Privacy and Data Protection Policy

1- Introduction and Scope

This Policy describes how Bankingly collects, uses, processes, and protects information in the course of providing its Electronic Banking as a Service (SaaS) solutions

Bankingly operates as a Data Processor in accordance with SOC 2 standards. Our clients, the Financial Institutions (hereinafter referred to as the "FI" or the "Controller"), act as the Data Controllers and are the owners of their end users' data.

2 -Data Classification and Collection

Bankingly adheres to the principle of Data Minimization. We strictly distinguish between the data we store and the data we only process in transit.

All end-customer data is considered critical by Bankingly. No explicit categorization is applied, as all data is treated as highly important and subject to our security policies.

2.1. Stored Data (Persistent Data)

Bankingly stores only the essential information required for identity management, security, and audit purposes. This includes:

Limited Personally Identifiable Information (PII): First name, last name, phone number, and email address.

Device Information: Device identifiers, security tokens, IP addresses, and geolocation data (when applicable for fraud prevention).

Audit Logs: Activity records, access timestamps, and operational traces to ensure security compliance and traceability.

2.2. Financial Data (Not Stored / In Transit Only)

Bankingly does NOT store sensitive financial information at rest in its databases.

Types of Data: Account balances, full credit/debit card numbers, and account statements are stored in the FI's core banking system, not within Bankingly's infrastructure.

Mechanism: This information resides exclusively in the FI's Core Banking environment. Bankingly retrieves it in real time through secure channels, only after successful user authentication, for display on the front-end. Once the session ends, this information does not persist within Bankingly's infrastructure.

2.3. Additional Data

Any additional data storage required by the FI will only be performed under a specific and documented request, always respecting the principle of not storing unnecessary information for service delivery.

3- Roles and Responsibilities

3.1. Financial Institution Responsibilities (Controller)

End-User Relationship: The FI is solely responsible for obtaining user consent for data processing. The FI may perform any additional procedures outside of Bankingly before approving a user's onboarding onto the platform.

Terms and Conditions: The FI must create and manage the Terms and Conditions and Privacy Policies that end users accept in order to use the channels provided by Bankingly.

Processing Instructions: The FI determines the purposes and means of data processing.

3.2. Bankingly Responsibilities (Processor)

Process personal data solely in accordance with the documented instructions set forth in the service agreement with the FI.

Implement appropriate technical and organizational measures to ensure data security.

4 - Data Retention and Disposal

4.1. Retention Periods

Data stored by Bankingly is retained strictly for the periods established in: The Master Service Agreements (MSA) executed with the FI. Applicable legal requirements related to audit and security

logs. If the Financial Institution requires a specific retention period, it must be explicitly defined in the contract. The FI may request full database backups and apply its own data retention policies.

4.2. Deletion and Return

Upon termination of the contractual relationship or upon a specific request from the FI:

The FI may request the secure deletion (sanitization) of its users' data stored within Bankingly.

The FI may request full backups of the information in order to apply its own retention policies.

Bankingly will certify the destruction of the data once the retention period has expired or the request has been processed, unless applicable law requires its preservation.

5 - Information Security (SOC 2)

Bankingly implements security controls aligned with SOC 2 standards to protect data confidentiality and integrity:

Encryption: All data is encrypted in transit (TLS 1.2 or higher) and at rest (AES-256) for stored information.

Access Control: Access to data by Bankingly personnel is restricted under the principle of least privilege and requires multi-factor authentication (MFA).

User Authentication: Access to financial information requires user identification, an active session, and the defined security factors.

6 - Data Subject Rights (End Users)

As Bankingly is not the data owner:

Any request for access, rectification, erasure, or objection (ARCO/GDPR rights) from an end user must be directed to the Financial Institution.

Bankingly will assist the FI in responding to such requests when formally required, ensuring compliance with contractual conditions.

7 - Transfers and Sub-processors

Bankingly will not share data with third parties except:

Infrastructure providers (e.g., AWS/Azure) necessary for operations, who must also comply with applicable security standards.

Legal or judicial requirements, with prior notice to the FI where legally permitted.

Version history

Version	Date	Description	Author	Approver	Notes
1.0	Jan 07, 2026	First version	Pedro Crosta	Martin Naor	First Version