Personal Data Protection Policy

1. Objective

The objective of the Personal Data Protection Policy (“this Policy”) is to set out the principles and standards for managing Personal Data Protection and Confidentiality Risk across NordBank and its Subsidiaries (the “Group”). In relation to Confidentiality Risk, the scope of this Policy is limited to confidentiality of Personal Data. Confidentiality Risk related to data other than Personal Data is covered by the IT Risk Management Policy.

This Policy is designed to facilitate compliance with relevant data protection law including Article 8(1) of the Charter of Fundamental Rights and Article 16(1) of the Treaty on the Functioning of the European Union, the General Data Protection Regulation (EU) 2016/679 (“GDPR”) and national data protection laws.

Lack of adherence to this Policy may lead to disciplinary actions.

2. Definitions

The definitions for the terms used throughout this Policy are available in Appendix 1.

3. Scope and target group

This Policy applies to all Personal Data Processing performed by the Group.

This Policy applies to all Employees.

The Management Body of a Subsidiary may approve this Policy with deviations to ensure the policy is fit for purpose for the subsidiary. The policy administrator in the Subsidiary should discuss the rationale behind the deviation and ensure that the administrator of the Group Policy is consulted on material deviations.

The administrator of this Policy must document and report material deviations from this Policy to the owner of this Policy.

4. Policy Content

4.1 Governance and Accountability

Principle 1: The effective management of Personal Data Protection & Confidentiality Risk must be embedded in a defined risk governance framework

The risk governance framework in relation to Personal Data Protection and Confidentiality Risk is established in accordance with the standards outlined within the Group’s Enterprise Risk Management Policy and data protection governance framework. This includes:

• clear roles, responsibilities and accountabilities defined in accordance with the three lines of defence model to enable effective risk management of Personal Data Protection and Confidentiality Risk, including risk ownership, risk oversight and risk assurance;
• appointment of an independent DPO;
• creation and maintenance of records of Personal Data Processing;
management of Personal Data Protection and Confidentiality Risk in accordance with the Risk Tolerance Statement;
• clear standards outlined to enable effective risk management;
• management information and reporting to monitor and oversee Personal Data Protection and Confidentiality Risk;
• identification, assessment and mitigation of Personal Data Protection and Confidentiality Risks for the Group and for Data Subjects by way of risk assessments, including Data Protection Impact Assessments;
• a robust control framework that is designed and operating effectively to promote a “Data Protection By Design and By Default” approach to mitigate Personal Data Protection and Confidentiality Risk;
• adequate resources allocated to Personal Data Protection and Confidentiality Risk management, oversight and assurance in respect of personnel, competency and tools.

Roles and Responsibilities for Principle 1

• Employees who handle Personal Data are responsible for complying with this Policy and related instructions so far as it relates to their daily work.
• Business Units and relevant Group Functions are responsible for identifying, assessing and mitigating Personal Data Protection and Confidentiality Risk through development and maintenance of suitably designed and effective processes and controls, as well as ensuring that employees have adequate competencies and awareness.
• Product, Process and System Owners are responsible for:
o documenting all Personal Data Processing in a Record of Processing;
o considering data protection principles and applying Data Protection By Design and By Default requirements when designing new or amending existing products, processes and systems/applications under their ownership;
o conducting appropriate Data Privacy Risk Assessments for all new or substantially amended products, processes and systems/applications that use Personal Data under their ownership.
• 1LoD (with particular relevance for risk and controls teams) are responsible for:
o provision of advice on risks and appropriate controls to Business Units and Group Functions in relation to products, processes and systems/applications that process Personal Data;
o escalation of business/legal risks to SME units where specialist input is required;
o escalation of business/legal risks to management and/or Risk Committees as appropriate in accordance with the Group's procedures.
• Group Compliance is responsible for:
o developing and maintaining policies, instructions and relevant training in relation to Personal Data Protection and Confidentiality Risk, as well as overseeing and monitoring the

Group's compliance with the standards and requirements;
o design of the Group's Data Privacy Risk Assessment framework;
o providing data protection compliance information, advice, review and challenge and issuing recommendations to the Group where required/appropriate;
o reporting internally on Personal Data Protection and Confidentiality Risks affecting the Group, including trends and operational improvements.
• DPO is responsible for:
o overseeing and monitoring the Group's compliance with the GDPR, national data protection laws, and data protection governing documents including the assignment of responsibilities;
o providing information and advice to Group entities, including Data Controllers, Data Processors and Employees who carry out Personal Data Processing, on their obligations;
o providing advice, where requested, as regards the Data Protection Impact Assessment and monitoring of its performance;
o escalating issues/risks that have a substantial impact on Data Subjects, where necessary/appropriate. Escalation includes the ability to directly report to the highest management level;
cooperating with, and acting as a point of contact for, the relevant national Data Protection Authorities, in accordance with the Regulatory Engagement Policy where applicable;
o acting as a contact point for Data Subjects;
o providing advice, to non-EU branches and Subsidiaries on matters of territorial scope for data protection requirements.
• Senior Management are accountable for the proper implementation of the Personal Data Protection and Confidentiality Risk framework by:
o establishing clear ownership of Personal Data Protection and Confidentiality Risk within their Business Unit or Group Function;
o establishing adequate compliance governance arrangements across all principles within this Policy;
o appointing accountable roles to manage and be responsible for implementation of Personal Data Protection and Confidentiality Risk and Personal Data Processing activities on behalf of their Business Unit or Group Function.

4.2 Personal Data Protection Requirements

Principle 2: The Group must have a legal basis for Personal Data Processing

Sub-principle 2.1: To ensure the processing of Personal Data is lawful, the Group must determine and document a valid legal basis before commencing Personal Data Processing

Personal Data Processing is only lawful where one or more of the following legal bases applies:
• the Data Subject has given consent to the processing for one or more specific purposes;
• the processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
• the processing is necessary for compliance with a legal obligation;
• the processing is necessary in order to protect the vital interests of the Data Subject or another natural person;
• the processing is necessary for the performance of a task carried out in the public interest;
• the processing is necessary for the purposes of the legitimate interests of the Data Controller or a Third Party.
The legal basis or bases for Personal Data Processing must be documented.
The Personal Data Processing Principles must be taken into account regardless of the legal basis chosen – see further Principle 3.

Sub-principle 2.2: Processing of Special Categories of Personal Data is prohibited unless a legal exception applies

The processing of Special Categories of Personal Data is generally prohibited. To lawfully process Special Categories of Personal Data, the Group must – before commencing the Personal Data Processing – identify a legal basis for processing as set out in sub-principle 2.1, and a separate condition for processing.
The conditions are:
• The Data Subject has given explicit consent to the processing (except where Member State law provides that the prohibition cannot be lifted by consent of the Data Subject).
• Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment and social security and social protection law.
• Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
• Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.
• Processing relates to Personal Data which are manifestly made public by the Data Subject.
• Processing is necessary for the establishment, exercise or defence of legal claims.
• Processing is necessary for reasons of substantial public interest, on the basis of European Union or Member State law.
Processing is necessary for the purposes of preventive or occupational medicine.
• Processing is necessary for reasons of public interest in the area of public health.
• Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Sub-principle 3.3: The Group must identify a specific legal basis for the processing of Personal Data relating to criminal convictions and offences

The Group may only process Personal Data relating to criminal convictions and offences or related security measures when the processing is authorised by European Union or Member State law and provides for appropriate safeguards for the Rights and Freedoms of Data Subjects.

Roles and Responsibilities for Principle 2

• Process Owners must ensure that they identify and document an appropriate legal basis before commencing Personal Data Processing activities.

Principle 3: The Group must comply with the Personal Data Processing Principles

Compliance with the Personal Data Processing Principles provides the foundation for the protection of Personal Data. The Personal Data Processing Principles require that Personal Data must be:

• processed lawfully, fairly and in a transparent manner ("lawfulness, fairness and transparency");
• collected for specified, explicit and legitimate purposes, and not further processed in 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 ("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 and unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality");
• In addition, the Group shall be responsible for and be able to demonstrate compliance with the above principles (the "accountability principle").

Roles and Responsibilities for Principle 3

• All employees must comply with the Personal Data Processing Principles when using Personal Data.
• Product, Process and System Owners must ensure that products, processes and systems/applications that include Personal Data Processing comply with the Personal Data Processing Principles.
• Senior Management are accountable for ensuring that teams under their management are aware of the requirements and responsibilities set out above relevant to their business remit and/or product, process and system ownership and for promoting compliance with the same.

Principle 4: Any Transfer of Personal Data to a Third Country must comply with regulatory requirements

Any transfer of Personal Data to a Third Country must firstly identify a legal basis for the processing of the Personal Data in question as set out at Principle 2.

In addition, the Group can only Transfer Personal Data to a Third Country (also known as " International Transfers") where the conditions for such Transfers laid down in the GDPR are also met. Additional conditions apply for Transfers from the United Kingdom to other Third Countries. The Group and the Third Country recipient of Personal Data from the Group must ensure the security of Personal Data, but moreover they must protect the Rights and Freedoms of Data Subjects regardless of how the International Transfer is structured/executed.

Roles and Responsibilities for Principle 4

• Product, Process, System and Contract/Service Owners are responsible for ensuring that Third Country Transfers of Personal Data are only carried out where regulatory requirements are met. Technology & Services Legal provide legal advice on International Transfers of Personal Data and are responsible for evaluating the legal compliance of the Transfer.

Principle 5: The Group must ensure Data Subjects can exercise their rights in a timely and transparent way

The Group must implement and maintain processes to manage and ensure that Data Subjects can exercise the following rights related to their Personal Data:

• The right to information or to be notified about the processing of Personal Data.
• The right to access Personal Data.
• The right to request the restriction of processing.
• The right to request rectification of inaccurate or incomplete Personal Data.
• The right to request erasure of Personal Data where specific grounds apply.
• The right to data portability.
• The right to object to the processing of Personal Data where the processing is based on the performance of a public task, the legitimate interests of the Data Controller, or for the purposes of direct marketing.
• The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects on the Data Subject unless specific conditions and safeguards apply.

Roles and Responsibilities for Principle 5

• Employees are responsible for identifying Data Subject rights requests and ensuring they are actioned accordingly.
• Technology and Services is responsible for implementation and operation of appropriate processes to manage Data Subject Rights.
• Product, Process and System Owners are responsible for ensuring that the products, processes and systems/applications under their ownership are designed and implemented to facilitate the Group's compliance with the rights of Data Subjects.
• Complaints Management Function is responsible for managing complaints related to Personal Data Processing and Data Subject rights from customers and their representatives in collaboration with the relevant Business Unit or Group Function.
• HR Legal is responsible for managing complaints from Employees.

• Where the complainant or the Data Protection Authority escalates a complaint or issue relating to the handling of a Data Subject Right to the DPO, the DPO may provide advice, review and challenge on the handling of the complaint, and liaise with the Data Protection Authority.

Principle 6: The Group must ensure an appropriate level of security to protect Personal Data

The Group must implement and assess the effectiveness of Appropriate Technical and Organisational Measures to ensure protection against unauthorised or unlawful processing and against accidental alteration, loss, destruction or damage.

Appropriate Technical and Organisational Measures include physical and information security controls, to ensure a level of security appropriate to the risk to Data Subjects from the Group's Data Processing activities. The measures taken must be considered in relation to the Security and IT Risk Management policies, the state-of-the-art and costs of implementation, as well as the nature, scope, context and purpose of the Personal Data Processing.

The Group must be able to demonstrate the compliance of Personal Data Processing with the GDPR (and national data protection law where additional requirements apply) including the effectiveness of the Technical and Organisational Measures applied. In addition to and supporting the specific assessments on Personal Data Protection and Confidentiality Risk (see further Principle 1), relevant security risk assessments and regular audits must be conducted on related ERM Technology Risks so far as they apply to Personal Data Processing. Assessments must be documented.

Roles and Responsibilities for Principle 6

• Employees are responsible for following relevant governing documents connected to physical and information security, including access management, to protect the security of Personal Data used in their daily work.

• Product, Process, System and Service Owners are responsible for:

ensuring Appropriate Technical and Organisational Measures are implemented for products, processes and systems/applications under their ownership to protect the security of Personal Data and provide sufficient safeguards to protect the Rights and Freedoms of Individuals;

o ensuring appropriate security related risk assessments and periodic audits are performed.

• 1LoD (with particular relevance for risk and controls teams) are responsible for:

o provision of risk advice to Business Units and Group Functions on necessary Appropriate Technical and Organisational Measures and controls for products, processes and systems/applications that process Personal Data;

o escalation of business/legal risks to SME units where specialist input is required.

o escalation of business/legal risks to management and/or Risk Committees as appropriate in accordance with the Group's procedures.

• Technology and Services (in particular the Security Resilience and Controls team) are responsible for:

o establishing and implementing a control framework for assessing ERM Technology risks in relation to Personal Data Processing activities aligned to regulatory requirements and demonstrating that the framework is compliant;

o facilitating and overseeing risk assessments in relation to Appropriate Technical and Organisational Measures to enable the Risk Owner to treat their Technology and Data risks in relation to Personal Data Processing activities such that they are in line with the Group's risk tolerance;

o monitoring and controlling the identification, implementation and assessment of baseline controls (e.g. control catalogue) to ensure Appropriate Technical and Organisational Measures regulatory requirements are met;

o monitoring threats and vulnerabilities affecting Personal Data;

o monitoring and controlling escalations and reporting to appropriate levels of the organisation on the technological and physical security risks relating to Personal Data Processing.

Principle 7: The Group must comply with requirements relating to Data Controller and Data Processor relationships

Data Controllers in the Group must only use Data Processors that provide sufficient guarantees to implement Appropriate Technical and Organisational Measures to ensure the security of personal data and to protect the rights of the Data Subject. The Data Controller must take steps to ensure that the Data Processor only processes the Personal Data according to its instructions. Further, in accordance with the accountability principle, the Data Controller must also be able to demonstrate the steps it has taken to meet legal requirements.

The Data Controller must have a sufficient end-to-end process that includes appropriate governance and control measures to meet the legal requirements including, but not limited to, pre-contractual checks, appropriate governance, mandatory Data Processing Agreements that comply with the relevant legal requirements and include provisions for regular audits and/or inspections of the measures taken by the Data Processor to ensure compliance.

This Principle also applies to intra-Group data processing arrangements where a legal entity in the Group acts as a Data Processor for another legal entity in the Group, e.g. where NordBank acts as a Data Processor for a Group Subsidiary (the principle does not apply to processing arrangements between NordBank and its branches outside of Denmark). The legal entity acting as Data Controller must meet the obligations on Data Controllers set out above and must be able to demonstrate the steps it has taken to meet legal requirements. The legal entity acting as a Data Processor must be able to demonstrate its compliance with legal requirements and with the instructions imposed by the legal entity acting as Data Controller.

This Principle also applies where a legal entity in the Group acts as a Data Processor for a Data Controller outside of the Group. As set out above, the Group member legal entity acting as a Data Processor must be able to demonstrate its compliance with legal requirements and with the instructions

imposed by the Data Controller.

Roles and Responsibilities for Principle 7

• Contract and Service Owners, are responsible for ensuring that they meet the obligations set out in Principle 7 and for record-keeping in order to demonstrate the steps taken to meet legal requirements.

Technology and Services are responsible for the implementation of a framework to provide an end-to-end process to support Contract and Service Owners to meet the requirements when using Data Processors.

• Technology and Services Legal is responsible for legal assessment of Data Processing Agreements.

Principle 8: The Group must implement and maintain a process to manage Personal Data Breaches

The Group must implement and maintain a sufficient Personal Data Breach management process that enables compliance with the sub-principles set out below. The Personal Data Breach management process must have sufficient controls and documented governing documents.

Sub-principle 8.1: The Group must notify relevant Personal Data Breaches to the relevant Data Protection Authorities

Potential Personal Data Breaches must be reported following internal processes as soon as they are discovered.

In case of a Personal Data Breach, the Group must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the relevant Data Protection Authority about the Personal Data breach unless it is unlikely to result in a risk to the Rights and Freedoms of the Data Subject. Where the notification to the relevant Data Protection Authority is not made within 72 hours, it must be accompanied by reasons for the delay. To facilitate this requirement the Group must maintain a record of all Personal Data Breaches, including the facts relating to the breach, its effects and the remedial action taken.

Outcomes from investigations and any consequent regulatory actions must be communicated to relevant internal stakeholders.

Sub-principle 8.2: The Group must communicate Personal Data Breaches to impacted Data Subjects

Where a Personal Data Breach is likely to result in a high risk to the Rights and Freedoms of Data Subjects, or otherwise where it is deemed necessary, affected Data Subjects must be notified without undue delay.

The risk to Rights and Freedoms of Data Subjects in this context is interpreted to mean the potential negative consequences for Data Subjects – taking into consideration the severity and likelihood – including, but not limited to, risk of identity theft or fraud, financial loss, reputational damage, inconvenience and/or distress.

Roles and Responsibilities for Principle 8

• Employees are responsible for:

o ensuring that they are familiar with the concept of a Personal Data Breach

o reporting Personal Data Breaches, including potential Personal Data Breaches in a timely manner and in accordance with Group instructions.

• Leaders are responsible for ensuring that they are familiar with what constitutes a Personal Data Breach or a complaint and the procedures for reporting and handling such incidents including Personal Data Breach remediation and lessons learned and notification of Data Subjects (in collaboration with Security, Legal and Group Compliance.

• Technology and Services is responsible for the implementation and operation of appropriate Personal Data Breach management processes, including investigation and assessment of Personal Data Breach reports and notification of relevant Personal Data Breaches to Data Protection Authorities within regulatory timescales.

• The DPO is responsible for contact and cooperation with the relevant national Data Protection Authorities (in cooperation with Legal and other SME teams where appropriate) in relation to Personal Data Breaches and related inspection and enforcement matters.

• Group Compliance is responsible for reporting internally on Personal Data Breach events affecting the Group, including highlighting trends and areas of concern.

Principle 9: The Group must provide mandatory training and awareness communications to all employees concerning their responsibilities for managing Personal Data Protection and Confidentiality Risk

To raise awareness of data protection legal requirements and the management of Personal Data Protection and Confidentiality Risk, the Group must provide mandatory annual training for all employees and specialised training for employees in high-risk areas. Additional ad hoc training must be provided where risks/knowledge gaps are identified.

Completion of training must be monitored.

Roles and Responsibilities for Principle 9

• Employees are responsible for completing relevant assigned training.

• Business Units and Group Functions are responsible for documenting and monitoring the completion of training in their respective areas and developing and deploying any additional Business Unit or function-specific training on Personal Data Protection & Confidentiality Risk where deemed appropriate.

• Group Compliance is responsible for developing relevant training in relation to Personal Data Protection and Confidentiality Risk, as well as oversight of the Group's compliance with standards and requirements.

DPO is responsible for monitoring the Group's compliance with the GDPR, national data protection laws and with the Group's internal governance requirements in respect of the provision of training and awareness for employees involved in Personal Data Processing activities.

5. Escalation

Where a breach or potential breach of this Policy has been identified, an employee should notify an immediate manager, main contact in the Business Risk & Control function and Group Compliance. Where a breach of this Policy is also defined as an event, this must be registered and categorised immediately in ORIS in accordance with requirements set out in the Non-Financial Risk Event Escalation Instruction.

The Chief Compliance Officer must report to the Executive Leadership Team on significant breaches to this Policy as deemed appropriate. Significant breaches include, but are not limited to:

• Significant regulatory non-compliance with GDPR or national data protection laws;
• Inappropriate or insufficient adherence to the three lines of defence model, potentially causing ineffective management of Personal Data Protection and Confidentiality Risks to which the Group and Data Subjects are exposed;
• Interference with the independence of the Data Protection Officer in the discharge of their regulatory tasks;
• Failure to implement the Group's risk taxonomy and/or inaccurate reporting of material risks as defined by the taxonomy;
• Examples of excessive risk-taking culture or other behaviour that conflicts with the Group's desired risk culture.

Appendix 1 – Definitions

The below definitions apply to the terms used throughout this Policy.

1LoD First Line of Defence. Consists of the frontline and direct support functions.

Appropriate Technical and Organisational Measures
information security measures implemented at a technical and organisational level to ensure a level of security appropriate to the risk for the Data Subjects presented by Personal Data Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
The Appropriate Technical and Organisational Measures must take into account the state of the art, the costs of implementation and the nature scope context and purposes of processing as well as the risk of varying likelihood, and severity for the Rights and Freedoms of the Data Subject.

Business Unit a generic term that covers Personal Customers, Business Customers and Large Corporates & Institutions.

Contract Owner the individual responsible for the third party arrangements within a Business Unit / Group Function.

Data Controller a natural or legal person, public authority, agency or other body who (either alone or jointly or in common with others) determines the purposes for which, and the manner in which, any Personal Data is processed, or is to be processed.

Data Privacy Risk Assessments
methods used to identify, assess and mitigate potential Personal Data Protection and Confidentiality Risks, including risk to the Rights and Freedoms of the Data Subject presented by Personal Data Processing.
Data Privacy Risk Assessments implemented within the Group include, but are not limited to, Privacy Threshold Assessment ("PTA"), Privacy Impact Assessment ("PIA"), and Data Protection Impact Assessment ("DPIA").

Data Processing Agreement a contract or other legal act under European Union ("EU") or Member State law between a Data Controller and a Data Processor that is binding on the Data Processor with regard to the Data Controller and that sets out the subject matter and duration of the Personal Data Processing, the nature and purpose of the Personal Data Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Data Controller. The Data Processing Agreement must further meet the conditions set out in Article 28 of the GDPR.

Data Processor a natural or legal person, public authority, agency or other body, which processes Personal Data on behalf of the Data Controller.

Data Protection Authority[1] an independent public authority that supervises, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against possible violations of the General Data Protection Regulation and relevant national laws.
They are also the authority for approving Personal Data Processing if the processing is of such a nature, that their approval is needed.
There is one in each EU/EEA Member State and the United Kingdom

Data Protection By Design and By Default
a legal requirement that obliges Data Controllers and Data Processors to design and by default implement and configure,

systems, processes and products with data protection and confidentiality in mind. Data Protection By Design and By Default means that measures are put in place to ensure that Personal Data Processing complies with the Personal Data Processing Principles in the GDPR and that Appropriate Technical and Organisational Measures are applied.

Data Protection Officer ("DPO") a regulated role, with tasks defined in the GDPR. The GDPR requires that organisations such as NordBank appoint a DPO to monitor compliance, inform and advise, provide advice regarding Data Protection Impact Assessments and act as a contact point for Data Subjects and Data Protection Authorities.
The Group appoints a single DPO, except for where a local requirement or regulatory expectation requires the appointment of a local DPO (e.g. Northern Bank Ltd).

Data Subject any natural person that can be identified, directly or indirectly, whose Personal Data is processed by the Group and its Data Processors, (e.g. an employee, a customer, a guarantor, a person holding a Power of Attorney, a signatory of a company, a sole trader, etc.).
For the purposes of GDPR requirements, Data Subjects do not include deceased persons. National data protection rules may apply up to 10 years after the death of the Data Subject depending on the jurisdiction where the Personal Data Processing takes place.

Employee for the purposes of this Policy only, an Employee covers:
• an individual who is employed by the Group on a permanent or temporary basis
• an individual who is working for but is not directly employed by the Group (including consultants, contractors, agency workers, etc.)

GDPR the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)).

Group NordBank, including its branches and Subsidiaries.

Group Function covers CFO Area, Group HR, Group Internal Audit, Group Legal, Group Risk Management, Group Compliance, Group Sustainability, Stakeholder Relations, Communications & Marketing, Technology & Services.

International Transfer any Transfer of Personal Data to a Third Country or an international organisation outside the European Economic Area ("EEA"). It covers both intra-Group Transfers as well as Transfers with external parties, such as external vendors and partners of the Group, provided that one of the parties to the Transfer is located in a Third Country, including any onward Transfers of the Personal Data within a Third Country or to another Third Country.

Management Body an institution's governing body, which is appointed in accordance with national law, and is empowered to set the strategy, objectives and overall direction of the institution.

Personal Data any information concerning an identified or identifiable natural person ("Data Subject"); an identifiable Data Subject is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, identification number, address, e-mail, phone number, IP address or by means of other data such as metadata, purchases, location or payment transaction data.
Personal Data can also include references to one or more factors specific to the physical, physiological, behavioural, economic, cultural or social identity of a person.
Personal Data includes information concerning Data Subjects connected to a corporate customer or other legal persons. A Data Subject connected to a corporate customer or other legal person could be its employee, director, board member, member of partnership or a beneficial owner, etc.

Personal Data Breach a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Personal Data Processing any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated/technical 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.

Personal Data Processing Principles the seven principles for lawful processing of Personal Data listed in the GDPR: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability.

Personal Data Protection and Confidentiality Risk the risk of or incurring regulatory, criminal or administrative sanctions, material financial loss, or loss of reputation, which the Group may suffer as a result of the Group's failure to comply with laws, rules and standards applicable to its activities in relation to the protection and confidentiality of personal data.
Data Protection and Confidentiality Risk includes the risk impact to individuals resulting from the Group's activities, which results in data loss, security compromise, material financial loss or other potential detriment to individuals.

Process Owner the person accountable for the oversight of the management of a business process and its execution during its lifecycle. This includes the underlying activities of the process as well as the related business procedures and SOPs.

Product Owner the person who is overall responsible for the product during its lifecycle including the ongoing assessment and monitoring of the product.

Record of Processing a regulatory requirement whereby the Group's use of Personal Data is recorded in accordance with the requirements in Article 30 of the GDPR.

Rights and Freedoms of the Data Subject general collective term referring to the fundamental rights and freedoms of the Data Subjects.
Data Subject's rights refers in particular to the protection of Personal Data included in the Charter of Fundamental Rights of the European Union and the Data Subject's right to access and control of their Personal Data provided for in the GDPR.
Freedoms refers specifically to the absence of necessity, coercion, or constraint in choice or action over how Data Subjects exercise their rights in respect of their Personal Data.

Senior Management the most senior staff in the Group, who perform key roles. This includes the Executive Leadership Team.
When this Policy is adopted by a Subsidiary, references to Senior Management should be understood as meaning the responsibilities undertaken by the Management Body of that Subsidiary.

Service Owner the person accountable for the management of a business service and its execution during its lifecycle.

Special Categories of Personal Data Personal Data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning an Data Subject's sex life or sexual orientation.

Subject Matter Expert ("SME") general collective term referring to Employees or teams with specific expertise in legal, regulatory or subject specific areas, for example in the area of GDPR, Group Legal Data Protection and equivalent in subsidiaries, Business Risk and Control teams and Data Protection Compliance; for data/information security matters, Security, Resilience and Controls (including Technology Risk and Controls and the Data Breach Investigation Team).

Subsidiary any undertaking over which NordBank exercises control. [2]

System Owner the employee (or tribe lead within the BWOW structure) who is responsible for a system/application that processes Personal Data.

Third Country any country other than the EU and EEA Member States. For the purposes of UK data protection law, a Third Country is any country outside of the United Kingdom.

Third Party a natural or legal person, public authority, agency or body other than the Data Controller or the Data Subject to whom the Personal Data relates. For example, where NordBank is the Data Controller, Third Parties includes members of the Group that are separate legal entities (e.g. Danica Pension, Realkredit Danmark, Hypotek, Northern Bank, etc.).

Transfer the transfer, disclosure, handover, transmission of Personal Data or grant of access to a Data Processor or Data Controller (including remote access) to Personal Data.