

Privacy Policy



Version	Date	Document owner	Decision	Status
1.0	3 August 2022	Legal department	Group Management	Adopted

Contents

1	BACKGROUND.....	4
2	PURPOSE.....	4
3	TARGET GROUP.....	4
4	FRAMEWORK CONDITIONS.....	4
4.1	Legislation and guidelines.....	4
4.2	Governing documents.....	4
4.3	Commitments.....	4
5	GUIDELINES.....	5
5.1	General.....	5
5.2	The basis for collecting personal data.....	5
5.2.1	Contract.....	5
5.2.2	Consent.....	5
5.2.3	Legal obligation.....	5
5.2.4	Legitimate interest.....	6
5.3	The types of personal data the bank collects.....	6
5.3.1	Primary information.....	6
5.3.2	General information.....	6
5.3.3	Assets, income and liquidity.....	6
5.3.4	Credit scoring and defaults.....	6
5.3.5	Conduct and demography.....	6
5.3.6	Statutory information.....	6
5.4	Sources from which the bank collects personal data.....	6
5.4.1	Information disclosed by customers.....	6
5.4.2	Information received from third parties.....	6
5.4.3	Information that is collected from customers through our digital surfaces, including through the use of cookies.....	7
5.5	The bank uses personal data for.....	7
5.5.1	Customer administration.....	7
5.5.2	Customer follow-up and marketing.....	7
5.5.3	Statistics, analysis of service use, error correction and further development of services.....	7
5.5.4	Risk classification of customers and credit portfolios.....	8
5.5.5	Customer verification (customer identification) when using electronic services.....	8
5.5.6	Use of push notifications.....	8
5.5.7	Preventing and detecting criminal acts.....	8
5.5.8	Recording telephone conversations.....	8
5.5.9	Video surveillance.....	9
5.6	Disclosure of personal data.....	9
5.6.1	Internally in Sparebanken Sør.....	9
5.6.2	To government authorities.....	9
5.6.3	Banks and financial institutions.....	9
5.6.4	Transfer of personal data abroad.....	9
5.6.5	Use of data processors.....	10
5.7	Customers' right of access.....	10
5.7.1	Right of access.....	10
5.7.2	Right to rectification.....	10
5.7.3	Right to deletion.....	10
5.7.4	Right to restrict processing.....	10
5.7.5	The right to receive personal data in machine-readable format.....	10
5.7.6	Right of objection.....	11

5.7.7	Automated decision-making	11
5.7.8	How to exercise your rights	11
5.8	How long does the bank store personal data?	11
5.8.1	As long as is necessary.....	11
5.8.2	Examples of storage periods	11
5.9	Questions and complaints	12
5.9.1	Contact details.....	12
5.9.2	Complaints about our processing.....	12
6	KPIs.....	12
7	RESPONSIBILITY, MANAGEMENT, FOLLOW-UP AND REPORTING	12

1 BACKGROUND

Sparebanken Sør's mission is to "Create sustainable growth and development for our region".

Our work on sustainability (ESG – Environmental, Social and Governance), which encompasses the climate and the natural environment, social conditions and corporate governance, is a natural continuation of the role the bank has played for almost 200 years. For Sparebanken Sør, sustainable development means that the bank should contribute to positive development within ESG, while safeguarding the bank's social responsibility in areas where the bank operates. Our work on sustainability is intended to strengthen our competitiveness and reduce the bank's ESG risk. As an employer, investor, lender and supplier of financial products and services, the bank should contribute to sustainable growth and development by strengthening the positive effects and reducing the negative impacts on people, society, the climate and the natural environment.

The bank relies on trust from its customers, public authorities and other stakeholders, and safe management of customer data and other information is therefore crucial for the bank. Sparebanken Sør processes personal data in accordance with applicable laws and procedures, and requires our suppliers and partners to do the same.

2 PURPOSE

The purpose of this policy is to protect individuals' privacy from being violated through the processing of personal data.

The policy is further intended to ensure that the bank has clear principles and guidelines that highlight the requirements and expectations the bank makes of our own activities, our customers, suppliers and partners around privacy.

3 TARGET GROUP

The target group for this policy is the Sparebanken Sør Group and the bank's customers, suppliers and partners.

4 FRAMEWORK CONDITIONS

4.1 Legislation and guidelines

Sparebanken Sør undertakes to comply with all legislation that is relevant to the bank's activities. We also attach importance to ensuring that the companies the bank is involved with conduct their activities in line with the bank's policies and relevant legislation.

The following laws and conventions are relevant:

- The Norwegian Personal Data Act including the General Data Protection Regulation (GDPR)

4.2 Governing documents

- Sustainability strategy
- Processing of personal data

4.3 Commitments

Sparebanken Sør undertakes to process personal data in accordance with the Norwegian Personal Data Act.

Sparebanken Sør is a member of a number of national and global organisations that work to promote sustainable development. We also expect our customers, suppliers and partners to prioritise these organisations' goals and principles in their commercial conduct.

UN Global Compact

Sparebanken Sør has endorsed the UN Global Compact. The Global Compact is the world's largest initiative for work on sustainability and corporate social responsibility. The bank submitted its first Communication on Progress report (CoP) in Q1 of 2019.

UNEP Principles for Responsible Banking (PRB)

The UN Principles for Responsible Banking are a guide that describes responsibilities and ambitions for actions to meet sustainable development goals and the targets of the Paris Agreement. Sparebanken Sør is a signatory to UNEP PRB.

The UN Sustainable Development Goals

The UN Sustainable Development goals, which were adopted in 2015, represent a global plan to eradicate poverty, combat inequality and stop climate change. The plan consists of 17 goals, which are referred to as the world's common blueprint for sustainable development. Sparebanken Sør supports all 17 of the sustainable development goals.

5 GUIDELINES

5.1 General

The bank processes personal data in accordance with the Norwegian Personal Data Act, including the General Data Protection Regulation (GDPR), industry standards and internal procedures.

5.2 The basis for collecting personal data

5.2.1 Contract

A contractual agreement signed by the customer as data subject. Examples include deposit, lending and payment solution agreements.

5.2.2 Consent

The bank needs permission to use information about the customer relationship to contact customers electronically. This includes providing information about events, useful products and solutions that the bank believes the customer may need. We also need permission to share personal data within the Group and with our business partners.

This consent can be amended or withdrawn via online or mobile banking. Customers who do not have access to online or mobile banking can contact their advisor or Customer Services.

5.2.3 Legal obligation

The bank processes personal data to meet our obligations in accordance with laws, regulations or authority decisions. This could include:

- reporting criminal acts such as money laundering, financing of terrorism or fraud
- reporting to the police or to tax, enforcement or supervisory authorities
- risk classification relating to risk management such as credit development, credit quality and capital adequacy
- requirements and obligations relating to payment services

- other obligations relating to products, securities, funds or home loans

5.2.4 Legitimate interest

The bank may process personal data if this is necessary to safeguard a legitimate interest that outweighs the consideration of the customer's privacy. The legitimate interest must be lawful, defined in advance, genuine and objectively justified.

5.3 The types of personal data the bank collects

5.3.1 Primary information

This information is collected based on contractual agreement or the customer's consent. Examples include names, dates of birth, contact information, social status, relations (children, parents, guardians), gender and citizenship.

5.3.2 General information

This relates to rights and obligations between the bank and the customer. Examples include information about the products and services the customer uses. Such information could also include utilisation details, account numbers, loan terms, maturities and dates of agreements.

5.3.3 Assets, income and liquidity

This includes financial information about customer and product agreements, account numbers, credit history, income information, payment card numbers and transaction data.

5.3.4 Credit scoring and defaults

Information about customers' ability and willingness to pay. This includes information about payment remarks, overdrafts, reminders, credit scoring, defaults, loss write-downs and distraint or seizure of assets.

5.3.5 Conduct and demography

Information about the customer's use of the bank's website, platforms and digital apps such as traffic data, location data and other communication data. We also collect demographic data such as age and location. Our lawful basis for collection is legitimate interest and the purpose is statistics, error correction and improvement of our services.

5.3.6 Statutory information

Information required to meet statutory obligations such as tax domicile, foreign tax registration numbers and information relating to money laundering and reporting to government authorities.

5.4 Sources from which the bank collects personal data

5.4.1 Information disclosed by customers

Personal data the customer discloses to the bank when establishing a customer relationship. This could include names, national identity numbers, contact information and income and debt information. The bank also collects other information in connection with applications for loans and feedback through digital channels.

5.4.2 Information received from third parties

In some cases the bank will obtain customers' personal data from third-party business partners. This could include publicly available sources/databases or private businesses. The bank also obtains information from

the Norwegian National Population Register and the Norwegian National Property Register, as well as credit information from the debt information company Gjeldregisteret AS and credit rating agencies.

5.4.3 Information that is collected from customers through our digital surfaces, including through the use of cookies

In some cases we use cookies to collect information. In accordance with the Norwegian Act relating to Electronic Communications (the Electronic Communications Act), all visitors to websites that use cookies must be able to find out whether the website uses cookies. We collect information from users of our digital surfaces about the use of our services and about demographics.

5.5 The bank uses personal data for

5.5.1 Customer administration

The bank processes customers' personal data to meet the obligations we have undertaken in order to execute assignments and service agreements with the customer. For example, we will process customers' personal data to be able to issue invoices, execute payment transactions on accounts and answer customer enquiries.

5.5.2 Customer follow-up and marketing

The bank may use the customer's name, contact information, date of birth and details of services or products for which an agreement on marketing has been entered into based on legitimate interest.

Sparebanken Sør uses its own channels, email, social media, text messages and external media to disseminate information about products and services. Our aim is for our customers to receive and view content that they perceive as relevant.

We market the bank's own products and services, as well as relevant products from the following companies in which we are co-owners: Frende Forsikring, Brage Finans, Norne Securities, Vipps and Sørmeqleren.

We will occasionally issue emails with relevant offers, advice and the latest news on loans, savings, insurance, property and payment solutions. Customers can easily unsubscribe from the newsletters at any time if they no longer wish to receive them.

Sparebanken Sør also uses the services Custom Audience on Facebook and Customer Match on Google for marketing purposes. The bank has evaluated these technical solutions and is confident that these safeguard our customers' privacy.

Customers can opt out of adapted marketing on:

- Facebook
- Google

5.5.3 Statistics, analysis of service use, error correction and further development of services

We process data collected from use of our services and digital surfaces (for example, online banking, mobile banking and websites) to compile statistics on use and users and in order to analyse use of our services for the purpose of error correction and further development of our services. Our lawful basis for processing is legitimate interest.

5.5.4 Risk classification of customers and credit portfolios

The bank uses personal data to assess risk on the sale of products and services. This assures our customers that we take care of our assets.

In accordance with the provisions of the Norwegian Financial Institutions Act, the Norwegian Securities Trading Act and the Capital Requirements Regulations, the bank processes credit information and other personal data to calculate credit requirements for credit risk. We also process such information in connection with the establishment of customer relationships and to assess which services and products are suitable for the customer.

We perform calculations using dedicated models, work and decision-making processes for granting credit and credit management, control mechanisms, IT systems and internal guidelines relating to classification and quantification of the bank's credit risk and other relevant risk. We may obtain personal data from credit rating agencies to perform the above.

5.5.5 Customer verification (customer identification) when using electronic services

Processing of customers' personal data when using BankID is described in the Terms of Agreement for BankID.

The bank uses the BankID app to verify customers' identities for online and mobile banking. Personal data that is collected for this purpose includes names, dates of birth, photographs to identify you as a customer, expiry dates of ID documents etc. The information is used to update our customer database, verify your identity as the customer submitting the documentation or for a more specific purpose that is described when you are asked to verify your identity. Customers who do not wish to provide identification in this way can visit one of our offices who can then scan their ID. You can learn more about ID checks at [BankID.no](https://www.bankid.no) by clicking [here](#) (opens in a new window).

5.5.6 Use of push notifications

To give customers a good customer experience, the bank sends notifications to its mobile banking customers – for example, notifications of e-invoices for processing. Notifications of e-invoices will include the name of the invoice recipient and amount. Customers can manage this function themselves by activating or deactivating push notifications on their mobile phone. If push activations are activated, notifications will be displayed on the lock screen.

5.5.7 Preventing and detecting criminal acts

The bank will process personal data for the purpose of preventing, detecting, resolving and handling frauds and other criminal acts committed against the bank and other customers.

The bank will also process personal data in order to prevent and identify transactions connected with the proceeds of criminal acts or with the financing of terrorism. We do this because the bank has a duty to investigate and report suspicious transactions in accordance with the Norwegian Anti-Money Laundering Act, and to verify the identity of all our customers.

Under the Act, the bank is required to report suspicious information and transactions to the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) through the Financial Intelligence Unit (FIU). The data will be obtained from and delivered to other banks and financial institutions, the police and other government authorities.

5.5.8 Recording telephone conversations

The bank may only make sound recordings for an expressly stated purpose that has been disclosed and is objectively justified. Sparebanken Sør has a legal obligation to record telephone conversations and to store electronic communication whenever the customer receives advice on investment services; see the

Norwegian Securities Trading Act. The bank records all conversations between customers and brokers and investment advisors who provide these services. Sound recordings of such conversations and documentation of other types of communication with customers are stored for three years. Examples of sound recordings made by the bank:

- recordings involving investment firms
- documentation of the signing of agreements
- recordings made for security purposes where threats have been made
- recordings of conversations for quality-assurance and employee training purposes

5.5.9 Video surveillance

Sparebanken Sør uses video surveillance in its offices, bank premises and cash dispensers in order to prevent and detect criminal acts. Signs indicating that an area is monitored must be displayed close or next to the camera. Such recordings will be deleted three months after the time of recording, unless they are handed over to the police or the bank is entitled to use the recorded image for another purpose.

5.6 Disclosure of personal data

5.6.1 Internally in Sparebanken Sør

The bank has a duty of confidentiality regarding customer data. The duty of confidentiality also applies between other companies in the Group. However, the following information may still be shared internally between Group companies:

- your contact details
- your date of birth
- information regarding where you are a customer, and which services and products you have signed an agreement for

Consent given to the bank by the customer to share information internally is registered in the customer's mobile or online banking. If the customer does not use these services, they should contact their advisor or Customer Services.

The bank will also disclose personal data to companies in the Group if this is necessary to meet group-wide management, control and/or reporting requirements established by or in accordance with law.

5.6.2 To government authorities

Customers' personal data will be disclosed to government authorities, including the Financial Supervisory Authority of Norway, tax authorities and the police, as well as to other third parties as a result of a statutory duty of disclosure or right to inform.

5.6.3 Banks and financial institutions

If permitted by legislation and not precluded by the bank's duty of confidentiality, the bank may also disclose personal data to other banks and financial institutions and partners for use for the stated processing purposes. We may also disclose data to other parties who are involved in a payment transaction, provided this is necessary to execute the transaction in a secure manner.

5.6.4 Transfer of personal data abroad

When executing a payment transaction to or from abroad, related personal data will be disclosed to a foreign bank and/or its auxiliary. The bank may disclose personal data to countries outside the EU/EEA if this is regulated in an agreement between the bank and companies that look after the bank's interests.

5.6.5 Use of data processors

The bank uses data processors to collect, store or otherwise process personal data on our behalf. In such cases the bank will enter into agreements with a data processor to ensure that the data is processed in accordance with the privacy regulations and the bank's requirements for processing personal data. Use of data processors is not deemed to constitute disclosure of personal data.

5.7 Customers' right of access

5.7.1 Right of access

The customer has the right to request access to information regarding which personal data the bank processes, and to receive a copy of this data. The customer also has the right to information about how the bank processes the customer's personal data.

Information about the customer's products, agreements, contact information and transaction history is available in the customer's mobile and online banking. If the customer cannot find relevant information, they can send a written request for such to the bank. The bank may request that the customer details which information or processing activities they wish to access. If the customer does not have access to mobile or online banking, or for any other reason cannot read electronic documents, the bank will send the information on paper.

There are certain exceptions to the right of access. This includes information subject to a statutory duty of confidentiality or information the bank is obliged to keep secret in order to prevent, investigate, identify or prosecute illegal acts. There is also no right of access if the information concerned only exists in documents prepared for internal case handling or is necessary in order to ensure proper case handling.

5.7.2 Right to rectification

It is important to make sure that customers' personal data held by the bank is accurate and up to date. Sparebanken Sør regularly checks data against the Norwegian National Population Register and other sources. If the customer believes that the data is inaccurate or incomplete, the customer has the right to request that this be corrected or updated.

5.7.3 Right to deletion

The customer also has the right to request that the data be deleted if the information is no longer needed for the purpose for which it has been collected or where consent for the processing has been withdrawn. This means that there is no obligation to delete the information if there is still a need to process the information for the intended purpose. This also applies if the bank still requires the information to fulfil a legal obligation or to establish, assert or defend a legal claim.

5.7.4 Right to restrict processing

The customer may request that the bank restrict processing of their personal data if the accuracy or legality is contested or an objection is raised to the processing. The processing will then be limited to storage until the information has been corrected or it can be established that the bank's legitimate interest overrides the customer's interest.

5.7.5 The right to receive personal data in machine-readable format

The customer has the right to receive, in machine-readable format, personal data that the customer has disclosed to the bank if the processing is based on consent or fulfilment of a contract, and this is processed

automatically. The customer may also request that the personal data be sent directly to another Data Controller if this is technically feasible.

5.7.6 Right of objection

The customer may request that Sparebanken Sør cease processing their personal data, unless the bank's interest in the processing outweighs the customer's interests (legitimate interest). The customer may also request that Sparebanken Sør stop using their personal data for personalised marketing, including profiling connected to such a purpose. Customers can opt out of direct marketing in the declaration of consent in their mobile or online banking or by contacting their advisor or Customer Services.

5.7.7 Automated decision-making

If automated decision-making is used, this will be disclosed, together with the underlying reasoning as well as the importance and the expected consequences of such processing for the customer.

Automated decision-making means decisions that are made by computer software without human involvement or influence. If automated decision-making will have legal consequences for the customer or have any other significant impact, the bank may only utilise automated decision-making if:

- it is necessary in order to enter into or execute an agreement with the customer
- the customer has given their consent

One example is fully automatic processing and decision-making regarding applications for credit cards. With the customer's consent, information is collected from Altinn (Norwegian Internet portal for public reporting) and the debt information company Gjeldregisteret AS, and is then processed fully automatically. Based on the results this gives, the decision to approve or reject a credit card application may be taken with no human intervention.

5.7.8 How to exercise your rights

To exercise your rights as customer, you must submit a request to personvern@sor.no, or phone Customer Services on (+47) 38 10 92 00. The bank will respond to your enquiry as soon as possible and within 30 days at the latest.

In order to answer the enquiry, the bank will require you to confirm your identity or disclose further information.

5.8 How long does the bank store personal data?

5.8.1 As long as is necessary

This means that the bank generally stores personal data as long as is necessary to fulfil the agreement between the customer and the bank, or in accordance with the requirements for storage periods established in laws and regulations. The bank will at all times limit access to personal data to personnel who have an official need for such access.

Where storage of your personal data is based exclusively on your consent as a customer, and this consent is withdrawn, the bank will delete the data as soon as possible.

5.8.2 Examples of storage periods

Offers: up to six months after the customer receives the offer.

Documentation that is obtained and prepared to prevent and identify cases of money laundering and the financing of terrorism: five years after the concluded transaction or cessation of the customer relationship.

Information the bank is obliged to store in accordance with the Norwegian Bookkeeping Act and the Norwegian Accounting Regulation: up to ten years.

Sound recordings of investment services: at least five years.

5.9 Questions and complaints

5.9.1 Contact details

The Data Controller for personal data processed by Sparebanken Sør is the CEO, who has delegated day-to-day responsibility to Business Support Director Rolf H. Søraker.

Contact information for Sparebanken Sør:

Address: Rådhusgt. 7/9, 4611 Kristiansand, Norway

Email: personvern@sor.no

Phone: (+47) 38 10 92 00

Organisation number: 937894538

If you have any questions about this privacy policy or Sparebanken Sør's processing of personal data, please email Sparebanken Sør's Data Protection Officer lawyer Frode Mathiesen at personvernombud@sor.no.

5.9.2 Complaints about our processing

If you have any questions or complaints concerning our processing of personal data, please contact us via our website ([submit complaint here](#)).

Any official complaints concerning Sparebanken Sør's processing of personal data should be sent to the Norwegian Data Protection Authority. You can find information about this on www.datatilsynet.no (link opens in a new window).

6 KPIs

The following guidelines have been established covering privacy breaches:

KPI	Description	Unit	Goal	Time
KPI B1	Orders, fines related to privacy by the Norwegian Data Protection Agency	Number	0	Y

7 RESPONSIBILITY, MANAGEMENT, FOLLOW-UP AND REPORTING

Sparebanken Sør presents the way it organises work on personal data in the management document "Processing of personal data".

Sparebanken Sør has drawn up instructions, procedures and guidelines that describe how the bank should follow up, report and ensure compliance with the General Data Protection Regulation.

