific 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 (such as mobile or PC) you are using. When logging in to your online or mobile bank, you can choose to allow the answer from the device to apply to you as a customer as well.

You can choose which categories of cookies we can use.

Read more about our use of cookies here.

Cookies, pixels and scripts used by us

Technical cookies

For the websites to work, we must use technical cookies. These, therefore, cannot be turned off.

Functional cookies

We use functional cookies so that you do not have to go through the same choices every time you are on our websites. They store information about your use of the website and the settings you have selected.

Cookies that archive statistics

We use cookies that store statistics to make our websites better and simpler 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 present you with more relevant and targeted marketing, including from 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 give you 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 violating privacy rules or you are unhappy with how your enquiry was 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 data protection officer at the bank or institution..

Complaints to the Norwegian Data Protection Authority

You also have the right to lodge complaints with the Norwegian Data Protection Authority. Information about this can be found 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

The following provides an overview of changes made to the privacy policy.

Change	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.	27 March 2023
Necessary adjustments and clarifications in line with the development of our services, products and websites, and in line with legal developments.	28 August 2023
Adjustments to wording, changes to the layout of information, and addition of individual purposes and areas of use for personal data in line with business development.	16 May 2024