Privacy Policy
SpareBank 1 Østlandet and subsidiaries

Owner	Executive Vice President HR and Legal
Approved by	*The Board of Directors of SpareBank 1 Østlandet*
Status	Approved 28.10.2022
Created	11.06.2018
Last amended	01.07.2022
Number of pages	5

Contents

1. BACKGROUND AND PURPOSE

1.1 INTRODUCTION

The Privacy Policy describes the overarching principles and requirements for protecting privacy in the SpareBank 1 Østlandet Group. The policy applies to subsidiaries wherever appropriate and provides a basis for the companies' own privacy procedures. The policy is reviewed annually and revised as necessary.

SpareBank 1 Østlandet (SB1Ø) processes personal data as part of its everyday operations. SB1Ø must safeguard the data subjects' rights and freedoms related to privacy in relevant processes and tasks.

1.2 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 an integral part of the governance element of internal control. It describes general requirements and obligations for processing personal data, as well as the internal organisation, responsibilities and authorities. The policy is supported by specific routines that specify the requirements in this policy.

1.3 OBJECTIVES

It is important that SB1Ø processes personal data in a proper and secure manner in order to earn the trust of customers and employees, and at the same time be able to create new business opportunities. The objective of the privacy work is, through a systematic and risk-based approach:

- to respect the data subjects' privacy and family life, their home and their correspondence, as well as their other human rights
- to comply with the Norwegian Personal Data Act and the EU's General Data Protection Regulation (GDPR), other privacy legislation and recognised guidelines to ensure that business operations in SB1Ø are in control over its processing of personal data at all times
- to ensure SB1Ø's reputation is protected through to the correct processing of personal data

2. PRINCIPLES FOR PROCESSING PERSONAL DATA

SB1Ø's processing of personal data must comply with fundamental principles for processing personal data. SB1Ø must demonstrate and document that it is complying with the requirements of privacy legislation.

Personal data shall:

- be processed in a lawful, fair and transparent manner
- only be collected for specific, expressly stated and authorised purposes and not processed further in a manner incompatible with the purposes of the processing
- be adequate, relevant and limited to what is necessary (data minimisation)
- be correct and up to date
- be stored such that it is not possible to identify the data subjects for any longer than necessary (storage limitation)
- processed in a manner that fulfils the requirements for information security

3. REQUIREMENTS FOR THE PROCESSING OF PERSONAL DATA

SB1Ø must have processes and routines that protect privacy and the security of personal data.

- Privacy legislation and relevant routines must be complied with in everyday operations.
- The internal control system for processing personal data must be up to date, documented and understood.
- The record of processing activities for personal data for the roles of controller and processor shall be up to date.
- Routines must address the data subjects' rights to access, erasure and rectification. The privacy statement must address the data subjects' right to information.
- Satisfactory information security is required when processing personal data.
- Privacy must be safeguarded during development processes and throughout systems' service lives (privacy by design).
- Risk assessments must be conducted and updated as necessary.
- Data protection impact assessments (DPIAs) must be conducted and updated as necessary.
- Data processor agreements must be entered into with third parties that process SB1Ø's personal data.
- Breaches of personal data security must be dealt with. Timely notification must be provided to supervisory authorities and timely information to data subjects.
- SB1Ø must have internal controls for monitoring the ongoing processing of personal data to ensure compliance with established measures and routines.

4. ORGANISATION, ROLES AND RESPONSIBILITY

4.1 CONTROLLER AND PROCESSOR

SB1Ø processes personal data as a controller and as a processor. SB1Ø is a controller when SB1Ø determines the purposes of the processing of personal data, and which means will be used. SB1Ø is a processor when SB1Ø processes personal data on behalf of a controller.

4.2 BOARD OF DIRECTORS

Each individual company in SB1Ø is a controller and processor, and the Board of Directors bears overarching responsibility pursuant to privacy legislation. The Privacy Policy is adopted by the Board of Directors.

4.3 CHIEF EXECUTIVE OFFICER

The Chief Executive Officer of the company is responsible for ensuring that the tasks necessary to fulfil the Bank's processing responsibilities and controller responsibilities are complied with in line with the privacy legislation.

The Chief Executive Officer has delegated tasks to ensure compliance with the privacy legislation in compliance with the general principles for risk management and internal control.

4.4 DATA PROTECTION OFFICER

In those companies that have appointed a Data Protection Officer, that person bears specific responsibility for ensuring that the data subjects' rights and freedoms are safeguarded. The Data Protection Officer reports to the Board of Directors. The Data Protection Officer plays an advisory and controlling role in the internal control of privacy. The Data Protection Officer must provide the Norwegian Data Protection Authority with information when the authority requests it, which includes carrying out investigations in specific cases.

4.5 ALL EMPLOYEES

All employees, temps and hired consultants have a duty to familiarise themselves and comply with the routines and guidelines that apply to privacy.

5. DEVIATIONS FROM THE PRIVACY POLICY AND FOLLOW-UP

Breaches of the Privacy Policy and associated standards and routines may constitute breaches of the Personal Data Act and must be reported as possible non-conformance in accordance with applicable routines.

6. DEFINITIONS

Term	Description
Personal data	Information related to an identifiable natural person.
Processing	Any operation performed on personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Controller	The enterprise that determines the purposes and means of the processing of personal data.
Processor	The enterprise which processes personal data on behalf of the controller.
Data subject	The person to whom the personal data can be linked.
Personal data breaches	Breaches of confidentiality, integrity and availability of the personal data.