Data Privacy Policy

Company:	Nordnet AB (publ), Nordnet Bank AB
Approved by:	Board of Directors
Date of approval:	2024-11-25 (replaces 2023-11-23)
Document owner:	Data Protection Officer
Revised:	Annually or more often if required
Confidentiality class:	Open

Table of Contents

1 Introduction

1.1 Background

The protection of personal data in relation to the processing of personal data is a fundamental right. To ensure that processing of personal data is conducted in a lawful, correct, and secure manner in compliance with external requirements, the board of directors of Nordnet AB (publ) and Nordnet Bank AB (together referred to as "Nordnet") have, respectively, adopted this *Data Privacy Policy.*

1.2 Purpose and objective

The purpose of this policy is to ensure that Nordnet conducts is operations in a manner which complies with external requirements and to establish the board of director's requirements on the role of the data protection officer ("DPO"). Corresponding policies are adopted in other relevant companies within the Nordnet group.

As a DPO is not appointed for Nordnet AB (publ), the sections regarding the DPO's tasks and assignments in this policy shall only be deemed relevant for Nordnet Bank AB.

This policy shall together with the underlying instructions and routines constitute the basis for processing of personal data at Nordnet.

1.3 Regulatory basis

This policy has been established in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR").

2 Definitions

Personal data	Personal data means any information regarding an identified or identifiable living natural person. An identifiable person is someone who can be identified, either directly or indirectly, through identifiers. Information which in itself does not identify a person can be personal data if the information in combination with other information identifies a person, regardless of whether the data is in its combined state or not.
Processing	Processing of personal data means any operation or set of operations which is performed on personal data, whether or not by automated means. This includes, but is not limited to, collection, recording, organization, structuring, storing, use, disclosure, analyzing, combining, or deletion.
Sensitive personal data	Sensitive personal data is explicitly regulated in Article 9 of the GDPR and are referred to as "special categories of personal data", which are racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation. Sensitive data shall as a general rule not be processed if not absolutely necessary and only provided that a legal exemption from the prohibition applies and strict safeguards are implemented.

Integrity sensitive personal data	Certain categories of personal data are more sensitive than other even though they are not classified as "special categories" in the GDPR. These categories are commonly described as "integrity sensitive data" and refers to categories that, due to their sensitivity, should be subject to extra security measures. Such categories include, but are not limited to, social security numbers, criminal offenses, financial information, information on an individual's private sphere or social relations, information about minors, and descriptions/evaluations of personal attributes.
Profiling	Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Automated decision-making	Automated decision-making means the ability to make decisions by technological means without human involvement. The GDPR provides a general prohibition on automated decision-making, including profiling, that has a legal or similarly significant effect. Nordnet may only conduct automated decision-making if a legal exemption applies, and transparency requirements are met.
Controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
Processors	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
Data subject	A natural person whose personal data is processed.
Privacy risk	The current or prospective risk to earnings and capital arising from violations or non-compliance with privacy related laws, rules, regulations, agreements, prescribed practices or ethical standards which can lead to fines, damages and/or the voiding of contracts and can diminish Nordnet's reputation.

3 Nordnet's data protection principles

3.1 General

Nordnet shall commit to comply with the following principles in every processing activity that Nordnet is responsible for. No processing of personal data shall occur unless these basic principles are met.

3.2 Lawfulness and fairness

Processing of personal data is only lawful and fair when based on a valid and approved legal basis. The eligibility of each legal basis depends on the purpose for which Nordnet needs to process personal data.

Nordnet shall establish processes to ensure that no personal data is processed before the purpose and its legal basis has been determined and subject to a legal assessment.

Nordnet shall have a separate process for assessing legitimate interest as a legal basis, where the weighing of interests is documented to ensure fairness and proportionality.

Nordnet's processing activities upon consent as legal basis shall be conditioned by an active and explicit consent from each data subject after the provision of relevant information on the processing and their rights.

3.3 Transparency

Nordnet's data flows shall be designed to ensure that data subjects have been informed about the data processing in a concise, transparent, intelligible, and easily accessible form.

Nordnet shall provide privacy notices on its external websites available to the data subjects at all times. Nordnet shall ensure that updates are communicated through established communication channels with the data subjects.

In the event of a data breach incident that is likely to result in a high risk for the data subjects, Nordnet shall ensure that affected data subjects are duly notified about the incident in order to enable necessary precautions. Such communication shall be made without undue delay.

3.4 Purpose limitation

Processing of personal data is only allowed if it is processed in a manner that it is compatible with the purpose the data was collected for. The purpose must be specified and explicit.

Nordnet shall keep and maintain a records of processing activities which strictly determines each business function's processing activities. Any planned deviation must undergo new assessments and procedures.

3.5 Data minimization

Nordnet shall ensure that processing activities only use the personal data necessary in relation to the purpose for which the data is being processed. This means that in each and every set of processing, Nordnet shall make sure that no more personal data than what is absolutely necessary to fulfil the purpose of the specific processing are used. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility.

3.6 Storage limitation

No personal data at Nordnet shall be kept in a form which permits direct or indirect identification of a data subject for longer than what is absolutely necessary for the purpose(s) for which the personal data was initially collected and processed.

Nordnet shall remove personal data by deleting/destroying or by anonymizing it as soon as the purpose has seized to exist. To ensure that personal data are not stored for longer than necessary, Nordnet shall introduce specific deadlines and routines for deletion and anonymization.

3.7 Security and confidentiality

Nordnet shall continuously work to ensure that Nordnet's products and services as well as internal processes meets the requirements set by privacy regulations.

Nordnet shall commit to implement leading data protection standards and continuously educate our employees regarding data privacy management. Nordnet's security is based on well-established standards for architecture and security that ensures continuous maintenance and improvements in accordance with the ongoing changes of the threat landscape. Audits, vulnerability scans and security tests are an integral part of Nordnet's ongoing risk and security management.

Nordnet shall take all reasonable steps to ensure that all processing activities are carried out in a manner which ensures appropriate security of the personal data. Such consideration includes, but is not limited to, the nature, scope, context and purposes of processing, likelihood and severity of the risks posed by the processing activities, cost of implementation, and the current state of art. Examples of security measures are pseudonymization, encryption of personal data and effective access controls. Internal confidentiality, like between departments and staff groups, are regulated by internal policies and access controls.

Nordnet shall adopt processes for every planned processing activity, which include privacy impact and risk assessments to ensure that all security and privacy risks are handled properly.

3.8 Accountability

Nordnet shall at all times be able to demonstrate compliance with what has been stated in this section.

4 Roles and responsibilities

4.1 Board of Directors

The Board of Directors bears ultimate responsibility for oversight, ensuring that the processing of personal data adheres to this policy.

4.2 CEO

The CEO is responsible for appointing a DPO, ensuring that the content of this policy is implemented and adhered to by the organization and for ensuring that Nordnet has the expertise and resources necessary to fulfil the objectives and processes stated in this policy. The CEO shall establish further instructions for the business to ensure that the principles set forth in this policy are adhered to.

4.3 All employees

All employees shall comply with applicable laws and regulations as well as Nordnet's internal standards and routines. Every employee shall contribute to the work of ensuring that Nordnet's processing of personal data is appropriate and compliant and shall be provided with appropriate trainings, tools, and resources for this objective.

4.4 Data Protection Officer (DPO)

4.4.1 General

Nordnet shall at all times have an appointed DPO who shall work independently and have the required knowledge to perform the tasks referred to in the GDPR

The DPO shall provide recommendations to the business, e.g. in regards to privacy impact assessments. Data subjects who wish to raise concerns about their data privacy shall be able to contact the DPO directly through provided contact details in Nordnet's privacy notice as always available on Nordnet's websites.

Nordnet's DPO shall be registered with the local supervisory authorities and shall function as a contact point vis-à-vis the supervisory authorities in case of e.g. a data breach incident or a prior consultation on a planned processing activity.

The DPO shall be provided with relevant training on an ongoing basis.

4.5 Internal reporting

The DPO shall report to the highest level of management. Nordnet shall construct its organization in a way which enables and secures the DPO's independence in relation to the management so that data protection can remain the DPO's one and only objective.

The DPO shall report regularly, at least annually, on significant privacy risks identified to the board of director and to the CEO. The annual report shall follow up on previously identified and reported deficiencies and risks and should report on each new identified deficiency and risk. An impact assessment and a recommendation for measures shall be included in the report. The report shall include a summary of data breaches which have occurred during the year and whether any data breaches have been reported to the supervisory authority.

4.5.1 Annual work plan

The DPO shall identify privacy risks within Nordnet and perform monitoring and control to ensure that such risks are managed by relevant functions. Nordnet shall apply a risk-based approach when monitoring its privacy risks, and the risk management shall be based on the same principle as those that apply within operational risk management.

The DPO shall establish a plan for its work during each calendar year. The work plan shall include a list of the areas the DPO intends to control and a prioritization order based on the performed risk assessment, thus the work plan should be established with a risk-based approach. When preparing the work plan, the DPO shall consider all areas of products and services provided by Nordnet.

4.5.2 Information, advice, and trainings

The DPO shall be responsible for ensuring that applicable privacy laws, regulations, general advice, industry rules and internal rules that are relevant to the business are known to the Nordnet's employees and to the board of directors.

The DPO shall keep itself informed and updated about Nordnet's operations and changes to the same.

The DPO shall ensure that GDPR related trainings are provided to new employees and that any further trainings are provided when deemed necessary.

4.5.3 New products and processes

The DPO shall assess that new products and processes in Nordnet are adapted to comply with the currently applicable external privacy regulations.

5 Data subject rights

Nordnet shall ensure that data subjects have the right to exercise the following:

Right to access: The data subject has the right to know if Nordnet is processing his/her personal data and in such case get information about what personal data Nordnet is processing about him/her.

Right to rectification: If the data subject finds any of processed personal data to be incorrect or incomplete, he/she has the right to request amendment or supplementation of that personal data.

Right to erasure: The data subject has the right to have his/her personal data deleted. However, this is not applicable in certain cases, e.g. if the retention of the personal data is required to fulfil legal obligations.

Right to restrict processing: Under certain conditions, the data subject has the right to restrict the data processing to certain selected purposes or restrict the processing during a limited period.

Right to data portability: The data subject has the right to obtain his/her personal data, or have it sent to a third party, in a structured, commonly used, and machine-readable format. This right is limited to the personal data which the data subject has provided to Nordnet and which Nordnet is processing based on the data subject's consent or his/her contractual relationship with Nordnet.

Right to object: The data subject has the right to object whenever the data processing is based on consent as lawful basis, whenever the personal data is being used for direct marketing purposes or whenever the data processing entails automated decision-making, including profiling, that results in legal effects concerning him or her or similarly significant affects him or her.

The right to object in other situations shall be assessed on a case-by-case basis. The processing purpose can prevail e.g. if Nordnet can demonstrate compelling legitimate reasons for the processing that override the individual's interests, rights, and freedoms or if the processing is carried out in order to establish, exercise or defend against legal claims.

Right to lodge a complaint: The data subject has the right to lodge a complaint to the supervisory authority.

Further details on Nordnet's management of data subject rights can be found in underlying instructions and routines.

6 Personal data breaches

Nordnet shall monitor and document its personal data breaches. In addition, Nordnet shall assess whether an incident is not unlikely to result in a risk or a whether a breach is likely to result in a high risk to the rights and freedoms of natural persons.

If an incident is not unlikely to result in a risk to the data subject, Nordnet shall notify the relevant supervisory authority without undue delay, but at the latest within 72 hours of the incident being identified and reported internally. If the breach is likely to result in a high risk, Nordnet shall, if possible, confirmed those concerned directly without undue delay.

All personal data breaches and their risk assessment shall be documented.

7 Third parties

As a part of Nordnet's operations, information may be shared with third parties, e.g. entities within the Nordnet corporate group, suppliers (including usage of third-party tools and services), trusted partners and administrative authorities.

Disclosure to data processors for processing operations on Nordnet's behalf shall be treated as data processing operations carried out by Nordnet, since it is Nordnet that determines the purpose and means of such.

Data disclosure with another data controller, regardless of whether the recipient is a joint or separate controller, requires a lawful basis and assessment of compatibility. Nordnet shall never share more information than what is strictly necessary for the relevant processing purpose about which information has been provided to the data subjects.

Nordnet shall take appropriate and relevant contractual, technical, and organizational measures to ensure that suppliers, both in and outside of the EU/EEA, handle personal data in a secure and correct manner in compliance with applicable privacy regulations and Nordnet's privacy and security policies.

7.1 Data processors

Any personal data processing carried out by a data processor on behalf of Nordnet shall be governed by an entered data processing agreement (DPA) that determines clear instructions for the data processing operations and the data processors undertakings in terms of security and confidentiality.

The DPA shall require the data processor to provide means for and assist Nordnet in enabling data subject's rights laid down in the GDPR. Unless already provided and guaranteed as a standard, the DPA shall be supplemented with Nordnet's information security requirements.

Nordnet shall have established procurement and change initiative processes to ensure that data processors can and will live up to their undertakings in correspondence with Nordnet's privacy and information security standards. Nordnet shall reviews its data processors on a regular basis to ensure that entrusted personal data and processing operations are duly handled.

7.2 Joint controllers

Where Nordnet and another operator jointly determine the purposes and means of processing, joint controllership shall be at hand. The respective responsibilities for compliance with the obligations under the GDPR shall be determined in a data sharing agreement. The arrangement shall reflect the respective roles and relationships of the joint controllers towards the data subjects. The essence of the arrangement shall be available to the data subjects. The arrangement does, however, not affect the exercise of data subject's rights; the data subjects shall be able to exercise their rights and lodge complaints against any and each of the controllers.

7.2.1 Separate controllers

Whenever Nordnet discloses personal data to a data controller that determines its own purpose and means for their own data processing, each operator shall be deemed as a separate controller. Before such disclosure Nordnet shall carefully assess the lawful basis for such disclosure. Furthermore, Nordnet is responsible for safeguarding the data during transfer and for not disclosing more data than what is necessary for the purpose.