Sparebanken Sør's Privacy Policy

Personal data is information that can be linked to you as a private individual. This could be your name, telephone number or an assessment. You have the right to determine how your personal data is used. It is important for us that you know which information we collect and how we safeguard your privacy.

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.

Basis for collecting your personal data

- **Contract**
  The Bank may collect personal data on the basis of a contractual agreement signed by the customer as data subject. Examples include deposit, lending and payment solution agreements.

- **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  This consent can be amended or withdrawn via online or mobile banking.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 account manager or Customer Services.

- **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.

- **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.

The types of personal data the Bank collects

- **Overarching 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.

- **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.

- **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.

- **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.

- **Behaviour**
  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.

- **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.

Sources from which the Bank collects personal data

- **Information disclosed by customers**
  Personal information 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.

- **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.

- **Information collected using 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.

  For more information on our cookies, please visit (link to cookies at sor.no).

The Bank uses personal data for

- **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.

- **Customer follow-up and marketing**
  The Bank may use the customer's name, contact information, date of birth and details of services or products the customer uses for marketing purposes.

  For digital marketing Sparebanken Sør uses the service Custom Audience on Facebook. We use Customer Match for marketing on Google. The Bank has assessed these technical solutions and is confident that these safeguard our customers' privacy.

  The Customer can opt out of adapted marketing at:
  Facebook
  Google

- **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.

- **Customer verification (customer identification) when using electronic services**
  Processing of the customer's personal data when using BankID is described in the Terms of Agreement for BankID.

- **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 activation is activated, notifications will be displayed on the customer's phone.

- **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.

- **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 where the customer receives advice on investment services; see the Norwegian Securities Trading Act. The Bank records all conversations between customers and brokers and investment advisers 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 training purposes

- **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.

Disclosure of personal data

- **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 account manager or Customer Services.

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

- **To government authorities**
  Customers' personal information 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.

- **Banks and financial firms**
  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 firms 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.

- **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.

- **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.

The Customer's rights

- **Right of access**
  The customer has the right to request access to which personal data the Bank processes, and to receive a copy of this information. 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 specify which information or processing activities they wish to access. If the customer does not have access to mobile or online banking, or cannot read electronic documents in any other way, the Bank will send the information in paper form.

  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 and 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.

- **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.

- **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.

- **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 your interests as customer.

- **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.

- **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 account manager or our Customer Services centre.

- **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 to enter into or execute an agreement with the customer.
  - The customer has given their consent.

- **How you can 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.

  The Bank will require the customer to confirm their identity or disclose further information in order to answer the enquiry.

How long does the Bank store personal data?

- **As long as is necessary**
  This means that the Bank generally stores personal data for 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 customer, and this consent is withdrawn, the Bank will delete the data as soon as possible.

- **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 Bookkeeping Regulation: up to ten years.

Sound recordings of investment services: at least five years.

Questions and complaints

- **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, NO-4611 Kristiansand, Norway

  E-mail: personvern@sor.no

  Phone: (+47) 38 10 92 00

  Organisation no.: 937894538

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

- **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.