Published by the Board of Directors

Privacy policy

September 2023

Version	Changes	Changed by	Confirmed by	Day.
1.0	First version	DPO	Board	28 October 2020
2.0	Review	DPO	Board	30 November 2022
3.0	Review	DPO	Board	29 September 2023

Contents

This version of the policy is an English translation. The original Icelandic text, as published on the Bank's website is the authoritative text. Should there be discrepancy between this translation and the authoritative text, the latter prevails.

1. Introduction

Íslandsbanki (hereafter the Bank or responsible) provides a rich emphasis on privacy in its operations and is responsible for processing personal information in accordance with fundamental privacy principles, rules of privacy and privacy laws.

1.1. Legal framework

This Privacy Policy is based on the principle of accountability and Art. 24. of the General Data Protection Regulation (EU) 2016/679 (GDPR) which has been implemented in Iceland through Act No. 90/2018 on Data Protection and the Processing of Personal Data (hereafter the Privacy Act). The Privacy Act stipulates, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, that the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Privacy Act. Where proportionate in relation to processing activities, the measures shall include the implementation of appropriate data protection policies.

1.2. Definitions

The following definitions are from the Privacy Act:

Controller: The natural or legal person, public authority or other body which determines, alone or jointly with others, the purposes and means of the processing of personal data. In this policy: Íslandsbanki.

Personal data: Information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing: Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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.

Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal data breach: Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

1.3. Objectives and scope

The aim of this Policy is to ensure that the Bank, its board, and employees adhere to the appropriate laws, rules, and internal rules that apply to the processing of personal data. The Policy is intended to specify the main obligations of the Bank when it comes to protection and processing of personal information and define responsibilities within the bank for that purpose. The Policy is also intended to ensure that the Banks framework is consistent with the relevant laws, rules, recommendations, and guidelines that apply at any given time. The Policy is also intended to ensure that the responsibility and work distribution within the Bank in relation to privacy is clear and adequate monitoring is conducted.

This Policy shall apply to all processing of personal data by the Bank, irrespective of the geographical location of such information. The Policy applies to employees, regulators, contractors, and all those who oversee and process personal data on behalf of the bank as a controller.

1.4. Ownership and audit policy

The Policy is approved by the Board of Directors. The Policy shall be reviewed at least every two years and updated when necessary. The Data Protection Officer is responsible for ensuring that a review takes place and to manage its implementation within the Bank.

2. Roles and responsibilities

2.1. Board of Directors

The Board of Directors approves this Policy and shall ensure that appropriate and adequate internal rules, processes, systems, and procedures are in place.

2.2. All Risk Committee

The All Risk Committee reviews and verifies risk management policy documents, including this Policy, whether periodic reviews or ad hoc amendments, before they are submitted to the Board for approval.

2.3. Executive Board

The Executive Board is responsible for implementing this Policy. This includes ensuring that employees know the Policy and their obligations according to it. Executives are responsible for their employees working in accordance with the Privacy Act as well as relevant external and internal policies, processes, systems and procedures set by the Bank. Executives shall be responsible for employee privacy training, including training on data breaches.

2.4. Data Protection Officer

The Bank's Data Protection Officer (DPO) informs and advises on privacy matters and monitors the implementation of this Policy. It shall be ensured that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data and he or she has the necessary resources to do their work. Furthermore, it shall be

ensured that they receive no instructions regarding the exercise their tasks and will not be suspended or punished for performing their tasks.

The DPO shall inform the responsible person and employees of their obligations under the Privacy Act and provide them with advice thereof. The DPO shall monitor compliance with the Privacy Act including the assignment of responsibilities, awareness-raising and training of staff and the related audits. The DPO shall also provide guidance regarding data protection impact assessments and monitor its performance. The DPO shall act as contact point for the supervisory authority on issues relating to processing of personal data.

Further information on the status and role of the DPO is provided in Article 35 of the GDPR and the DPO's appointment letter.

2.5. Risk Management

Risk Management has a control of implementation and monitoring in accordance with the Bank's rules on management of risk and internal controls. Risk Management along with the DPO and stakeholders shall assess the risk to the rights and freedoms of naturals persons in case of a data breach.

2.6. Compliance

Compliance oversees, monitors, and assesses the bank's compliance risk related to data protection in collaboration with the Data Protection Officer.

2.7. Internal Audit

Internal Audit assesses whether laws, policies, frameworks, and procedures are adequately satisfied and monitors the work of the DPO.

2.8. All employees

All employees shall know and operate in accordance with this Policy.

Employees shall always:

- maintain confidentiality of personal data and process it in a legitimate and fair manner,
- follow procedures that has been implemented for privacy, including reporting without delay any data breaches that may occur according to data breach procedures,
- be aware of the rights of the data subjects,
- seek to limit any damage that the Bank might suffer because of data breach or violation of the Privacy Act.

Employees can seek the advice of the DPO when in doubt about how personal data should be processed. They shall also notify the DPO if they believe personal data is not being processed in accordance with laws, rules, or procedures. Employees can also submit anonymous tips as notifications of misconduct on the Bank's webpage.

3. Privacy Act

3.1. Accountability

To protect the rights and freedoms of individuals when processing personal data appropriate technical and organisational measures shall be taken to ensure and demonstrate that the principles and requirements of the Privacy Act are fulfilled ("accountability"). The appropriate technical and organisational measures include technical measures in systems that store personal data and placement of internal policies and procedures that contribute to and ensure compliance with the Privacy Act.

3.2. The principles of personal information

The processing of personal data should be consistent with principles relating to processing of personal data set out in the Privacy Act with the exceptions that apply, and procedures should reflect those principles. Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency"),
- collected for specified, explicit and legitimate purposes and not processed further in a manner that is incompatible with those purposes ("purpose limitation"),
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation"),
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay (“accuracy”),
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation"),
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

3.3. Rights of the data subjects

The following rights of the data subjects shall be ensured with appropriate limitations:

- The right to be informed about processing, storage, and handling of personal data at the bank
- The right of access
- The right to rectification
- The right to erasure ("right to be forgotten")
- The right to restrict processing
- The right to data portability
- The right to object

3.4. Data protection by design and default

When method of processing personal data is decided and when the processing itself is carried out, appropriate technical and organisational measures shall be implemented. These measures shall be designed to meet the principles of privacy and protect the rights of the data subjects under the Act. This means that the Bank shall put in place rules that contribute to data protection by design and default.

3.5. Records of processing activities

A record of processing activities shall be kept. The record should be made available to the Supervisory Authority at its request. The record should be held in a special system that the privacy officer has access to.

3.6. Processors

Where processing of personal data is carried out by a third party the bank will only use parties that provide sufficient guarantees to implement technical and organisational measures that meet the requirements of the Privacy Act. A written agreement shall always be made in such cases. Outsourcing shall be in accordance with the bank's policy on outsourcing.

When a third party is considered a processor a written data processing agreement shall also be made.

3.7. Data protection impact assessment

When a particular type of processing is likely to pose a high risk for the rights and freedoms of individuals, particularly where new technologies are applied and in terms of the nature, scope, context and purpose of the processing, the responsible party shall assess the impact of the proposed processing operations on the protection of personal data before the processing begins. The Data Protection Officer's advice shall be sought when carrying out this assessment.

3.8. Security

Appropriate technical and organisational measures shall be made in order to obtain satisfactory security of personal data and the handling of personal data is in accordance with the Bank's Security Policy. Personal data breaches shall be handled in accordance with the Privacy Act and the Bank's rules on the handling of personal data breaches.