NORDIC INVESTMENT BANK

FINANCING THE FUTURE

Privacy Policy

Adopted by the Board of Directors of the Nordic Investment Bank on 6 November 2025 with entry into force as of 1 April 2026

NORDIC INVESTMENT BANK | FINANCING THE FUTURE

Adopted by	Board of Directors
Entry into force	1 April 2026
Version and adoption date	Version 1 adopted on 6 November 2025
Document ownership	Data Protection Officer
Implementation responsibility	Departments and units processing personal data
Control responsibility	Data Protection Officer
Responsible committee	Executive Committee
Information to (committee)	n/a
Review cycle	At least every three years
Replaced documents	Privacy Protection Regulations of 1 September 2021
	Personal Data Governance Policy of 1 September 2021
	External Data Protection Policy of 1 September 2021

NORDIC INVESTMENT BANK | FINANCING THE FUTURE

Table of Contents

DEFINITIONS 1
ROLES AND RESPONSIBILITIES 2
1 INTRODUCTION 4
2 COMMITMENT 4
3 IMPLEMENTING PRIVACY 4
4 PERSONAL DATA PROCESSING 5
4.1 Principles 5
4.1.1 Legitimacy of processing 5
4.1.2 Transparency 6
4.1.3 Processing of Sensitive Personal Data 6
4.2 Purposes of processing 6
4.3 Confidentiality and security 7
4.4 Disclosure and transfer of Personal Data 7
4.5 Processing by third parties 7
4.6 Retention and deletion 8
4.7 Data Subject Rights 8
4.7.1 Restrictions to Data Subject Rights 9
4.8 Notification of Personal Data Breach 9
5 DATA SUBJECT REQUESTS AND COMPLAINTS 9

DEFINITIONS

Data Controller means a natural or legal person which determines the purposes and means of processing Personal Data.

Data Processing means any operation or set of operations performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, use, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data.

Data Processor means a natural or legal person which processes Personal Data on behalf of a Data Controller.

Data Subject means an identified or identifiable natural person to whom Personal Data relates.

Personal Data means any information relating to an identified or identifiable natural person (the Data Subject). Personal Data includes, for example, identifiers such as name, contact information, identification number, date of birth, or location, as well as other information which can directly or indirectly identify the Data Subject, for example an online identifier.

Personal Data Breach means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by NIB or by third-party Data Processors processing personal data on behalf of NIB.

Personal Data Transfer means the intentional sending of Personal Data to another party or making the data accessible by it, where neither sender nor Recipient is the Data Subject.

Recipient means a natural or legal person to which Personal Data is disclosed or made available, whether a third party or not.

Sensitive Personal Data means Personal Data relating to race or ethnic origin; social, political, or religious beliefs; a criminal act or sanction; health status or disability; biometric data; sexual orientation; or social welfare needs or benefits.

ROLES AND RESPONSIBILITIES

- NIB's **Board of Directors** is responsible and accountable for data protection and the Bank's compliance with its data privacy framework. This includes responsibility for setting the objectives for data protection in the institution, approving the policies for data protection and privacy, and appointing the Data Protection Officer.

- NIB's **Control Committee** is responsible for monitoring that NIB's operations are conducted in accordance with its Statutes.

- NIB's **President & CEO** is responsible for governance oversight and has the overall responsibility on data protection within the organisation, which includes ensuring commitment to the Bank's approach on data protection and approving rules and guidelines on privacy and data protection.

- NIB's **Executive Committee** is responsible for ensuring that the different departments and functions in the Bank have appropriate processes in place and resources available to fulfil privacy and data protection requirements. Each member of the Executive Committee is responsible for the collection and processing of Personal Data within the areas under their responsibility, and for ensuring that such processing is carried out in compliance with the Bank's data privacy framework.

- NIB's **Head of Risk & Compliance** has the responsibility for the appropriate resourcing and staffing for the proper functioning of the role of the Data Protection Officer.

- NIB's **Data Protection Officer** (DPO) oversees the implementation of NIB's data privacy framework and acts as the Bank's main point of contact in all matters relating to data protection. The DPO is supported by the **Data Privacy Team**, consisting of representatives of the Integrity & Compliance Office, Legal and IT security, and is responsible for:

  - Maintaining NIB's data privacy framework in line with NIB's status and needs;
  - Monitoring the processing of Personal Data across the organisation and assessing compliance with the Bank's data privacy framework;
  - Providing NIB and its Staff Members with information and advice on their duties pursuant to the data privacy framework;
  - Giving advice on carrying out data protection impact assessments and monitoring their implementation;
  - Serving as the contact person for Data Subjects in matters related to the processing of Personal Data;
  - Managing NIB's response to Personal Data Breaches;
  - Whenever required, act as the point of contact for any national or supranational data privacy supervisory body;
  - Reporting on data privacy matters to the President and the Head of Risk & Compliance as well as providing annual reports on data protection to the Board of Directors and the Control Committee;
  - Maintaining current knowledge of data privacy standards and liaising with the data protection functions of other International Financial Institutions and other similar bodies as required.

  NIB has appointed the Chief Compliance Officer to act as the Bank's DPO.

- NIB has appointed departmental **Data Privacy Coordinators** (DPCs) who support their respective heads of department/unit in ensuring compliance on data protection and privacy matters and act as a focal point with NIB's Data Protection Officer.

- NIB **Staff Members** are responsible for ensuring the processing of all Personal Data arising from the Bank's activities is carried out in accordance with NIB's data privacy framework.

PRIVACY POLICY

1 INTRODUCTION

This Privacy Policy ("Policy"), in conjunction with the Code of Conduct for Staff, sets out the Nordic Investment Bank's ("NIB", or "the Bank") commitment to upholding the principles of individuals' privacy in its operations. As part of this commitment, this Policy outlines how NIB will process Personal Data.

As an international organisation, NIB is not subject to any national or international Personal Data protection regulation, nor to the supervision of any supra-national or national data protection authority. NIB, however, considers its member countries' legislation and the legislation of the European Union in developing its policies and procedures. As such, NIB seeks to align itself with the applicable standards and requirements of the EU's General Data Protection Regulation ("GDPR").

2 COMMITMENT

The concept of privacy is based on the fundamental belief that aspects of an individual's life should be free from intrusion or interference and that they have control over their personal information. Privacy includes personal autonomy, the freedom to express oneself, and the ability to maintain confidentiality with regards to matters such as family life or personal communications. Respect for privacy is essential for building trust and preventing discrimination.

Expectations of what is considered private or intrusive can differ from one person to another. However, there are commonly accepted norms of the level of privacy that can be expected in a particular situation, such as in an employment relationship.

NIB is committed to respecting the privacy of all individuals it engages with in its operations and shall not unduly interfere with their personal lives. The Bank shall at all times act with integrity and in a fair and transparent manner towards the individual. In the workplace, NIB shall uphold the principles of privacy and adopt proportionate controls, such as monitoring protocols, which allow the fulfilment of the Bank's employer obligations and the performance of its activities. This commitment to privacy shall be considered in the development of all relevant policies, products, systems, and business processes.

A critical part of privacy is the safeguarding of Personal Data, which includes details such as people's names and medical records, as well as online identifiers and location data. Any personal information that arises during an interaction between NIB and an individual shall be protected to prevent its misuse and any subsequent harm to the individual. Consequently, NIB has a data privacy framework in place to establish proper procedures for the processing of Personal Data, such as guidelines regarding data subject requests and other components required for data protection. NIB shall implement appropriate technical and organisational measures to ensure that processing is performed in accordance with this framework and to safeguard the IT systems and physical records which contain Personal Data.

3 IMPLEMENTING PRIVACY

NIB shall afford individuals appropriate levels of confidentiality and protection of their personal interests in their interactions with the Bank. NIB's safeguards shall be aimed at preventing harm to individuals, including discrimination and financial or reputational damage.

In certain situations, an individual's interests need to be balanced with those of NIB, for example in relation to legal or contractual requirements involving third parties, the defence of legal claims, management of security or compliance risks, or fulfilment of employer or employee obligations. In such situations, a balancing test shall be carried out to evaluate whether NIB's interests are sufficiently compelling and legitimate such that they take priority over privacy considerations.

As part of such a balancing test, NIB shall consider i) the context and whether its interests present a genuine and direct need; ii) the nature of its relationship to the individual, iii) the reasonable expectations of privacy in that context, iv) the actual or potential impact on the individual of any proposed measures, and v) whether the same result could be achieved through other means that are less invasive to the privacy of the individual. The balancing test should ensure that neither the rights of NIB nor of the individual are unduly prejudiced.

Where compelling and legitimate grounds are identified for NIB's interests to take precedence over privacy considerations, any measures implemented shall be proportionate to the matter being addressed.

4 PERSONAL DATA PROCESSING

4.1 Principles

NIB shall process Personal Data in accordance with the following principles:

Lawfulness, Fairness, and Transparency: Personal Data shall be processed in a lawful, fair, and transparent manner in relation to the Data Subject;

Purpose Limitation: Personal Data shall only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

Data Minimisation: Personal Data shall be adequate, relevant, and limited to what is necessary for the purposes for which it is processed;

Accuracy: Personal Data shall be accurate and updated as necessary to fulfil the purpose for which it is processed;

Storage Limitation: Personal Data shall be retained no longer than is reasonably necessary to fulfil the purpose for which it is processed;

Integrity and Confidentiality: Personal Data shall be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

4.1.1 Legitimacy of processing

Processing of Personal Data is only permitted if and to the extent that at least one of the following bases applies:

i. *Consent*: The Data Subject has given consent to the processing of their Personal Data for one or more specific purposes. Consent must be a freely given, specific, informed, and unambiguous indication of the Data Subject's wishes. The Data Subject can withdraw consent at any time.

ii. *Performance of contract*: The processing is necessary for the performance of a contract to which the Data Subject is party, or to entering into a contract with the Data Subject, e.g., an employment contract.

iii. *Legal obligations*: The processing is necessary for compliance with legal obligations to which NIB is subject, which includes compliance with NIB's legal framework.

iv. *Vital interest*: The processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.

v. *Public interest*: The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in NIB.

vi. *Legitimate interest*: The processing is necessary for purposes that are in the legitimate interest of NIB, except where such interests are materially overridden by the interests of the Data Subject.

4.1.2 Transparency

Where Personal Data is collected directly from the Data Subject, NIB shall inform the Data Subject in a clear and concise manner of the purpose of the processing. Data Subjects should understand what Personal Data is collected, who the data is shared with, and, where applicable, if NIB intends to transfer the data outside of the European Union/European Economic Area or to an international organisation. Further, NIB shall provide information on the Data Subjects' rights set out in this Policy.

The actual processing of Personal Data must always correspond to the information provided to the Data Subjects.

The Data Protection Officer is responsible for issuing standard information notices that include the above information to staff and external Data Subjects.

4.1.3 Processing of Sensitive Personal Data

Sensitive Personal Data is critical to protect in order to avoid violations of an individual's privacy and to prevent discrimination.

Sensitive Personal Data may only be processed for NIB's legitimate interests, including legal process and employer obligations. Where reasonable, NIB will obtain consent from the Data Subject for the processing of Sensitive Personal Data.

NIB shall process Sensitive Personal Data with appropriate safeguards and shall ensure that the persons handling such data understand the applicable confidentiality and security requirements. With the exception of fulfilment of employer obligations, NIB shall not disclose such data to third parties without the consent of the Data Subject.

4.2 Purposes of processing

In line with the purpose limitation principle, NIB may only process Personal Data for specified, explicit, and legitimate purposes, and not further process the data in a manner that is incompatible with those purposes. These purposes include, but are not limited to:

Compliance with NIB's statutory and legal obligations, including its legal framework and any data processing agreements.

Management of NIB's credit and funding processes, including project appraisals, integrity due diligence, and arranging funding transactions.

Management of NIB's human resources processes, including recruitment, onboarding, payroll, and administration of social security, taxation, pension, insurances, and staff benefits.

Management of NIB's operational, administrative, and communication processes, including physical security, IT security and systems monitoring, investigation of misconduct and non-compliance, travel management, internal procurement, communication with customers and other external counterparties, promotion of NIB's products and services, visitor and event management.

4.3 Confidentiality and security

Personal Data shall be processed in a manner that ensures its integrity and security, which includes its protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

NIB shall implement appropriate technical and organisational measures to ensure the ongoing security and confidentiality of Personal Data. Personal Data shall be treated in a confidential manner and shall only be handled by designated persons. These designated persons are not entitled to view or in any way process the data, except such as is required for the fulfilment of a specific work task. NIB shall ensure that those persons are aware of these restrictions.

4.4 Disclosure and transfer of Personal Data

NIB may have grounds to disclose Personal Data to certain public authorities and other third parties to satisfy its obligations as an employer or other legal obligations that the Bank determines are required for the performance of its activities and in accordance with its legal framework.

When disclosing data to third parties, NIB shall use appropriate efforts to ensure that the Recipient complies with applicable data protection legislation and maintains an adequate level of protection and safeguards for the processing of Personal Data.

Further, NIB may have grounds to transfer Personal Data outside the EU or EEA or to another international organisation. In such cases, NIB shall ensure that the Recipient maintains an adequate level of protection, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage. This includes the implementation of necessary contractual or other safeguards to ensure the protection of Personal Data in accordance with applicable data protection legislation.

4.5 Processing by third parties

NIB may engage a Processor to process Personal Data on its behalf. In such cases, NIB shall ensure that the Processor complies with applicable data protection legislation and NIB's instructions and maintains adequate levels of protection and safeguards for the processing of Personal Data.

If adequate safeguards are absent in a third party, and the transfer of Personal Data cannot be avoided, the data may only be transferred on the basis of the prior consent of the Data Subjects, following the provision of comprehensive information to the Data Subjects on the potential risks related to such a transfer.

4.6 Retention and deletion

In accordance with the storage limitation principle, NIB shall retain Personal Data for no longer than is reasonably necessary for the original purpose for which it was processed.

The department or unit collecting the Personal Data is responsible for its retention and deletion and shall establish procedures for the systematic erasure of the data after the end of the applicable retention period.

As erasure processes are often done on an annual cycle, records should be destroyed in the year following the expiry of the applicable retention period. With regards to Sensitive Personal Data, NIB shall use its best efforts to evaluate at least every five (5) years which data is no longer needed.

4.7 Data Subject Rights

NIB respects and upholds the following rights of the Data Subject:

Right to access: Data Subjects have the right to get a confirmation as to whether NIB is processing Personal Data on them. If so, the Data Subject is entitled to receive a copy of the Personal Data being processed. Access requests are managed in line with NIB's Guidelines for handling Data Subject Requests.

Right to rectification of inaccurate or incomplete data: Data Subjects have the right to request NIB to rectify any inaccurate Personal Data that is being processed on them. Data Subjects also have the right to request incomplete Personal Data be completed.

Right to erasure: Data Subjects have the right to request the deletion of their Personal Data where there are no overriding legitimate grounds for NIB to retain the data any longer for the specific purpose(s) it is processed for.

Right to object to processing based on NIB's legitimate interest: Data Subjects can object to the processing of their Personal Data in cases where NIB's processing is based on legitimate interest. This means to request that the Personal Data shall no longer be processed for such purposes. In case of marketing, Data Subjects always have the right to object to the processing.

Right to restrict processing of Personal Data: Data Subjects have the right to request that NIB restricts the processing of their Personal Data under certain circumstances. Restriction entails that the Personal Data in question may only continue to be processed (i) with the Data Subject's consent; (ii) for the establishment, exercise or defence of legal claims; (iii) for the protection of the rights of another natural or legal person; or (iv) for reasons of important public interest.

Right to data portability: Data Subjects have the right to receive the Personal Data they have directly provided to NIB in a structured, commonly used, and machine-readable format, and have the right to transmit those data to another controller, if the processing is based on consent or contract, and is carried out by automated means.

Right not to become subject to automated decision-making: Data Subjects have the right not to be subject to decision based solely on automated processing, including profiling, which produces legal effects concerning the Data Subject or significantly affects them.

4.7.1 Restrictions to Data Subject Rights

NIB's activities and related processing of Personal Data may result in some of the Data Subject rights outlined above not being fully applicable. This concerns, for example, the right to data portability or the right not to become subject to automated decision-making.

Further, the Bank may restrict the application of the Data Subject rights set out in this Policy if such restriction respects the interests of the Data Subject, and constitutes a necessary and proportionate measure to safeguard:

a) the management of safety and security risks to staff and other individuals involved in the Bank's activities;

b) the prevention of, or inquiry or investigation into, misconduct, prohibited practices, or any other type of criminal offences occurring in the Bank's operations or activities, as set out in NIB's Investigation Policy;

c) the establishment, exercise of defence of legal claims;

d) dispute resolution proceedings;

e) the protection of the rights and freedoms of others.

4.8 Notification of Personal Data Breach

Where NIB becomes aware of any Personal Data Breach, measures to respond to the breach and mitigate its consequences shall be taken in accordance with the instructions on handling Personal Data Breaches[1].

If a Personal Data Breach is assessed to likely result in a material risk to the privacy of the affected Data Subjects, NIB shall notify the Data Subjects without undue delay.

Notification of Data Subjects is not required if the Bank is able to demonstrate that i) appropriate technical and organisational protection measures have been implemented, and that those were applied to the Personal Data affected by the breach, in particular those that render the Personal Data unintelligible to any person who is not authorised to access it, e.g., through encryption; and ii) subsequent measures to ensure that the high risk is no longer likely to materialise were taken.

5 DATA SUBJECT REQUESTS AND COMPLAINTS

NIB's Data Protection Officer acts as the main point of contact for Data Subjects in matters regarding their privacy and the processing of their Personal Data.

Data Subjects can exercise their rights and address requests and complaints to the DPO by email at: dataprotection@nib.int

[1] Internal document