Privacy Policy

Content

Owner	*Executive Vice President, HR and Legal, Liv Krokan Murud*
Written by	Chief Privacy Officer, Tone Hoddø Bakås
Decided by	*The Board of SpareBank 1 Østlandet*
Status	*Approved by Board of Directors*
Versjon	3.0
Lagring	Governance Documents
Opprettet	11.06.2018
Sist endret	27.01.2025
Antall sider	7

Revision history

Date	Ver	Description	Authors	Approved
13.06.2018	1.0	Updated after a meeting in the compliance forum	Simen Tollersrud Lars Chr. Stensrud	
14.09.2021	2.0	Updated structure and content, clarifications and improvements. Annual review with input from CCO.	Tone Hoddø Bakås	28.10.2021 by the Board
1.7.2022	2.5	Revised after internal audit. Now applies to the group. Some minor changes have been made.	Tone Hoddø Bakås	28.10.2022 by the Board
5.7.2023	2.5	Annual review and sent for consultation. No changes	Tone Hoddø Bakås	No new approval
27.3.2025	3.0	Policy and overarching routine are merged. Minor content changes.	Tone Hoddø Bakås	27.3.2025 by the Board

1. INTRODUCTION

The privacy policy describes the fundamental principles and requirements for privacy in the SpareBank 1 Østlandet (SB1Ø) group. The policy applies to subsidiaries as far as applicable and provides a basis for the companies' own privacy routines.

SB1Ø shall safeguard the rights of the registered and the company's obligations regarding privacy. SB1Ø shall process personal data in accordance with privacy regulations, the Working Environment Act, the Financial Agreements Act, and other financial regulatory frameworks, AI act, and relevant regulations. This policy describes how SB1Ø shall ensure compliance with privacy regulations.

1.1 PURPOSE

The purpose of the privacy policy is to establish principles and requirements, roles, and responsibilities for the processing of personal data in SB1Ø. The policy is part of the governing part of internal control and is supported by specific routines that specify
the requirements.

1.2 GOALS

SB1Ø shall process personal data in a lawful, fair, and secure manner to build trust from customers and employees. The goal of privacy work is, through a systematic and risk-based approach, to ensure:

- Respect for the privacy and human rights of the registered
- Compliance with the Personal Data Act and the EU General Data Protection Regulation (GDPR), other privacy regulations, and recognised guidelines
- Support for business operations by ensuring that SB1Ø always has control over its processing of personal data
- Ensuring the confidentiality, integrity, and availability of personal data
- Protecting SB1Ø's reputation through correct processing of personal data

2. REQUIREMENTS FOR PROCESSING PERSONAL DATA

SB1Ø shall safeguard and document the compliance of the following requirements in the privacy regulations. Routines for the various requirements are available as separate routines.

2.1 SAFEGUARDING PRIVACY PRINCIPLES

In SB1Ø, we shall process personal data so that the fundamental principles for the processing of personal data are complied with. SB1Ø shall document that the requirements in the privacy regulations are complied with.

2.1.1 LAWFULNESS, FAIRNESS, AND TRANSPARENCY

SB1Ø shall only process personal data when it is permitted under the privacy regulations. Each purpose for processing personal data requires a legal basis, which shall be documented and justified. The legal basis can be consent, agreement, legal obligation, or legitimate interest. Processing of special categories of personal data is generally prohibited but can be carried out with additional requirements for the legal basis.

The processing shall be done in respect of the rights of the registered, and it shall be necessary and proportionate. The processing of personal data shall be described in privacy statements in a brief and understandable manner, which shall be easily accessible to all registered (customers, employees, others).

2.1.2 PURPOSE LIMITATION

SB1Ø shall only collect and process personal data for specific, explicitly stated, and legitimate purposes. Each purpose shall be identified and described precisely, and all purposes shall be explained in a way that ensures all affected parties understand what the personal data will be used for. Personal data shall not be further processed for purposes that are incompatible with the original purposes.

2.1.3 DATA MINIMISATION

All processing of personal data shall be relevant and limited to what is necessary for the purpose for which it was collected. SB1Ø shall not use more or additional personal data than what is necessary for the purpose.

2.1.4 ACCURACY

SB1Ø shall have correct and updated personal data. Customers, employees, and others whose personal data we process can request that incorrect information be corrected.

2.1.5 STORAGE LIMITATION

SB1Ø shall only store personal data as long as they are necessary for the purpose for which they were collected. They shall then be anonymised or deleted. A separate routine for the deletion of personal data describes principles and deletion deadlines for the processing of personal data. Deletion deadlines for each processing shall be documented in the Records of the processing activities, and deletion routines shall be documented.

2.2 SAFEGUARDING THE RIGHTS OF THE REGISTERED

SB1Ø shall safeguard the rights of the registered, including:

- The right to information about the processing of their own personal data, through updated privacy statements and other information.
- The right to access the processing of their own personal data.
- The right to rectification and erasure of their own personal data.
- The right to restricted processing of their own personal data.
- The right to data portability.

The rights shall be safeguarded in a simple, comprehensive, and consistent manner across the organisation. When SB1Ø is the data controller, SB1Ø is responsible for safeguarding the rights of the registered. It shall be easy for the registered to exercise their rights. The Data Protection Officer shall assist the registered in exercising their rights. When SB1Ø provides services to other businesses and is the data processor, SB1Ø shall contribute to the data controller's ability to fulfil the rights of the registered.

2.3 RECORDS OF PROCESSING ACTIVITIES

SB1Ø shall have documented and updated Records of processing activities that are carried out, both in the role of data controller and data processor.

2.4 DISCLOSURE OF PERSONAL DATA

Personal data can only be disclosed to external entities that have a legal basis for processing, such as a legal obligation or consent from the registered. Upon request from public authorities for disclosure of information, SB1Ø shall ensure that the necessary purpose and legal basis are safeguarded. The daily data controller shall decide whether personal data can be disclosed. Where SB1Ø is the data processor, the data controller must ensure that there is a legal basis for processing. SB1Ø will then only disclose personal data according to the instructions from the data controller.

2.5 Training

All employees shall have the necessary knowledge of the privacy regulations. Training shall be adapted to different roles, based on responsibilities and tasks.

2.6 Acquisitions and Changes in systems etc

When developing/acquiring and making significant changes to products and systems, SB1Ø shall ensure that privacy requirements are safeguarded, embedded, and documented. SB1Ø shall safeguard and document privacy in development and throughout the system's lifecycle (privacy by design).

2.7 Information security and risk assessment

The processing of personal data shall have satisfactory information security. Systems and digital services shall meet requirements for availability, confidentiality, and integrity. IT systems shall be resilient and robust, so that normal conditions can be quickly restored.

- Availability means that personal data and systems are accessible when needed.
- Confidentiality means maintaining and ensuring that unauthorised persons do not have access to personal data.
- Integrity means that personal data is accurate and reliable.

SB1Ø shall conduct and continuously update risk assessments for information security. Impact assessments shall be carried out for both SB1Ø and the registered. The purpose of the risk assessment is to ensure that the risks identified in the processing of personal data are within acceptable levels, for both SB1Ø and the registered. Necessary measures shall be implemented.

A supplier's risk assessment can be used as a basis but cannot replace SB1Ø's own risk assessment. Where SpareBank 1 Utvikling has conducted risk assessments with satisfactory quality, SB1Ø can document that the documentation has been reviewed and assessed and ensure that it is available in our documentation.

2.8 Data protection impact assessment

A data protection impact assessment shall be prepared when processing personal data that may involve a high risk to the privacy, rights, and freedoms of the data subjects. The purpose of the data protection impact assessment is to ensure that privacy principles and the rights and freedoms of the data subjects are at an acceptable level. The system owner or project manager is responsible for assessing the need for and, if necessary, conducting a data protection impact assessment, and shall always seek advice from the Data Protection Officer. A system shall not be put into operation until the data protection impact assessment is approved by the data controller.

A supplier's data protection impact assessment can be used as a basis but cannot replace the bank's own assessment. Where SpareBank 1 Utvikling has conducted a data protection impact assessment with satisfactory quality, SB1Ø can document that the data protection impact assessment has been reviewed and assessed and ensure that it is available in our documentation.

2.9 Use of data processor

2.9.1 Requirements for data processing agreement

Where SB1Ø uses another entity to process personal data on behalf of SB1Ø, this entity will be considered a data processor. SB1Ø shall then ensure that the data processor complies with privacy regulations and maintains an adequate level of security. SB1Ø shall enter into a written data processing agreement that regulates responsibilities and sets requirements for privacy and information security. If the data processor, or its subcontractor, processes personal data outside the EU/EEA, there must be a valid transfer basis.

2.9.2 FOLLOW-UP OF DATA PROCESSORS

SB1Ø shall regularly review and follow up the data processor's compliance with the data processing agreement, including whether the data processor has implemented sufficient technical and organisational measures to ensure compliance with privacy regulations. The review shall be documented. If the data processor uses a sub-processor, SB1Ø shall have an overview of the entire supply chain. However, it is the data processor's responsibility to ensure that its sub-processors comply with SB1Ø's requirements in the data processing agreement.

Upon termination of a data processing relationship, SB1Ø shall ensure that the solution and personal data are processed as described in the agreement upon termination of the service.

2.10 BREACH OF PERSONAL DATA (INCIDENT)

A breach of personal data (incident) is a breach of confidentiality, integrity, and/or availability of personal data. Incidents shall be managed, followed up, and systematised to ensure continuous learning and improvement. Measures to prevent recurrence and reduce damage shall be implemented.

All employees in SB1Ø shall have knowledge of what constitutes a breach of personal data and shall report any breach or suspicion of a breach of personal data as soon as possible.

An overview of all breaches of personal data (incidents) shall be kept up to date. Breaches of personal data shall be handled in accordance with internal routines.

Breaches of personal data shall be reported to the Data Protection Authority unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The data subjects shall be informed of breaches of personal data if the breach is likely to result in a high risk to their rights and freedoms.

2.11 CONTROL AND FOLLOW-UP

SB1Ø shall have internal control to safeguard the processing of personal data and ensure that established measures and routines are followed. The roles that perform tasks to ensure that the bank complies with privacy regulations shall control their own tasks.

The Data Protection Officer and other internal control functions shall control selected areas assessed based on the risks associated with the processing activities.

3. ORGANISATION, ROLES AND RESPONSIBILITIES

3.1 DATA CONTROLLER OR DATA PROCESSOR

SB1Ø is the data controller when SB1Ø determines the purpose of the processing of personal data and the means to be used. The data controller must comply with the requirements of this policy and associated routines. SB1Ø is the data processor when SB1Ø processes personal data on behalf of a data controller.

3.2 THE BOARD

Each company in SB1Ø is the data controller and data processor, and the board has the overall responsibility under the privacy regulations. The board adopts the privacy policy.

3.3 CHIEF EXECUTIVE OFFICER

The Chief Executive Officer is responsible for ensuring that the responsibilities of the data controller and data processor are complied with in accordance with privacy regulations. The Chief Executive Officer

delegates tasks to ensure compliance with privacy regulations in accordance with the general principles of risk management and internal control.

3.4 DATA PROTECTION OFFICER

The General Data Protection Regulation determines whether the organisation should have a Data Protection Officer and sets out the statutory tasks of the Data Protection Officer. The Data Protection Officer has a special responsibility for safeguarding the rights and freedoms of the data subjects. The Data Protection Officer reports to the board. The Data Protection Officer shall inform and advise and shall monitor compliance with privacy requirements. The Data Protection Officer shall provide information to the Data Protection Authority when requested, including conducting investigations in specific cases.

3.5 EMPLOYEES

All employees shall familiarise themselves with and comply with privacy routines. All employees shall undergo training to ensure that they have a basic knowledge of privacy regulations.

4. REPORTING OF PRIVACY

The Data Protection Officer and the data controller shall report the status of privacy to SB1Ø's board regularly. As part of this report, breaches of personal data security (incidents) shall be reported.

5. DEVIATION FROM PRIVACY POLICY

Breaches of the privacy policy and associated routines may constitute breaches of privacy regulations and shall be reported as a possible deviation.

6. REVIEW

This policy shall be reviewed annually and revised as needed.

7. DEFINITIONS

Personal Data breach	A breach of personal data security that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data that has been transmitted, stored, or otherwise processed.
Processing	Any operation of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, compilation or alignment, restriction, erasure, or destruction.
Data Controller	The entity that determines the purpose of the processing of personal data and the means to be used.
Data Processor	An entity that processes personal data on behalf of the data controller.
Data Subject	The person to whom the personal data can be linked.
Personal Data	Information about an identifiable natural person.
Privacy Regulations	The Personal Data Act, including the General Data Protection Regulation (GDPR), internal policies, and routines to ensure compliance with privacy requirements.
Special Categories of Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a person, health data, sex life, and sexual orientation.