Privacy policy

Updated 8 March 2021.

How we safeguard your privacy

At SpareBank 1, we take your privacy seriously, and we are continually working to ensure that your personal data are secure with us. You can find further information about how we process your personal data in this privacy policy.

Terms

By "you" we mean you as a customer, potential customer, employee of one of our customers or other users of our services. When we write "SpareBank 1" or "we", we mean banks and enterprises in SpareBank 1.

Data controller

SpareBank 1 and/or the enterprises in SpareBank 1 with whom you have a customer relationship are responsible for processing your personal data. If you need to get in touch with us about data protection, you can send an email to our Data Protection Officer.

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 enterprises 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, citizenship, other identification numbers issued by the government and a copy of ID.
- Contact details such as phone number, address and email address.
- Financial information such as customer agreements and product agreements, credit history, revenue information, payment card number and transaction data.
- Information to meet regulatory obligations such as tax country, foreign tax registration number, information in connection with financial advice, information related to money laundering work and reporting to public authorities.
- Specific categories of personal data such as health information and trade-union membership.
- Information on income, debt, place of work and employment, education, marital status, family relations and dependent responsibilities.
- Photos and video recordings that we take in connection with our customer and sponsorship events.

Where do we collect your personal data from?

From you

The personal data that we collect about you will generally come from you as our customer. For example, as a new customer, we ask you for personal information such as your name, national identity number, contact details and income and debt information. We do this to enable us to provide you with products and services. We also collect other information that you provide to us, such as in conjunction with processing a loan application, feedback in digital channels and chat conversations.

For security reasons, we have cameras in our branches and at our ATMs.

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 may include:

- Identity information, family relations, demographic information and security interest information from the National Population Register (Folkeregisteret), the National Property Register (Eiendomsregisteret) or the Register of Motor Vehicles (Motorvognregisteret). For example, from the Register of Motor Vehicles, we collect information about the vehicles you own. When you apply for a loan as a customer, we collect credit information about you from the debt registers and the credit reference agency Bisnode.
- In the execution of 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 control under the money laundering and financial agreement regulations, we collect information from other public authorities such as the tax authorities, Brønnøysund Register Centre (Brønnøysundregistrene) and the police. In addition, we collect information from sanction lists published by Norwegian authorities and international organizations 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, the bank is required by law to collect information about the key persons and rightful owners of the company. The information is collected from the Brønnøysund Register Centre (Brønnøysundregistrene) and commercial information services that provide information about matters that include rightful owners and politically exposed persons.
- If you establish and manage your own pension account, we collect information about your pension capital certificates from the Pension Account Register (Pensjonskontoregisteret).
- If you agree to it, your bank, in line with the payment services directive, may exchange account and transaction information with other banks or concession-only companies. This means, for example, that you can view accounts from DNB or Sbanken in our mobile bank and vice versa, and that you make payments from these.
- With your consent, Sparebank 1 may collect your account and transaction information from accounts in other banks.

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.

Mobile applications and accesses

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 accesses the apps request in the various apps.

Our apps in the App store
Our apps in Google Play

About biometrics

Sparebank 1 does not store or process biometric information about you. Your biometric data is only stored locally on your mobile phone and will not be sent to Sparebank 1. Processing your biometric data on your phone is handled by the manufacturers (Apple, Google, Huawai, Samsung, etc.). Please refer to their privacy policies for further information about the use of biometric data to identify the computer or mobile device that you use to access our online services.

It is up to you as a customer to choose the authentication solution (pin code or biometrics) that you want to use.

We inform you

You will be informed if we collect personal information about you, unless collection is stipulated by law, notification is impossible or disproportionately difficult, or if we think you already know the information the notice will contain.

Legal basis for the use of your personal data

We will always ensure that we have a basis for processing – a legal justification – when we use your personal data. In SpareBank 1 we apply four bases for processing.

Necessary to fulfil an agreement with you

The main reasons for processing your personal data are customer management, financial advice, billing and implementation of banking, insurance and financial services in line with the agreements we have entered into with you. In the event we wish to enter into new agreements with you, you will always be made aware of the terms of such an agreement.

Consent

In some cases, we will ask for your consent to process personal data. Consent given by you as a customer 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. health information).

Once you have provided consent to Sparebank 1, you may withdraw it at any time. For example, consent to receive marketing notices can be revoked by turning it off in your mobile bank or web bank. If you withdraw your consent, the processing will cease and the personal data will be deleted, since retention of the data is contingent solely on your consent.

Legal requirements

We also process your personal data to fulfil our obligations in compliance with statutes, regulations or governmental decisions.

Examples of processing based on legal requirements:

- Prevention and disclosure of criminal acts such as money laundering, financing terrorism 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, collateral security, insurance or home loan mortgages

Legitimate interest

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

Examples of basing our processing on legitimate interest:

- SpareBank 1 may, among other things, have a legitimate interest in using personal data for marketing, product and customer analyses. The analyses create the basis for marketing, process, business and system development. The purpose is to improve our solutions and provide the best possible offers, products and services to our customers.
- We have a legitimate interest in using profiling, such as conducting customer analysis for marketing purposes or monitoring transactions to detect fraud and other criminal acts.
- Transaction classification of your expenses and earnings in categories to give you a better overview and understanding of your private finances.
- Automatic transfer to your SpareBank 1 bank when you log into your mobile bank, so you avoid disclosing your bank affiliation every time you log in.
- Identify your subscriptions or other overhead expenses that we can assist you in terminating.
- In connection with infection tracking, SpareBank 1 has a legitimate interest in storing your contact information when you visit our offices. The purpose is to be able to deliver relevant data from the register in accordance with infection control legislation.

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.

In certain cases, we may also conclude that we have the option to process personal data for a new purpose, but one that is so close to the original purpose of the processing of personal data that these purposes are compatible. In such a case, we will have documented this in a so-called compatibility assessment.

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.

Customer management

We will process your personal data to fulfil the obligations we have undertaken for the execution of assignments and service agreements made with you. In order to send you invoices, execute payment transactions on your accounts and respond to inquiries from you, in addition to meeting any requirements you may have with SpareBank 1, we will need to process your personal data.

Basis for processing

The basis for processing is primarily the agreement with you, including administrating your customer relationship and storing documentation and history that shows we have fulfilled our obligations to you and to various supervisory and regulatory authorities.

Customer service and 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 product company. The bank/product company will use neutral personal data such as your name, contact details, date of birth and the services or products the customer has already contracted.

Our products are distributed across the following categories:

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

General insurance and personal insurance policies are provided by Fremtind Forsikring.

Read more about Fremtind's processing of personal data. In addition, SpareBank 1 has a collaborative agreement with LOfavør AS to offer certain benefits to members of associations that are part of the Norwegian Federation of Trade Unions, which is also a customer of SpareBank 1.

The various financial companies in SpareBank 1 have a right to mutually share certain information about you, including your name, contact information, date of birth and the services or products that you have contracted. SpareBank 1 Markets is subject to special confidentiality provisions that entail limitations on the disclosure of personal data between banks, corporations and product companies.

With the aid of personal data, interest and user group profiles, we adapt 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. Analytics for marketing purposes that include transaction data will only be extracted if you have expressly consented to this.

Digital customer service and marketing channels:

- Web pages: Home page/online banking, News Centre, Exchange Weekend
- Apps: Apps in App store, Apps i Google Play
- Social media: Facebook, Instagram, YouTube, Twitter, LinkedIn, Snapchat
- Other channels: Newsletters, email and customer surveys

Social media and responsibility for processing

For social media sites, such as our Facebook page, we may share the responsibility for processing with the social medium provider (limited to the data we have control over or access to). We encourage you to read the privacy information concerning the use of information about you.

We process information about your activities on our Facebook page, including when you visit it, publish content on it (e.g. text, images and videos) and respond to our own content or that of others (e.g. likes and comments). We use this to manage the page. The legal basis for our use of information for this purpose is our legitimate interest in making available our content on social media and in communicating with you. Remember that you should never provide personal information, whether on our wall, in posts or in the chat function.

We also manage aggregated information about visits and activity on our social media pages for statistical and analytical purposes. This is not personal data, because we cannot link it to individuals.

We do not store this information ourselves, but we do have access to it as long as we maintain the particular social media site. You can delete information about yourself at any time, e.g. by removing any content or responses you have published. Please note that your information will not be deleted simply because you stop following our site.

Ad purchases

You may experience seeing ads from us on social media and websites when we buy ad space through various media. The information is encrypted so that personal data is protected and the information is used only to place the advertisement.

Facebook Pixel

By using Facebook image pixel on SpareBank 1's website, we can deliver customised content from SpareBank 1 into 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 are to 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 customised 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 customised 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.

- Customer match services from Facebook and Google
  We may show interest-based ads to you when you use Facebook or Google through the Facebook Custom Audience and Google Customer Match services. Facebook Custom Audience enables us to customise our ads based on the information we have about you. When these services are used, your email address or phone number is linked up to what is registered on your user ID by the social media provider. In this way, we can advertise more relevantly than by a standard ad. We won't share any of your personal information with Facebook, and your email address or phone number will be deleted at the moment the information is incorporated in the ad purchase.

The following is an overview of how you can make changes (Norwegian articles):

- Change ads settings on Facebook
- How to opt out of ads on Facebook (applies to all advertisers)
- How to turn off custom ads from Google
- See how to manage cookies
- Reserve against direct marketing under the right to protest

Basis for processing

SpareBank 1 may process personal data for marketing purposes if is necessary to safeguard a legitimate interest that outweighs your privacy considerations. For marketing of products and services within a different product category than those you and the bank have entered into an agreement on, your consent is required to use customer information other than your name, contact information and the products you have. You may at any time opt out of receiving such information. Without your consent, we will not be able to provide you with equally relevant advice and offers.

The consents can be found in mobile banking and online banking. You may at any time change your consents.

If you have reserved against marketing in the Central Marketing Exclusion Register (Reservasjonsregisteret) in Brønnøysund, we will of course respect this decision.

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. In addition, we can 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 may opt out of responding to the survey we send you.

Basis for processing
The processing is based on SpareBank 1's legitimate interest in getting information about how our customers perceive us and what opinions our customers have about our products, services and customer service.

Product development and analyses

Sparebank 1 may collect information about you that is used for analysis of how you as a customer use Sparebank 1's services on digital surfaces 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

We use Google Analytics and Adobe Analytics for traffic analysis on our websites.

You can read more about our use of cookies.

Basis for processing
SpareBank 1 has a legitimate interest in conducting market and customer analyses to develop new and existing products and services, and to provide good customer service.

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.

In accordance with the rules of the Financial Services Act, the Securities Trading Act and the CRR/CRD IV Regulations, we will process credit information, application information and other information about you for calculating capital requirements for credit risk. Such processing is also carried out in connection with the establishment of your customer relationship and when ascertaining the services and products that are suitable for you.

Calculations are made with 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 conjunction with this, personal data may be collected from credit rating agencies. For the development of models for risk assessment and for the preparation of individual credit policy rules, information from the Norwegian national debt registry can also be collected.

Rules laid down in the Financial Enterprises Act, the Securities Trading Act and the CRR/CRD IV Regulations entail that companies must exchange customer information in order to meet the company's requirements for governance, control and reporting. In particular, this applies to information related to the breach of engagement.

Basis for processing
Personal data is processed to fulfil our legal obligations under the Financial Enterprises Act, the Securities Trading Act and the CRR/CRD IV Regulations.

Fulfilment of legal requirements

We will process personal data when necessary in order to comply with laws, regulations and government decisions. See more about this under «Legal obligations» and «Prevention and detection of criminal acts».

Basis for processing
Processing is necessary in order for SpareBank 1 to fulfil its 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.

In addition, we will process personal data to prevent and detect transactions related to gains derived from criminal acts or in conjunction with financing terrorism. We do this because we are required to investigate and report suspicious transactions under the Norwegian Anti Money Laundering Act, as well as to carry out credential checks on all our customers.

Under the Norwegian 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 collected from, and may be disclosed to, other banks and financial institutions, the police and other public authorities.

Basis for processing
Processing of personal data is necessary in order for SpareBank 1 to fulfil its legal obligations. In addition, we have a legitimate interest in developing good models and tools to meet these obligations. We also have a legitimate interest in preventing, detecting, clearing up and dealing with fraud and other criminal acts against you, other customers or us.

Security

SpareBank 1 implements technical and organisational security measures to safeguard your personal data. SpareBank 1 is continually working 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 camera monitoring, as well as other measures that support the security of SpareBank 1. Key measures are a separate management system for information security, access control, nonconformance management and training.

Logging

Your activity in online banking or similar platforms is logged in order to trace changes that have been made and by whom, for example, where there is an error in the systems or a breach of security occurs. In order to identify or prevent potential undesired acts against the websites, Sparebank 1 has a legitimate interest in logging traffic over the website. Such logging takes place to an extent that is strictly necessary and proportionate to ensure online and information security.

In a few simple steps, you can also enhance the security of your own personal data.

Read about Secure Online Banking and Mobile Banking, How to safeguard your card and 10 tips to prevent ID theft (Norwegian articles).

Basis for processing
Personal data is processed in order to fulfil our contractual obligations with you, the legal obligations we have, and our legitimate interest in safeguarding your and our assets and interests.

Image capturing via CCTV surveillance

SpareBank 1 uses CCTV surveillance to prevent and detect criminal acts. We have CCTV surveillance and make video recordings of our banking 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
Personal data is processed based on our legitimate interest in safeguarding both your and our assets and interests. If we turn over video-recorded footage to the police, we do this on the basis of a legal obligation.

Audio recording of phone calls

When we provide investment services, we are required by law to make audio recordings and store calls, meetings and other customer communications. In physical counselling meetings, we must write minutes of the meetings. Such documentation is kept for at least five years to document the investment services we provide.

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 saved 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. Such recordings are also justified by the bank's legitimate interest.

You can request access to audio recordings by contacting the bank. When you make your request, you must specify the time when the call was made and from what phone number.

Basis for processing
Processing of personal data by sound recording is done in order for SpareBank 1 to fulfil its legal obligations, and is based on the bank's legitimate interest.

Chat

If you start a chat when you are logged in to your online banking, 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 contact with the bank later on, and as documentation in the event a dispute should arise.

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 use in statistics and evaluation of customer service, but it cannot be linked to you as a customer. If you during the chat choose to talk to an adviser, the chat conversation will be made available to this adviser. The purpose is to give that person an opportunity to familiarize themselves with your inquiry before the chat continues. Chats are stored for one year.

Basis for processing
Personal data is processed based on our legitimate interest in following up on you as a customer and documenting our contact with you.

Customer authentication when using online services

When you use Sparebank 1's online services, we may record user behaviour and user environment, identify the computer or mobile device you use to execute the banking service, the state of your computer/device, etc. Sparebank 1 will use this information to verify that it is the right person using the relevant service. The processing of your personal data when you use BankID is described in the terms and conditions for BankID. Sparebank 1 may also use the information in a risk assessment to adapt the authentication method that you will use for the service.

Basis for processing
Personal data is processed in order to fulfil our contractual obligations with you and the legal obligations that SpareBank 1 has, in addition to our legitimate interest in conducting a risk assessment and adaptation of the authentication method that you will use for the service.

Testing and development purposes

SpareBank 1 continually works to improve our systems, services and products. In order to maintain personal data security and ensure that our solutions work properly, we depend on being able to use data for testing and development purposes. The main rule is that only fictitious or anonymised data are to be used, but sometimes we rely on using real customer data to ensure functionality and security. When this is the case, the customer data will be masked, and we will conduct a risk assessment and severely restrict access to the data.

Masking entails making it more difficult to identify individuals. For example, names and/or national identity numbers can be replaced with a code, some data fields can be replaced with fictitious information, or content in data fields can be removed altogether.

Basis for processing
The processing of personal data for testing and development purposes is deemed consistent with the original purpose of fulfilling the obligations we have undertaken for carrying out assignments and complying with service agreements we have with you, as well as ensuring that our systems operate reliably and securely.

Statistics for public and private enterprises

At Sparebank 1, we process personal data to provide statistics to public and private enterprises. The statistics we share with these businesses will be aggregated data that cannot be associated with you as an individual person (anonymized). For example, the statistics will be based on demographic information, product information and transaction information. Businesses can only use the statistics to improve goods, services, communication and services to consumers.

Examples of statistics may include the time of day when most people are in the grocery store, how many customers live in a detached house or what average citizens in a municipality pay for electricity, telephone subscriptions, food consumption, etc.

Basis for processing
The processing of personal data to create statistics for public and private enterprises is based on legitimate interest.

Joint processing responsibilities

Sometimes we share responsibility for processing your personal data. This applies, among other things, in the cases where companies in the SpareBank 1 alliance work together to develop common machine learning models that can be used in online banking and mobile banking to give you as a customer better insight into your own finances, and when companies in the SpareBank 1 alliance and BN-bank work together to develop common machine learning models for banks' legally mandated anti-money laundering efforts. In both cases, we use what is called pseudonymised information on a selected sample of our customers. When banks collaborate on the development of such machine learning models, you have a basic right to protest.

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 ensure our legitimate interests. 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. However, the following information may be shared internally between companies in consolidated financial enterprises:

- 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 give your consent that the enterprises in SpareBank 1 may share more information about you. The consents can be found in your mobile banking and online banking.

We will also provide personal data to companies in the banking group or concern when this is necessary to satisfy group-level management, control and/or reporting requirements laid down in or pursuant to the law.

To public authorities

In various circumstances, SpareBank 1 is required to disclose personal data to public authorities. Examples of this may include disclosure to tax authorities, NAV, the courts, the police, supervisory authorities and public committees. Registered personal data will be disclosed to public authorities and other third parties only when required by statutory disclosure obligations or access rights.

To private enterprises

Pursuant to the law, personal data may be provided to other banks, insurance companies, financial enterprises and partners. An example of this might be that you want to view your account information in a different bank. Another example is the execution of payment orders for you, where the recipient's bank and other parties involved in the payment order will see who has paid.

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 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 data processors

By disclosure of personal data, we mean transfer to other entities that have the right to use the information. Transfer of personal information to our data processors is not considered disclosure.

SpareBank 1 enters into data processing agreements with all companies that process personal data on our behalf, such as a provider of ICT services. The agreement governs how the data processor can use the personal data shared with the service provider.

SpareBank 1 will only use data processors that guarantee they will comply with the Norwegian Personal Data Act and GDPR. This means that they may not use information for purposes other than those agreed in the data processing agreement.

SpareBank 1 primarily wishes to use data 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 well safeguarded:

- There is an approved basis of transfer for the transfer of personal data to a third country, such as the use of standard contracts (EU Standard Contractual 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 corresponds to the level of protection in the EU/EEA, as a result of given technical and/or organizational measures.

Your rights

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

Right of access

You have the right to request access to the personal data we process about you, and you have the right to get a copy of this information. In addition, you 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 banking. 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. If you do not have online banking or cannot read electronic documents for some other reason, we can send you the information on paper.

In certain cases, there are exceptions to the right of access. This is typically 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.

If you are an employee, former employee or have applied for a position in SpareBank 1 and would like to order information related to this, please contact the HR department of your employer or former employer in SpareBank 1. The same applies if you have otherwise been engaged by SpareBank 1 to perform work.

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 (Folkeregisteret) 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 have 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 processing of personal data applies to minors if the data was collected in connection with providing information society services.

Right to limited processing

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

- You believe that the personal data are 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 balancing 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.

For further terms and conditions and information on restricting personal data, send an email to our Data Protection Officer.

Protecting your personal data

If you have a specific need for us to restrict the number of employees who have access to, and knowledge of, your personal information, we may consider whether you have a right to have your data shielded. Shielding your information substantially reduces our ability to follow up on you as a customer and to give you the customer experience that we would like to offer.

For further terms and conditions and information on shielding personal data, send an email to our Data Protection Officer.

Have your data delivered in machine-readable format (data portability)

You have the right to obtain a copy of personal data that you have given us in a machine-readable format. Contrary to the right of access, this right applies only to personal data that you yourself have provided to us and that are processed based on 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 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 protest

You have the right to require that SpareBank 1 no longer process personal data about you if the processing is based on legitimate interests, unless there are reasons that take priority over your interests or serve to establish, enforce or defend legal requirements. You may also demand that SpareBank 1 stop using your personal data for direct marketing sent to you, including profiling related to such purpose.

If you wish to opt out of direct marketing, please contact Customer Service.

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.

You will get information from us if we use automated decision-making. In addition, you can request to have the automated decision reviewed by a case worker, request an explanation of the decision made or contest the decision.

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.

How you can exercise your rights

If you wish to exercise your rights, please send an email to our Data Protection Officer.

Email is considered an insecure channel, so we advise you not to 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.

Even after you have given us your consent that we may use information about you, you can change this at any time in your mobile banking or online banking.

You can also contact us to change your consent.

How long do we store your personal information?

We store 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. After that, they are deleted or anonymized.

As long as necessary

This means that as a general 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. At all times, we will restrict access to your personal data based on who is in need of such access.

In cases where 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 storage times

- Offer: up to 6 months after the customer received the offer
- Documentation obtained and prepared to prevent and detect money laundering and terrorist financing: 5 years after completed transaction or terminated customer relationship
- Information we are required to keep under the Bookkeeping Act and bookkeeping regulations: up to 10 years
- Audio recording of investment services: at least 5 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 control.)
- 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, 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: Stored as long as appropriate for the individual service (The backup logs are kept separate with strict access control.)

How we use cookies and analysis tools

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.

Web analysis tools and statistics make us better

SpareBank 1's website makes use of cookies. These are small pieces of data that are stored on your computer or your mobile phone by the browser you are using. A cookie belongs to a particular website and cannot be read by other websites. In addition to cookies, we use pixels and scripts from third parties.

We use cookies on our websites to ensure that:

- The websites function technically.
- The websites can be customized to your use, your choices and your settings.
- We may collect statistics on how our websites are used and thus improve our services.
- We may provide you with personalized content and relevant ads, including through our partners, on websites and social media, for example.

You can turn the cookies on and off yourself, except the technical ones. The latter must be turned on for our website to work.

Turn cookies on and off

The tools we use

We use Adobe Analytics to collect information.

We use Adobe Audience Manager to collect and systematize data that we use to provide you with relevant content in our channels, such as websites, apps, social media, and ads.

We use Adobe Target, a testing and measurement tool, to analyze and view the content, offers, and other communications that are most interesting to you.

Cookies, pixels and scripts we use

Technical cookies

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

Functional cookies

In order to avoid having to make the same choices every time you are on our websites, we use functional cookies. They store information about your use of the websites and what settings you have selected so that you can have functionality adapted to you.

Cookies that archive statistics

To make the web pages better and easier, we use cookies that store statistics. 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 enables us to provide you with more relevant and customized marketing, including through our partners, such as websites, ads and social media.

Cookie overview

Questions and complaints

If you think we are violating the Privacy Policy or you are unhappy with the processing of your inquiry, we encourage you to 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 send an email to our Data Protection Officer.

Complaint to the Norwegian Data Protection Authority

You also have the right to lodge complaints with the Norwegian Data Protection Authority (Datatilsynet). Information about this can be found on the Norwegian Data Protection Authority's web pages.

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 line with the development of our services, products and websites.	8. March 2021