PERSONAL DATA PROTECTION POLICY AT SMN

Applicable to	SpareBank 1 SMN – all employees, all trade union representatives and all persons who have access to and/or process and manage personal data through SMN's ICT infrastructure, as well as group companies insofar as appropriate
Basis in law	Personal Data Act and GDPR Art. 5 and Art. 24
Responsible for compliance	CEO in the persons of group management directors
Responsible for updates/revision	Responsibility delegated to the Data Controller
Level of protection	Open
Version	3.1
Established	23.11.2017
Most recent update	02.12.2021
Considered by board of directors	04.12.2021 04.02.2021 05.03.2019 18.12.2017

Revision history

Date	Version	Change	Approved by	Author
22.11.17	**1.0**	**Guidelines established for personal data protection**	**Board of directors**	**Nina Marie Grinde**
23.01.19	**2.0**	**Aligned with new Personal Data Act, incl. GDPR, and 'Guidelines' replaced with 'Policy'**	**Board of directors**	**Åshild Margrethe Revhaug**
27.01.2021	**3.0**	**Addition of formal roles in the SB1-allianse collaboration**	**Board of directors**	**Åshild Margrethe Revhaug**
15.11.2021	**3.1**	**The delegated data controller has responsibility for policy updates and revisions**	**Board of directors**	**Åshild Margrethe Revhaug**

Contents

1. Introduction

1.1 Background

The Personal Data Act implements Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, (hereafter abbreviated to GDPR). The Act and the Regulation entered into force on 20 July 2018. The Regulation is designed to protect the individual's data privacy against violation through the processing of personal data and to ensure protection of the individual's fundamental rights and freedoms.

SpareBank 1 SMN ('SMN' or 'the bank' in the following) processes personal data related to customers and employees. The same is true of group companies.

1.2 Purpose

This policy forms part of the governance element of the internal control system, identifies overall requirements and obligations on the processing of personal data, and describes the in-house organisation set-up, and the responsibility and authority structure.

The bank is dependent on the trust and confidence of its customers, shareholders and investors, partners and supervisory authorities and other stakeholders in order to maintain and expand its own market position. The bank must therefore ensure that personal data are

handled in a confidence-inspiring and safe manner, in conformity with applicable rules. Using a systematic and risk-based approach, the overall purpose of the work on data privacy at SMN is to:

- ensure the protection of data subjects' (customers and others) personal data
- support the management of the business by ensuring that the bank at all times has control over its processing of personal data
- protect SMN's reputation through correct handling of personal data
- ensure compliance with the Personal Data Act and the GDPR

1.3. Policies, standards and procedures

This policy should be viewed in conjunction with other policies, guidelines, standards and procedures of the bank and of SpareBank 1-alliansen in general. See Annex 2 to this policy.

1.4 Relevant legislation in the data privacy sphere

The processing of personal data at SMN is regulated by a number of acts and regulations. Among the most central ones are:

- The Personal Data Act of 15 June 2018 No. 38 to which is annexed the General Data Protection Regulation (GDPR) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
    - Regulations on the use of electronic mailboxes and other electronically stored material
    - Regulations on camera surveillance in undertakings
    - Financial Supervision Act
    - Financial Institutions Act
    - Regulations on the use of information and communication technology (ICT regulations)
    - Financial Contracts Act
    - Regulations on risk management and internal control
    - Anti-Money Laundering Act with regulations
    - Marketing Act

2. Central requirements on the processing of personal data

In order to achieve its objectives the bank must ensure that anyone who handles or processes personal data at or on behalf of SMN contributes to ensuring that personal data:

- are processed in a lawful, fair and transparent manner
- are only collected for specified, explicit and legitimate purposes and are not further processed in a manner that is incompatible with those purposes
- are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)
- are accurate and kept up to date

- are processed in such a way that it is not possible to identify the data subjects for longer than is necessary
- are processed in a manner that ensures information security and the security of personal data

SMN shall

- maintain records of the data that are processed
- maintain an overview of the responsibility and authority structure in the bank as regards the processing of personal data
- maintain an overview and knowledge of regulatory requirements on the processing of personal data, including requirements on the legal basis for processing, fulfilment of quality requirements, compliance with the information requirement, and right of access to and rectification or erasure of personal data
- have established appropriate and practical procedures that describe how the day-to-day handling of personal data should proceed and be secured in order to ensure the confidentiality, integrity and availability of the data
- have established control procedures that provide information on whether established measures and procedures are adhered to
- have in place processes that ensure regular assessment of any need for new measures or changes to existing measures and procedures
- at all times have in place a data protection officer as part of the bank's internal control function
- ensure that the data protection officer becomes involved in an appropriate and timely manner in all matters concerning the protection of personal data. SMN shall in such instances ensure that the data protection officer's advice and assessments are heard and taken into consideration
- support the data protection officer in the performance of his/her tasks by providing the resources and accesses necessary to perform those tasks.

3. Security objectives

SMN's processing of personal information shall be in conformity with regulatory, in-house and contract law requirements regarding information security.

Personal data and other information worthy of protection shall be assessed, classified and handled and secured in a satisfactory manner through physical, technical and organisational measures such that data privacy is not violated.

Confidentiality

Personal data and other information worthy of protection that is processed at SMN shall be protected against unauthorised access.

Personal data shall be processed confidentially and may only be shared with other staff members to the extent necessary for the performance of their duties.

Personal data relating to the bank's own employees may only be processed by a person who needs the data for the performance of his/her duties.

Integrity
Information for which SMN has responsibility will only be produced or changed by employees, or by external parties that are authorised to do so. Information shall not be altered without the consent of the owner of the information/data.

Availability
The processing systems and services shall be available to authorised users as and when needed.

Robustness
Information systems used to process personal data shall be resilient and robust so that a normal situation can be rapidly restored.

4. Organisation and responsibility structure

The bank processes personal data mainly in the capacity of data controller, but in some cases also in the capacity of data processor, for example for subsidiaries. The data controller shall ensure that the body of rules governing data privacy are complied with, and that necessary agreements are in place; see point 5.7.

4.1 Board of directors

The board of directors has overall responsibility for ensuring the bank's compliance with the body of rules governing personal data.

The board of directors shall:

- Establish the objectives and overall strategy for the work on data privacy at SMN
- Ensure that the bank has good internal controls and appropriate systems
- Ensure that SMN bank has a satisfactory organisational set-up that supports compliance
- Ensure that the board keeps abreast of the bank's most important risk areas and determine whether the bank's data privacy management is appropriate to the overall risk faced
- Adopt a personal data protection policy

4.2 Group CEO

The data controller at SMN is the group CEO. The group CEO has paramount responsibility for ensuring that the body of rules governing personal data is complied with and operationalised in the business.

The group CEO shall:

- Operationalise goals and strategies for data privacy and information security
- Clarify responsibilities and authority structure within the bank, including the day-to-day responsibility for processing activities, and delegate tasks as required
- Ensure that adequate resources are available to comply with regulatory requirements in the data privacy area

- Chair the annual status review in the data privacy area (management team's review) which sums up the current position and guides the assignment of priorities ahead
- Contribute to a shared understanding of the risk picture and the need for security measures so as to ensure that the work on data privacy and information security is given the requisite weight and legitimacy throughout the organisation
- The group CEO may delegate his tasks to one of his directors in the role of delegated data controller

4.3 Delegated data controller

The group management director, Technology and Development, performs the role of delegated data controller. This director accordingly acts as data controller in the day-to-day business.

The delegated data controller shall:

- Have overarching responsibility for seeing that the company has in place written procedures and guidelines to ensure that personal data is processed on a day-to-day basis in accordance with the rules in force, and for ensuring that those procedures and guidelines are kept up to date
- Make decisions in personal data matters on behalf of the group CEO. This applies in particular to the approval of data protection impact assessments (DPIAs), and to decisions on whether discrepancies should be reported to the Data Protection Authority in the case of major discrepancies, and in cases involving more than one bank or involving all banks in SpareBank1-alliansen,
- At SMN the delegated data controller will make decisions concerning personal data in SpareBank 1's formal bodies, including Kunderåd Marked (KRM) and Kunderåd IT (KRIT)

4.4 All group management directors

Group management directors have overarching responsibility within their respective areas, and for ensuring that the personal data of customers and employees and other data subjects are duly protected in the processing activities performed in their area of responsibility.

Group management directors shall:

- Delegate tasks focusing on data privacy and information security to managers in the department and see to it that adequate resources are set aside to ensure compliance.
- Ensure that the respective departments are organised and perform their tasks in such a way that legal requirements and in-house guidelines etc., are complied with
- Ensure that requisite risk assessments are carried out in connection with the processing of personal data in the unit concerned, and that adequate measures are implemented to comply with the requirements on personal data processing and information security.
- Ensure that all managers and employees in the director's unit have the training needed to comply with the requirements on the processing of personal data in the performance of their duties.

- Ensure that identified discrepancies are followed up and closed within their particular areas in consultation with the data protection officer and technology, operations and security.
- Ensure that holders of the roles of 'system owner', 'system administrator', 'product owner', 'process owner' and equivalent roles are familiar with their respective roles and associated tasks in order to meet the requirements on data privacy and information security
- Ensure that the data protection officer, technology, operations and security and the legal services departments are consulted where assistance is required in relation to the use of personal data, the carrying out of risk assessments and entry into agreements with data processors (suppliers), etc.
- Consider, upon the introduction of new products or processes, or substantial changes to such products or processes, whether there is a need to call in the data protection officer to undertake a data protection impact assessment (DPIA) or a need for general advice and guidance.

4.5 Data protection officer

The bank has appointed one data protection officer. The data protection officer has a central, independent, advisory, coordinating and reporting role in the organisation as regards compliance with the Personal Data Act and in-house rules. The data protection officer shall assist the data controller in the work of complying with the requirements of the body of rules governing data privacy.

The data protection officer shall:

- Contribute to SMN's protection of the personal data of customers, employees and partners and others, in accordance with the provisions of the GDPR, the Personal Data Act and other relevant rules and regulations that include personal data protection provisions
- Provide information and advice on SMN's obligations under the GDPR
- Provide SMN with advice and guidance on the processing of personal data; see the GDPR Article 38, paragraph 1, and Article 39
- Give, on SMN's request, advice regarding the assessment of data protection impacts (DPIAs) and oversee the carrying out of DPIAs
- Be the point of contact for data subjects in matters concerning the processing of their personal data and concerning the exercise of their rights under the GDPR
- Be the point of contact towards, and collaborate with, the supervisory authorities, institute enquiries at the request of the Data Protection Authority, and coordinate communication between the Data Protection Authority and SMN on rule breaches and other discrepancies.
- Oversee compliance with the GDPR and in-house guidelines on personal data protection

4.6 Legal Services

The Legal Services Department has overarching legal responsibility for data privacy at SMN.

The department shall:

- Provide clarifications related to data privacy, including clarification of regulatory requirements on risk assessments and outsourcing
- Quality assure agreements, including data processing agreements

4.7 Policy compliance

The data protection officer's organisational placement is with the Compliance function, and the position includes responsibility for oversight of and advice related to compliance with the Personal Data Act. The Compliance function can also conduct checks in this area.

The Compliance function shall also:

- Contribute to identifying new and changed statutory requirements related to data privacy,
- Assess and report on the impacts of above changes to enable necessary modifications to be made to processes and procedures.

4.8 Risk Management

Risk Management is responsible for overall risk management and shall assist the various business lines' risk management process in the data privacy area.

Risk Management shall:

- See to the further development of the bank's framework for coherent risk management
- See to the establishment of a methodology and tools for risk management
- See to overarching reporting structures to the group CEO and board of directors as regards risk reporting (e.g. manager confirmation)
- See to an efficient procedure for the approval of new products and processes, in each case checking their compliance with the Personal Data Act.

4.9 All employees

All employees are required to acquaint themselves with the procedures and instructions that are in force and to consult their immediate superior or the data protection officer if anything is unclear.

Employees who learn of breaches of personal data security shall report them using the bank's channels and, as the case may be, directly to the data protection officer without undue delay, so as to enable the bank in the person of the data protection officer to comply with the 72-hour deadline for reporting any breach to the Data Protection Authority.

4.10 Collaborative forums in Sparebank 1-alliansen

4.10.1 'Felles Bestiller'

Felles Bestiller comprises representatives from the regional banks in SpareBank 1-alliansen and a representative for the Samspar banks. Felles Bestiller recommends and manages the

operating and investment budget on behalf of the board of directors of SB1 Utvikling (SB1U), and acts as the banks' contracting party with SB1U as supplier and data processor at the Shared Services Centre.

SMN's representative is the executive director, Group Finance.

4.10.2 'Kunderåd Marked' (KRM)

Kunderåd Marked has responsibility for the overall customer offering for the SpareBank 1 banks' shared services, including the development of joint products and services, a shared direction and content of collaborations on the business and market front, and puts forward proposals together with Kunderåd IT on Masterplan.

SMN's representative on this body is the executive director, Retail Banking.

4.10.3 'Kunderåd IT' (KRIT)

Kunderåd IT has responsibility for the development of joint capabilities, including architecture, infrastructure and solutions that are needed to support the business-related needs. KRIT is also assigned responsibility for the content of collaborative areas on the IT front and puts forward proposals together with Kunderåd Marked on Masterplan.

Kunderåd IT is responsible for overseeing that ongoing development activities conform to adopted architecture principles.

SMN's representative at Kunderåd IT is the executive director, Technology and Development.

5 Strategies to ensure compliance

5.1 Record of processing activities

SMN shall maintain an assembled overview of all processing of personal data. This record shall meet the minimum requirements listed in Article 30 of the GDPR.

The record constitutes documentation of the bank's processing of personal data and of the conformance of such processing to the regulatory requirements.

The bank's managers are responsible for ensuring that all new processing, or changes in the processing, of personal data in their respective areas are recorded and documented in the record of processing activities.

Processing activities handled by SpareBank 1 Utvikling shall in addition be recorded and documented in a separate record of such activities to which SMN has access.

5.2 Training

All staff members shall have a thorough knowledge of the rules relating to personal data and confidentiality. The training provided shall be tailored to the degree to which, and the way in which, staff members handle personal data.

5.3 Risk assessments

All processing of personal data at SMN shall be performed using a risk-based approach. Risk management and acceptance of risk is a management responsibility.

All information processing and use of personal data involves a risk of breach of confidentiality, integrity and availability. Risk acceptance and measures taken shall be proportional to the likelihood and consequences of security breaches. Residual risk (risk remaining after measures taken) shall have been accepted by the management team.

Risk assessments of personal data security shall be performed on a regular basis in connection with changes of significance for the individual's data privacy, and rights and freedoms, and in connection with any new processing of personal data.

Risk assessment is a method for establishing adequate security measures (technical or organisational) and shall be based on the need for protection of personal data and the data's established classification.

Risk assessments shall assess the risk of loss of life and health, financial loss to the individual or loss of reputation and personal integrity as a result of personal data falling into the hands of unauthorised parties, being changed unintentionally, being unavailable when needed or where data privacy is breached in other ways. Where such risk is present, the planned or systematic measures taken shall be proportional to the likelihood and consequences of a security breach. Such measures may be of an organisational, technical or physical nature.

Negative findings of a risk assessment beyond what are in advance defined as acceptable risk shall be reported upwards in the organisation so that measures can either be decided on or implemented, or a decision made to accept the risk concerned.

Risk assessments shall be conducted in accordance with the methodology and boundaries drawn up for use in SMN. The outcome of a risk assessment and acceptance of any residual risk shall be documented.

Risk assessments shall be reviewed annually or as and when required.

5.3.1 Data protection impact assessment (DPIA)

Where the processing of personal data may entail a high risk to data privacy, and to customers' and other data subjects' rights and freedoms, a data protection impact assessment shall be performed. A dedicated DPIA template shall be utilised.

Responsibility for the preparation and approval of a DPIA rests with the responsible group management director in the respective business line. The final DPIA shall be approved by the delegated data controller.

The data protection officer shall assist in the DPIA and give his/her own assessment of the matter, together with the head of information security.

If the DPIA shows that a high risk to data privacy remains after measures are taken, the Data Protection Authority shall be consulted.

The delegated data controller shall see to it that the DPIA is submitted to the Data Protection Authority for evaluation before the processing activity concerned can commence.

The responsible group management director shall see to it that a designated person in the director's own area of responsibility conducts and follows up DPIAs that are prepared on a regular basis.

5.4 Good and timely attention to customers' rights

Steps shall be taken to ensure that rights such as the customer's right to information, right to view personal data, to rectify incorrect data etc., are protected in a simple, coherent and identical manner across the organisation.

5.5 Controls

Procedures shall be established for appropriate controls to verify compliance with the requirement to safeguard data privacy. A plan for ongoing controls shall be drawn up and revised annually. Controls to be conducted by the departments themselves, by the Data Protection Officer and by the Compliance Function shall all be included in such a plan.

5.6 Systematic follow up of undesired events and discrepancies

Steps shall be taken to facilitate simple reporting of undesired events and discrepancies which are duly followed up and systematised in order to ensure continuous learning and improvement.

All managers have a particular responsibility to be alert to discrepancies and breaches of data privacy within their respective areas of responsibility, to ensure a proper response to discrepancies and breaches in cooperation with the data protection officer, and to ensure that discrepancies are reported to the Data Protection Authority in the event of breaches that may pose a risk to data privacy.

The bank, represented by the Compliance Function, shall report breaches of personal data security to the Data Protection Authority within 72 hours if there is a medium to high risk to the data subject.

5.7 Data processors and outsourcing of activities

The processing of personal data can within justifiable limits be outsourced. In such event SMN leaves it to other entities (a data processor) to perform processing activities including the processing of personal data which SMN could have performed itself.

In cases where the processing activity involves the transfer of personal data within the EEA, consideration shall be given to whether a specific legal basis exists for such transfer. Legal Services and/or the data protection officer shall invariably be consulted in such cases.

SMN shall in such cases have in place data processing agreements which at minimum meet the requirements laid down in Article 28 and 29 of the GDPR, and which ensure a transparent responsibility structure and oversight of all such external service providers.

SMN shall satisfy itself that the data processor maintains an appropriate level of security. This shall be done by conducting a risk and vulnerability analysis. The data processor must also be able to document how it assures information security.

SMN shall conduct security reviews of its most important data processors at least every two years, and otherwise when required based on a risk-based approach.

In cases where the bank shares processing responsibility with another data controller, the parties shall agree in writing an arrangement between them that ensures data privacy and sets out how data subjects' rights and freedoms are to be safeguarded.

Where the bank acts as data processor, the bank is responsible for providing advice to the data controller on the applicable body of rules with a view to ensuring that personal data are processed in accordance with fundamental regulatory requirements.

See also the 'Policy for outsourcing of services/activities at SpareBank 1 SMN', which sets requirements as regards entry into outsourcing contracts.

5.8 Reporting

The data protection officer shall report directly to the highest management level at SMN.

Such reporting shall comprise:

- Quarterly reports in conjunction with the Compliance report
- At minimum semi-annual reporting to the Group CEO on the general status of SMN's processing of personal data
- Yearly report to the board of directors

The data protection officer's advice and assessments in matters dealing with protection of personal data shall be documented and accompany the case file to the decision taker.

If decisions are made at SMN that may be in conflict with the personal data legislation or insufficient account is taken of the data protection officer's advice, the data protection officer shall be invited to present his/her assessments to those who are to take the decision, and if necessary, the enterprise's highest management in the person of the Group CEO. If the matter is not resolved, the data protection officer may report the matter to the board of directors.

5.9 Available documentation

Documentation of internal controls including relevant procedures shall be readily available to employees and others who perform tasks for the bank, any data processors and the Data Protection Authority.

6. Annex 1

Policies:

- Information security policy

- Policy for outsourcing of services/activities at SpareBank 1 SMN

Procedures and guidelines:

- Procedure for exception handling with regard to personal data
- Procedure upon request to view personal data
- Procedure for data processor agreements
- Procedure for DPIAs – data protection impact assessments
- Guidelines for erasure of personal data