NORD/LB

Finanzgruppe

Datenschutz-Rahmenrichtlinie der NORD/LB-Gruppe
(Extrakt für externe Veröffentlichung)

<u>Zusätzlicher Hinweis</u>:
Die Datenschutz-Rahmenrichtlinie wird bankextern nur in einer Kurzversion veröffentlicht (Extrakt). Die vollständige Version der Datenschutz-Rahmenrichtlinie der NORD/LB enthält detaillierte interne Prozesse, Rollen und Entscheidungswege, die für die Steuerung einer systemrelevanten Bank notwendig sind. Um Transparenz zu gewährleisten, stellen wir die wesentlichen Prinzipien und Strukturen in dieser kompakten Kurzfassung bereit. Diese hier vorliegende Kurzfassung ermöglicht unseren externen Stakeholdern einen klaren Überblick, ohne den gesamten Inhalt des bankinternen Rahmenwerks darzustellen. So schaffen wir eine Balance zwischen Offenheit und der Wahrung vertraulicher Informationen, die für die Erfüllung aufsichtsrechtlicher Anforderungen sowie die Wettbewerbsfähigkeit der NORD/LB entscheidend sind.

1. Einleitung und strategische Einordnung

Datenschutz hat für die NORD/LB eine hohe strategische Bedeutung. Als öffentlich-rechtliches Kreditinstitut unterliegen wir umfassenden regulatorischen Anforderungen, die sich aus der DSGVO, dem BDSG, bankenaufsichtlichen Vorgaben sowie gruppenweiten Compliance-Standards ableiten. Der Schutz personenbezogener Daten ist wesentlicher Bestandteil der verantwortungsvollen Unternehmensführung, der Risikosteuerung und der Integrität unserer Prozesse.
In einer zunehmend digitalisierten Finanzwelt nimmt die Komplexität der Datenverarbeitung zu. Die NORD/LB begegnet diesen Entwicklungen mit klaren Standards, strukturierten Verfahren und einem gruppenweiten Datenschutzverständnis, das auf Verlässlichkeit, Transparenz und Risikominimierung beruht. Diese Erklärung ist eine für die Öffentlichkeit bestimmte Abstraktion unserer internen Datenschutzrahmenrichtlinie.

2. Gesetzliche und regulatorische Rahmenbedingungen

Die NORD/LB erfüllt sämtliche gesetzlichen und aufsichtsrechtlichen Vorgaben, die für Kreditinstitute relevant sind. Dazu zählen insbesondere:

- EU-Datenschutzgrundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Landesdatenschutzgesetze (abhängig vom Standort)
- Telekommunikations- und Telemediengesetz (TDDDG)
- Sozialgesetzbücher (soweit anwendbar)
- Geldwäschegesetz (GwG)
- Kreditwesengesetz (KWG)
- bankaufsichtliche Anforderungen an die IT und die Organisation (u. a. MaRisk AT 5)

Diese regulatorischen Grundlagen verpflichten uns, technische und organisatorische Maßnahmen kontinuierlich weiterzuentwickeln und datenschutzkonforme Verfahren risikoorientiert zu überwachen.

3. Schutzziele der Datenverarbeitung

Die NORD/LB orientiert sich an folgenden Schutzzielen der DSGVO und der internen Datenschutzrichtlinie:

- Verfügbarkeit – Daten müssen bei Bedarf zugreifbar und nutzbar sein.
- Integrität – Daten müssen vollständig und unverändert vorliegen.
- Vertraulichkeit – Daten dürfen nur Berechtigten zugänglich sein.
- Transparenz – Betroffene müssen erkennen können, wie Daten verarbeitet werden.
- Intervenierbarkeit – Betroffene müssen Einfluss auf ihre Daten nehmen können.
- Nicht-Verkettbarkeit – Daten dürfen nicht unberechtigt miteinander verknüpft werden.
- Datensparsamkeit – Es werden nicht mehr Daten verarbeitet als notwendig.

4. Grundsätze der Datenverarbeitung

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich im Einklang mit den Vorgaben der DSGVO, klar definierten Zwecken und organisatorischen Richtlinien. Dazu gehören:

- Rechtmäßigkeit, Fairness und Transparenz
- Zweckbindung der Verarbeitung
- Datenminimierung und Speicherbegrenzung
- Richtigkeit und Aktualität der Daten
- Integrität und Vertraulichkeit
- Rechenschaftspflicht und Nachweisbarkeit

5. Kategorien personenbezogener Daten in der NORD/LB

Die NORD/LB verarbeitet personenbezogene Daten in vielfältigen Kontexten. Dazu zählen unter anderem:

- Identifikations- und Legitimationsdaten
- Kunden-, Vertrags- und Produktdaten
- Kommunikations- und Interaktionsdaten
- Finanztransaktionsdaten
- Daten aus KYC-, AML- und Sanktionslistenprüfungen
- Log-, System- und Sicherheitsdaten
- Daten von Beschäftigten (im Rahmen der Arbeitgeberfunktion)

6. Zwecke der Datenverarbeitung

Daten werden ausschließlich zu klar definierten, rechtlich zulässigen Zwecken verarbeitet, u. a.:

- Erfüllung gesetzlicher und regulatorischer Pflichten
- Durchführung und Abwicklung von Bank- und Finanzdienstleistungen
- Risikomanagement, Compliance und Betrugsprävention
- IT-Betrieb und Informationssicherheitsmanagement
- Personalverwaltung und organisatorische Abläufe
- Kommunikation mit Kunden und Geschäftspartnern

7. Datenweitergabe und Offenlegung

Die NORD/LB gibt Daten nur weiter, wenn dies gesetzlich erlaubt, vertraglich erforderlich oder durch eine Einwilligung gedeckt ist. Empfängerkategorien können sein: Aufsichtsbehörden, andere Finanzinstitute, Zahlungsdienstleister, IT-Dienstleister, Prüfungsstellen.

8. Technisch-organisatorische Maßnahmen (TOM)

Die NORD/LB betreibt ein umfassendes Sicherheitsmanagement, das technische, organisatorische und physische Maßnahmen umfasst. Dazu gehören:

- Verschlüsselungstechnologien
- Rollen- und berechtigungsbasiertes Zugriffskonzept
- Netzwerksicherheitsmechanismen und Monitoring
- Datenschutzfreundliche Voreinstellungen („Privacy by Default“)
- Strukturierte Verfahren vor Einführung neuer IT-Systeme
- Physische Sicherheitsmaßnahmen an Standorten

9. Aufbewahrung, Archivierung und Löschung

Personenbezogene Daten werden nur so lange gespeichert, wie es gesetzlich vorgeschrieben oder für den jeweiligen Zweck erforderlich ist. Nach Ablauf dieser Fristen erfolgt die Löschung oder Anonymisierung nach einem strukturierten Löschkonzept.

10. Dienstleistereinsatz und internationale Datenübermittlungen

Die NORD/LB setzt Dienstleister nach klaren Auftragsverarbeitungsstandards ein. Internationale Datenübermittlungen erfolgen ausschließlich auf Basis geeigneter DSGVO-Garantien.

11. Datenschutz-Governance, Risikoanalysen und Kontrollen

Datenschutz ist in das Kontroll- und Risikomanagementsystem der NORD/LB eingebettet. Dazu gehören:

- Regelmäßige Risikoanalysen und Datenschutzfolgenabschätzungen (DPIA/PIA)
- Wirksamkeitskontrollen und Angemessenheitsprüfungen
- Integration in Compliance- und Risikomanagementprozesse
- Regelmäßige interne Audits

12. Schulung, Awareness und Kommunikation

Die NORD/LB stellt durch verpflichtende Schulungen, zielgruppenspezifische Trainings und regelmäßige Kommunikation sicher, dass Mitarbeitende ihre datenschutzrechtlichen Pflichten kennen und einhalten.

13. Umgang mit Datenschutzvorfällen

Es existieren strukturierte Verfahren zur Erkennung, Bewertung und Meldung von Datenschutzverletzungen. Meldungen an Aufsichtsbehörden und betroffene Personen erfolgen fristgerecht gemäß DSGVO.

14. Aktualisierung dieser Grundsätze

Diese Grundsätze werden regelmäßig (mindestens jährlich) überprüft und an rechtliche, technische und organisatorische Entwicklungen angepasst. Die aktuelle Fassung wird veröffentlicht.