Política de Privacidad y Protección de Datos

1. Introducción y Alcance
La presente Política describe cómo Bankingly recopila, utiliza, procesa y protege la información en el curso de la prestación de sus servicios de Banca Electrónica como Servicio (SaaS).

Bankingly opera bajo el modelo de **Encargado del Tratamiento (Data Processor)** conforme a los estándares SOC 2. Nuestros clientes, las Instituciones Financieras (en adelante, "La IF" o "El Controlador"), actúan como los **Responsables del Tratamiento (Data Controllers)** y propietarios de los datos de sus usuarios finales.

2. Clasificación y Recopilación de Datos
Bankingly adhiere al principio de **Minimización de Datos**. Distinguimos estrictamente entre los datos que almacenamos y los datos que simplemente procesamos en tránsito. Todo dato de un cliente final es critico para Bankingly, no se hace una categorización explicita de los datos por ser todos considerados de alta importancia y sujetos a nuestras políticas de seguridad

2.1. Datos Almacenados (Persistentes)
Bankingly almacena únicamente la información esencial para la gestión de identidad, seguridad y auditoría. Esto incluye:

- **Información de Identificación Personal (PII) Limitada:** Nombres, apellidos, número de teléfono y dirección de correo electrónico.
- **Información de Dispositivo:** Identificadores de dispositivos, tokens de seguridad, direcciones IP y geolocalización (si aplica para prevención de fraude).
- **Logs de Auditoría:** Registros de actividad, tiempos de acceso y trazas de operaciones para cumplimiento de seguridad y trazabilidad.

2.2. Datos Financieros (No Almacenados / En Tránsito)

Bankingly **NO almacena** en sus bases de datos información financiera sensible en reposo.

- **Tipos de datos:** Saldos, números completos de tarjetas de crédito/débito, estados de cuenta se almancenan en el core de la institución financiera y no en infraestructura de Bankingly
- **Mecanismo:** Esta información reside exclusivamente en el Core Bancario de la IF. Bankingly consulta esta información en tiempo real a través de canales seguros, únicamente tras la autenticación exitosa del usuario, para su visualización en el front-end. Una vez finalizada la sesión, esta información no persiste en la infraestructura de Bankingly.

2.3. Datos Adicionales

Cualquier almacenamiento de datos adicional requerido por la IF se realizará bajo una solicitud específica y documentada, siempre respetando el criterio de no almacenar información innecesaria para la prestación del servicio.

3. Roles y Responsabilidades

3.1. Responsabilidad de la Institución Financiera (Controlador)

- **Relación con el Usuario Final:** La IF es la única responsable de obtener el consentimiento de sus usuarios (clientes/socios) para el procesamiento de datos. La IF podrá realizar cualquier procedimiento extra externo a Bankingly antes de aceptar el alta de un usuario en la plataforma.
- **Términos y Condiciones:** La IF debe generar y gestionar los Términos y Condiciones y las Políticas de Privacidad que los usuarios finales aceptan para utilizar los canales proveídos por Bankingly.
- **Instrucciones de Procesamiento:** La IF determina la finalidad y los medios del tratamiento de los datos.

3.2. Responsabilidad de Bankingly (Procesador)

- Procesar los datos personales únicamente siguiendo las instrucciones documentadas en el contrato de servicio con la IF.

- Implementar medidas técnicas y organizativas para garantizar la seguridad de los datos.

4. Retención y Disposición de Datos
4.1. Periodos de Retención
Los datos almacenados por Bankingly se retienen estrictamente durante los plazos establecidos en:

1. Los contratos de servicio (MSA) firmados con la IF.
2. Los requisitos legales aplicables a los logs de auditoría y seguridad.
3. Si la institución Financiera desean un periodo de retención especial debe estar especificado en el contrato. La IF puede solicitar backups full de la DB y aplicar su propia politia de retención de datos.

4.2. Borrado y Devolución
Al finalizar la relación contractual o tras una solicitud específica de la IF:

- La IF puede solicitar el borrado seguro (sanitización) de los datos de sus usuarios almacenados en Bankingly.
- La IF puede solicitar respaldos (backups) totales de la información para aplicar sus propias políticas de retención.
- Bankingly certificará la destrucción de los datos una vez cumplido el periodo de retención o procesada la solicitud, salvo que la ley exija su conservación.

5. Seguridad de la Información (SOC 2)
Bankingly implementa controles de seguridad alineados con SOC 2 para proteger la confidencialidad e integridad de los datos:

- **Cifrado:** Todos los datos se cifran en tránsito (TLS 1.2 o superior) y en reposo (AES-256) para la información almacenada.
- **Control de Acceso:** El acceso a los datos por parte del personal de Bankingly está restringido bajo el principio de "mínimo privilegio" y requiere autenticación multifactor (MFA).
- **Autenticación de Usuarios:** El acceso a la información financiera requiere identificación de usuario, sesión activa y factores de seguridad definidos.

6. Derechos de los Titulares de los Datos (Usuarios Finales)
Dado que Bankingly no es el propietario de los datos:

- Cualquier solicitud de acceso, rectificación, cancelación u oposición (derechos ARCO/GDPR) por parte de un usuario final debe ser dirigida a la **Institución Financiera**.
- Bankingly asistirá a la IF en la respuesta a dichas solicitudes cuando la IF lo requiera formalmente, asegurándose de que la solicitud cumpla con las condiciones contractuales.

7. Transferencias y Sub-procesadores
Bankingly no compartirá datos con terceros salvo:

- Proveedores de infraestructura (ej. AWS/Azure) necesarios para la operación, quienes también deben cumplir con estándares de seguridad.
- Requerimiento legal o judicial, previa notificación a la IF (si la ley lo permite).

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