

# DATA PROCESSING AGREEMENT

Agreement Reference: DPA-2025-CLOUD-001 Related MSA: MSA-2025-CLOUD-001

Date of Execution: January 15, 2025

## PARTIES

### Data Controller

- **Legal Name:** EuroFinance Bank AG
- **Legal Entity Identifier (LEI):** 529900ABCDEFGHJIJ1234
- **Data Protection Officer:** Dr. Klaus Weber
- **DPO Contact:** dpo@eurofinance.de
- **Registered Address:** Kaiserstrasse 45, 60329 Frankfurt, Germany

### Data Processor

- **Legal Name:** NordCloud Systems AG
- **Legal Entity Identifier (LEI):** 529900NORDCLD1234512
- **Data Protection Officer:** Anna Schneider
- **DPO Contact:** dpo@nordcloud.de
- **Registered Address:** Friedrichstrasse 123, 10117 Berlin, Germany

## 1. SUBJECT MATTER AND NATURE OF PROCESSING

### 1.1 Purpose of Processing

| Purpose ID | Description                              | Legal Basis            |
|------------|--|------------------------|
| PUR-001    | Provision of core banking SaaS services  | Contract performance   |
| PUR-002    | Payment transaction processing           | Legal obligation       |
| PUR-003    | Customer identity verification           | Legal obligation (AML) |
| PUR-004    | Security monitoring and fraud prevention | Legitimate interest    |
| PUR-005    | System backup and disaster recovery      | Contract performance   |

## 1.2 Nature of Processing Activities

| Activity     | Description                            |
|--------------|--|
| Collection   | Receiving data from Controller systems |
| Storage      | Secure storage in EU data centers      |
| Retrieval    | Access for service provision           |
| Organization | Structuring for efficient processing   |
| Adaptation   | Format conversion as needed            |
| Disclosure   | Transmission to authorized recipients  |
| Erasure      | Secure deletion upon termination       |

## 2. CATEGORIES OF DATA SUBJECTS

| Category                    | Estimated Volume | Description                                   |
|-----------------------------|------------------|---|
| Bank Customers (Retail)     | 500,000          | Individual account holders                    |
| Bank Customers (Corporate)  | 15,000           | Business account holders                      |
| Bank Employees              | 2,500            | Internal staff with system access             |
| Third Party Representatives | 1,000            | Authorized signatories, legal representatives |

## 3. CATEGORIES OF PERSONAL DATA

### 3.1 Data Categories Processed

| Category            | Examples                                       | Sensitivity |
|---------------------|--|-------------|
| Identification Data | Name, address, date of birth, nationality      | Standard    |
| Contact Data        | Email, phone, postal address                   | Standard    |
| Financial Data      | Account numbers, transaction history, balances | High        |
| Identity Documents  | Passport copies, ID card scans                 | High        |
| Authentication Data | Username, password hashes, MFA tokens          | High        |

| Category        | Examples                               | Sensitivity |
|-----------------|--|-------------|
| Behavioral Data | Login times, IP addresses, device info | Standard    |

### 3.2 Special Categories of Data

- **Processed:** No
- **Biometric Data:** Not applicable
- **Health Data:** Not applicable
- **Political Opinions:** Not applicable

## 4. DATA LOCATIONS

### 4.1 Storage Locations

| Data Category       | Primary Location       | Backup Location        | Country Codes |
|---------------------|------------------------|------------------------|---------------|
| Customer PII        | Frankfurt, Germany     | Amsterdam, Netherlands | DE, NL        |
| Transaction Data    | Frankfurt, Germany     | Amsterdam, Netherlands | DE, NL        |
| Authentication Data | Frankfurt, Germany     | Berlin, Germany        | DE            |
| Audit Logs          | Frankfurt, Germany     | Dublin, Ireland        | DE, IE        |
| Encrypted Backups   | Amsterdam, Netherlands | Dublin, Ireland        | NL, IE        |

### 4.2 Processing Locations

| Processing Activity             | Location               | Country Code |
|---------------------------------|------------------------|--------------|
| Primary Application Processing  | Frankfurt, Germany     | DE           |
| Secondary Processing (Failover) | Amsterdam, Netherlands | NL           |
| Security Monitoring             | Berlin, Germany        | DE           |
| Analytics Processing            | Frankfurt, Germany     | DE           |
| Backup Processing               | Amsterdam, Netherlands | NL           |

### 4.3 Data Center Certifications

| Location  | Operator             | Certifications       |
|-----------|----------------------|----------------------|
| Frankfurt | NordCloud DC         | ISO 27001, SOC 2, C5 |
| Berlin    | NordCloud DC         | ISO 27001, SOC 2, C5 |
| Amsterdam | DataCenter Europe BV | ISO 27001, SOC 2     |
| Dublin    | AWS EU               | ISO 27001, SOC 2, C5 |

## 5. INTERNATIONAL DATA TRANSFERS

### 5.1 Transfer Assessment

| Destination                | Legal Mechanism | Risk Assessment |
|----------------------------|-----------------|-----------------|
| Netherlands (NL)           | EU Member State | Low             |
| Ireland (IE)               | EU Member State | Low             |
| No third country transfers | N/A             | N/A             |

### 5.2 Transfer Safeguards

- All data remains within EEA
- No Standard Contractual Clauses required
- No Binding Corporate Rules required
- TIA (Transfer Impact Assessment) completed: December 2024

## 6. SECURITY MEASURES

### 6.1 Technical Measures

| Measure               | Implementation | Standard   |
|-----------------------|----------------|------------|
| Encryption at Rest    | AES-256        | FIPS 140-2 |
| Encryption in Transit | TLS 1.3        | PCI DSS    |
| Access Control        | RBAC with MFA  | ISO 27001  |

| Measure          | Implementation     | Standard   |
|------------------|--------------------|------------|
| Network Security | Firewalls, IDS/IPS | ISO 27001  |
| Logging          | Centralized SIEM   | SOC 2      |
| Key Management   | HSM-based          | FIPS 140-2 |

## 6.2 Organizational Measures

| Measure             | Description                             |
|---------------------|---|
| Security Training   | Annual mandatory training for all staff |
| Background Checks   | Pre-employment screening                |
| Access Reviews      | Quarterly access certification          |
| Incident Response   | 24/7 SOC with documented procedures     |
| Business Continuity | Tested annually                         |

## 7. SUB-PROCESSORS

### 7.1 Authorized Sub-Processors

| Rank | Name                 | LEI                | Services                    | Location    | Approval Date |
|------|----------------------|--------------------|-----------------------------|-------------|---------------|
| 1    | DataCenter Europe BV | 549300DCENTER12345 | Data center colocation      | Netherlands | January 2025  |
| 2    | SecureNet AG         | 549300SECNET67890  | Network security monitoring | Germany     | January 2025  |
| 3    | BackupSafe GmbH      | 549300BACKUP11111  | Encrypted backup services   | Germany     | January 2025  |

### 7.2 Sub-Processor Notification

- **Advance Notice:** 30 days minimum
- **Objection Period:** 14 days
- **Objection Process:** Written notice to DPO

## 7.3 Sub-Processor Agreements

All sub-processors bound by equivalent data protection obligations including: - Same security standards as this DPA - Audit rights passthrough - Liability provisions

---

## 8. DATA SUBJECT RIGHTS

---

### 8.1 Rights Support

| Right                   | Response Time    | Process                |
|-------------------------|------------------|------------------------|
| Access (Art. 15)        | 10 business days | Via secure portal      |
| Rectification (Art. 16) | 5 business days  | Via ticket system      |
| Erasure (Art. 17)       | 30 days          | Verified request       |
| Restriction (Art. 18)   | 5 business days  | Via ticket system      |
| Portability (Art. 20)   | 30 days          | Structured JSON export |
| Objection (Art. 21)     | 10 business days | DPO review required    |

### 8.2 Request Handling

- Processor notifies Controller within 48 hours of any DSR
  - Controller provides instructions within 5 business days
  - Processor assists with response preparation
- 

## 9. DATA RETENTION AND DELETION

---

### 9.1 Retention Periods

| Data Category       | Active Retention         | Archive Period | Total    |
|---------------------|--------------------------|----------------|----------|
| Transaction Data    | 10 years                 | 0 years        | 10 years |
| Customer PII        | Duration of relationship | 5 years        | Variable |
| Audit Logs          | 2 years                  | 5 years        | 7 years  |
| Authentication Logs | 1 year                   | 0 years        | 1 year   |

## 9.2 Deletion Upon Termination

- **Data Return:** Within 30 days in agreed format
- **Data Deletion:** Within 90 days of return confirmation
- **Deletion Certificate:** Provided upon completion
- **Backup Deletion:** Within 120 days (retention cycles)

---

## 10. AUDIT RIGHTS

### 10.1 Audit Schedule

| Audit Type               | Frequency | Notice Required |
|--------------------------|-----------|-----------------|
| On-site Inspection       | Annual    | 30 days         |
| Documentation Review     | Quarterly | 10 days         |
| Third-Party Audit Report | Annual    | On request      |
| Penetration Test Results | Annual    | On request      |

### 10.2 Audit Scope

- Technical security controls
- Organizational measures
- Sub-processor compliance
- Incident response capabilities
- Data handling procedures

---

## 11. BREACH NOTIFICATION

### 11.1 Notification Timeline

| Event              | Notification Deadline | Recipient                |
|--------------------|-----------------------|--------------------------|
| Breach Detection   | N/A                   | Processor SOC            |
| Initial Assessment | 4 hours               | Controller DPO           |
| Detailed Report    | 24 hours              | Controller DPO           |
| Full Investigation | 72 hours              | Controller + Authorities |

## 11.2 Breach Report Contents

- Nature of breach
  - Categories and volume of affected data
  - Likely consequences
  - Measures taken/proposed
  - Contact point for information
- 

## 12. LIABILITY AND INDEMNIFICATION

---

### 12.1 Liability Caps

| Scenario                                | Cap                                   |
|---|---------------------------------------|
| General liability                       | Annual contract value (EUR 2,500,000) |
| Data breach due to Processor negligence | 2x annual contract value              |
| Willful misconduct                      | Unlimited                             |

### 12.2 Indemnification

Processor indemnifies Controller against: - Regulatory fines due to Processor breach - Third-party claims from Processor violations - Costs from unauthorized sub-processor engagement

---

## 13. TERM AND TERMINATION

---

### 13.1 Duration

- **Effective Date:** February 1, 2025
- **Term:** Coterminal with MSA-2025-CLOUD-001
- **Survival:** Security and deletion obligations survive 5 years

### 13.2 Termination for Cause

Either party may terminate for: - Material breach not cured within 30 days - Insolvency or bankruptcy - Regulatory prohibition

---



# SIGNATURES

---

**For EuroFinance Bank AG (Data Controller):** Name: Dr. Klaus Weber Title: Data Protection Officer Date: January 15, 2025

**For NordCloud Systems AG (Data Processor):** Name: Anna Schneider Title: Data Protection Officer Date: January 15, 2025

---

## ANNEX A: TECHNICAL AND ORGANIZATIONAL MEASURES

---

[Detailed TOM document referenced by this DPA]

## ANNEX B: LIST OF SUB-PROCESSORS

---

[Maintained separately and updated per notification procedure]

## ANNEX C: DATA TRANSFER IMPACT ASSESSMENT

---

[Completed December 2024, available upon request]

---

*Document Classification: Confidential - Personal Data Processing Version: 1.0 Last Updated: January 15, 2025 Next Review: January 2026*