

Privacy Policy for Spar Nord Bank A/S

Introduction

Here you will find information on how Spar Nord Bank A/S (hereinafter "the bank") acts as a data controller in connection with the processing of your personal data. The privacy policy applies to private customers and potential private customers of the bank. It also applies to sole proprietorships and other third-party individuals such as guarantors, power of attorney holders, and other private individuals with whom the bank is in dialogue or cooperation with. You can read about how and when the bank collects, processes, discloses, and stores your personal data. The information is treated confidentially and in accordance with the Financial Business Act, the General Data Protection Regulation (GDPR), and the Danish Data Protection Act.

Collection and Processing of Personal Data

The bank collects and processes personal data for the provision of financial services of any kind, including payments, customer advice, customer care, customer administration, credit assessment, preparation of credit models, targeted marketing, improvement of customer service, security, and crime prevention, as well as compliance with legal obligations, including the prevention and detection of money laundering.

The bank collects information about you in accordance with the Act on Measures to Prevent Money Laundering and Financing of Terrorism (the AML Act). The information must be documented with a copy of your passport or driver's license and health card. Additionally, the bank continuously collects information about the purpose and intended scope of the customer relationship. The information forms the basis for the bank's knowledge of you as a customer and is also used in the bank's ongoing monitoring of the customer relationship.

If you use credit or debit cards, online banking, or other payment services, the bank collects information from businesses, financial institutions, and others. This is done to process payments, prepare account statements, payment overviews, and similar.

The bank collects information from the Central National Register and other publicly available sources and registers, such as the land charges register. When conducting credit assessments, the bank checks whether there is information registered about you in credit information agencies and warning registers. The bank updates the information continuously.

The bank receives information about you from partners, including other financial institutions, where consent has been given or where there is otherwise a legal basis for it.

The bank's processing of your personal data may be supported by AI systems.

The bank stores your information as long as it is necessary for the purposes that were the reason for the collection, processing, and storage of your data or as long as the bank is required to store the information.

Under the AML Act, information, documents, and records are stored for at least 5 years after the termination of the business relationship or the completion of the individual transaction.

If your information is included in the calculation of the bank's solvency needs, the bank may store the information for up to 20 years.

Surveillance videos are deleted 30 days after recording in accordance with applicable law. In connection with a case, information may be stored for a longer period.

Recordings of telephone conversations with the bank's customer service are deleted 90 days after recording. Recordings of telephone conversations and online meetings related to investments are stored for 5 years to ensure that the bank complies with its obligations under the MiFID II regulation. The Financial Supervisory Authority may request that this information be stored for up to 7 years.

The bank uses cookies and similar technologies to provide the best service and deliver targeted products and services. More information can be found at www.sparnord.dk/cookies.

Basis for Processing Personal Data

To be a customer of the bank, you are required to provide the bank with a range of information as a result of legislation or contractual relationships.

The legal basis for the bank's processing is financial regulation and other legislation, including:

- The Danish Financial Business Act
- Act on Measures to Prevent Money Laundering and Financing of Terrorism
- The Danish Tax Control Act
- The Danish Bookkeeping Act
- The Danish Credit Agreement Act
- The Danish Payment Act
- The Markets in Financial Instruments Directive (MiFID II)
- The Markets in Financial Instruments Regulation (MiFIR)
- The Market Abuse Regulation (MAR)
- The Danish Data Protection Act and The Danish Civil Registration System Act

Additionally, your information may be processed if the processing is necessary as a result of an agreement you have entered into or are considering entering into with the bank, or if you have given your consent, for example, for direct marketing, in accordance with Article 6 (1)(a) and (b) of the GDPR, or if one of the other processing rules in Article 6 (1) and Article 9 of the GDPR applies.

The bank also processes your information when it is necessary to pursue a legitimate interest for the bank, in accordance with Article 6 (1)(f) of the GDPR. This may include the prevention of misuse and loss, strengthening IT and payment security, and necessary testing of IT development.

Disclosure and Transfer of Personal Data

To fulfill agreements with you, for example, if you have asked us to transfer an amount to others, the bank discloses the information about you that is necessary to identify you and complete the agreement.

The bank also discloses information about you to public authorities to the extent that the bank is required to do so under the law, including to the Danish Money Laundering Secretariat at the National Unit for Special Crime (NSK) in accordance with the Danish Money Laundering Act, the Tax Authority in accordance with the Danish Tax Control Act, and the National Bank for statistical purposes.

Transfers of money to and from abroad are made via SWIFT, which is a collaboration between financial companies worldwide. SWIFT is required by US law to provide information to US authorities in case of suspicion of financing crime or terrorism. Therefore, such information may be disclosed to US authorities.

Additionally, with your consent or where permitted by law, information is disclosed to external partners, including correspondent banks, custodian banks, and other financial institutions and service providers that have permission for account information services and payment initiation services if you have requested such a provider to receive information.

If you default on your obligations to the bank, the bank may report you to credit information agencies and/or warning registers in accordance with applicable rules.

Transfers Outside the EU and EEA

In connection with IT development, hosting, and support, personal data is transferred to data processors, including data processors in third countries outside the EU and EEA.

When the bank transfers personal data to data processors in countries outside the EU and EEA, we ensure that your personal data is processed in accordance with the level of protection ensured by the GDPR. Personal data is only transferred to data processors in countries outside the EU and EEA if the bank has a valid transfer basis.

More information on which countries processing takes place can be found on the bank's website www.sparnord.dk/databeskyttelse.

Access to the Bank's Processing of Information

You can gain insight into which information the bank, as a financial institution, processes about you, where it comes from, and what the bank uses it for. You can also find out how long the bank stores your data and who receives data about you, to the extent that the bank discloses your personal data. However, access may be limited by law, the protection of other people's privacy, and the company's business basis and business practices. Additionally, trade secrets, internal assessments, and other material may be exempt from the right of access.

You request access via the bank's website at www.sparnord.dk/databeskyttelse.

Profiling and Automated Decisions

By profiling customer data, the bank conducts big data analyses used to, for example, personalize the bank's websites, develop credit scoring models and more user-friendly services, prevent money laundering, assess the risk of default on credits/loans, and target direct marketing to the bank's customers. You have the opportunity to gain insight into the

consequences of the processing, and you can object to profiling in connection with direct marketing.

The bank's branch Sparxpres makes automated decisions in accordance with Article 22 of the GDPR. Automated decisions assist Sparxpres' staff in concluding loan applications for rejection or approval. The process goes through the same checkpoints as an employee would, i.e., conducting, interpreting, or clarifying necessary register checks, inspecting and interpreting key figures necessary to comply with applicable law, and adhering to Sparxpres' credit policy for the current application. In cases where an automatic decision cannot be made, the application is delegated for manual processing for possible further documentation collection or final credit assessment. You always have the option to request manual processing of an automated decision by contacting info@sparxpres.dk.

Correction or Deletion of the Bank's Information

If the information is incorrect, incomplete, or irrelevant, you have the right to have the information corrected or deleted with the limitations that follow from legislation and applicable processing grounds, in accordance with Articles 16 and 17 of the GDPR.

Restriction of Processing

If you believe that the information the bank has registered about you is incorrect, or if you have objected to the processing of the information in accordance with Article 21 of the GDPR, you can request that the bank restrict the processing of this information to storage. The processing is only limited to storage until the accuracy of the information can be established, or it can be checked whether the bank's legitimate interests override your interests.

If you are entitled to have the information the bank has registered about you deleted, you can instead request that the bank restrict the processing of this information to storage. If the processing of the information the bank has registered about you is only necessary to assert a legal claim, you can also request that other processing of this information be limited to storage.

Withdrawal of Consent

Permission to process information that requires your consent can be terminated at any time by withdrawing your consent. You should be aware that this does not affect the legality of our processing up to the point where you withdrew your consent. If you withdraw your consent, we will store documentation of your consent for 2 years to be able to document valid consent, in accordance with Article 6 (1)(f) of the GDPR.

Withdrawal can be made at sparnord@sparnord.dk.

Data Portability

If the bank processes the information based on your consent or as a result of an agreement, and the processing is carried out automatically, you

have the right to receive the information you have provided to us in an electronic format, in accordance with Article 20 of the GDPR.

Complaint About the Bank's Processing of Information

It is recommended that you first contact us as the data controller if you are dissatisfied with our processing of your personal data.

You have the right to complain about our processing of your personal data to the Danish Data Protection Authority, Carl Jacobsens Vej 35, 2500 Valby, or dt@datatilsynet.dk.

Changes to the Privacy Policy

The privacy policy can be changed without notice if the changes are to the benefit of the customer.

The bank can change the privacy policy with one month's notice if the changes are not to the benefit of the customer. Information about such changes is provided in online banking or mobile banking and on the bank's website.

Contact Information for the Data Controller and Data Protection Officer

Data Controller:
Spar Nord Bank A/S
Skelagervej 15
Postbox 162
9100 Aalborg
CVR number: 13737584
Phone number: 96344000
Email: sparnord@sparnord.dk

Data Protection Officer:
Email: dpo@sparnord.dk
Phone number: 96344371

Address: Skelagervej 15, postbox 162, 9100 Aalborg, Att. Data Protection Officer