NORD/LB

Finanzgruppe

Data protection framework policy of the NORD/LB Group
(Extract for external publication)

<u>Additional note</u>:
The data protection framework guideline is only published externally in a short version (extract). The full version of NORD/LB's Data Protection Framework Policy contains detailed internal processes, roles and decision-making processes that are necessary for the management of a systemically important bank. To ensure transparency, we provide the essential principles and structures in this compact summary. This summary provides our external stakeholders with a clear overview without presenting the entire content of the bank's internal framework. In this way, we create a balance between openness and the preservation of confidential information, which is crucial for the fulfilment of regulatory requirements and the competitiveness of NORD/LB.

1. Introduction and strategic classification

Data protection is of great strategic importance to NORD/LB. As a public bank, we are subject to comprehensive regulatory requirements derived from the GDPR, the BDSG, banking supervisory requirements and Group-wide compliance standards. The protection of personal data is an essential part of responsible corporate governance, risk management and the integrity of our processes.
In an increasingly digitalized financial world, the complexity of data processing is increasing. NORD/LB is responding to these developments with clear standards, structured procedures and a Group-wide understanding of data protection based on reliability, transparency and risk minimisation. This statement is an abstraction of our internal privacy policy intended for the public.

2. Legal and regulatory framework

NORD/LB complies with all legal and regulatory requirements that are relevant to credit institutions. These include, in particular:

- EU General Data Protection Regulation (GDPR)
- Federal Data Protection Act (BDSG)
- State data protection laws (depending on location)
- Telecommunications and Telemedia Act (TDDDG)
- Social Security Code (if applicable)
- Money Laundering Act (AMLA)
- German Banking Act (KWG)
- Banking supervisory requirements for IT and the organisation (e.g. MaRisk AT 5)

These regulatory bases oblige us to continuously develop technical and organizational measures and to monitor data protection-compliant procedures in a risk-oriented manner.

3. Protection Objectives of Data Processing

NORD/LB is guided by the following protection objectives of the GDPR and the internal data protection directive:

- Availability – Data must be accessible and usable when needed.

- Integrity – Data must be complete and unaltered.
- Confidentiality – data must only be accessible to authorized persons.
- Transparency – Data subjects must be able to see how data is being processed.
- Intervention – Data subjects must be able to influence their data.
- Non-linkability – Data must not be linked to each other without authorization.
- Data economy – No more data is processed than necessary.

4. Principles of data processing

The processing of personal data is carried out exclusively in accordance with the requirements of the GDPR, clearly defined purposes and organizational guidelines. These include:

- Legality, fairness and transparency
- Purpose limitation of processing
- Data minimization and storage limitation
- Accuracy and timeliness of the data
- Integrity and confidentiality
- Accountability and Traceability

5. Categories of personal data at NORD/LB

NORD/LB processes personal data in a variety of contexts. These include, among others:

- Identification and legitimation data
- Customer, contract and product data
- Communication and interaction data
- Financial transaction data
- Data from KYC, AML and sanctions list checks
- Log, system, and security data
- Data of employees (in the context of the employer function)

6. Purposes of data processing

Data will only be processed for clearly defined, legally permissible purposes, including:

- Fulfilment of legal and regulatory obligations
- Implementation and processing of banking and financial services
- Risk Management, Compliance, and Fraud Prevention
- IT operations and information security management
- Personnel management and organizational processes
- Communication with customers and business partners

7. Data Sharing and Disclosure

NORD/LB will only pass on data if this is permitted by law, contractually required or covered by consent. Recipient categories can be: supervisory authorities, other financial institutions, payment service providers, IT service providers, audit bodies.

8. Technical and organisational measures (TOM)

NORD/LB operates a comprehensive safety management system that includes technical, organisational and physical measures. These include:

- Encryption technologies
- Role- and authorization-based access concept
- Network Security Mechanisms and Monitoring
- Privacy by default
- Structured procedures before the introduction of new IT systems
- Physical security measures at sites

9. Retention, Archiving and Deletion

Personal data will only be stored for as long as required by law or as necessary for the respective purpose. After these deadlines have expired, the deletion or anonymization takes place according to a structured deletion concept.

10. Use of Service Providers and International Data Transfers

NORD/LB uses service providers in accordance with clear order processing standards. International data transfers are carried out exclusively on the basis of suitable GDPR guarantees.

11. Data protection governance, risk analysis and controls

Data protection is embedded in NORD/LB's control and risk management system. These include:

- Regular risk analyses and data protection impact assessments (DPIA/PIA)
- Effectiveness and adequacy reviews
- Integration into compliance and risk management processes
- Regular internal audits

12. Training, awareness and communication

NORD/LB ensures that employees are aware of and comply with their obligations under data protection law through mandatory training, target group-specific training and regular communication.

13. Handling of data protection incidents

There are structured procedures for detecting, assessing and reporting data breaches. Reports to supervisory authorities and data subjects are made in a timely manner in accordance with the GDPR.

14. Update of these principles

These principles are reviewed regularly (at least annually) and adapted to legal, technical and organisational developments. The current version will be published.