Politique de confidentialité et de protection des données

1. Introduction et Champ d'Application

La présente Politique décrit la manière dont Bankingly collecte, utilise, traite et protège les informations dans le cadre de la fourniture de ses services de Banque Électronique en tant que Service (SaaS).

Bankingly opère selon le modèle de Sous-traitant (Data Processor), conformément aux standards SOC 2. Nos clients, les Institutions Financières (ci-après « l'IF » ou « le Responsable du traitement »), agissent en tant que Responsables du traitement (Data Controllers) et demeurent propriétaires des données de leurs utilisateurs finaux.

2. Classification et Collecte des Données

Bankingly adhère strictement au principe de minimisation des données. Nous distinguons clairement les données que nous stockons de celles que nous traitons uniquement en transit.

Toute donnée provenant d'un utilisateur final est considérée comme critique pour Bankingly. Aucune catégorisation explicite n'est appliquée, puisque toutes les données sont jugées hautement sensibles et soumises à nos politiques de sécurité.

2.1. Données Stockées (Persistantes)

Bankingly conserve uniquement les informations essentielles à la gestion de l'identité, à la sécurité et à l'audit. Cela inclut notamment :

- **Informations personnelles limitées (PII)** : prénom, nom, numéro de téléphone et adresse e-mail.
- **Informations relatives aux appareils** : identifiants de dispositifs, jetons de sécurité, adresses IP et géolocalisation (le cas échéant, à des fins de prévention de la fraude).
- **Journaux d'audit** : enregistrements d'activité, horaires d'accès et traces d'opérations, destinés à garantir la conformité en matière de sécurité et la traçabilité.

2.2. Données Financières (Non stockées / En transit)

Bankingly **NE stocke PAS** dans ses bases de données des informations financières sensibles au repos.

Types de données : soldes, numéros complets de cartes de crédit/débit, relevés de compte. Ces informations sont conservées exclusivement dans le Core bancaire de l'Institution Financière et ne sont pas hébergées dans l'infrastructure de Bankingly.

Mécanisme : ces informations résident uniquement au sein du Core bancaire de l'IF. Bankingly les consulte en temps réel via des canaux sécurisés, exclusivement après authentification réussie de l'utilisateur, et uniquement à des fins d'affichage sur le front-end.

À la clôture de la session, ces informations ne persistent pas dans l'infrastructure de Bankingly.

2.3. Données Supplémentaires

Tout stockage de données additionnelles requis par l'Institution Financière fera l'objet d'une demande spécifique et dûment documentée.

Ce stockage sera toujours réalisé dans le strict respect du principe de minimisation des données, en veillant à ne pas conserver d'informations non nécessaires à la prestation du service.

3. Rôles et Responsabilités

3.1. Responsabilité de l'Institution Financière (Responsable du traitement)

Relation avec l'utilisateur final :
L'Institution Financière est seule responsable d'obtenir le consentement de ses utilisateurs (clients/membres) pour le traitement de leurs données.

Elle peut également mettre en œuvre toute procédure complémentaire externe à Bankingly avant d'approuver l'inscription d'un utilisateur sur la plateforme.

Conditions Générales et Politiques :
L'Institution Financière est tenue de rédiger et de gérer les Conditions Générales ainsi que les Politiques de confidentialité que les utilisateurs finaux doivent accepter pour utiliser les canaux fournis par Bankingly.

Instructions relatives au traitement :
L'Institution Financière détermine les finalités et les moyens du traitement des données.

3.2. Responsabilité de Bankingly (Sous-traitant)

Traiter les données à caractère personnel uniquement conformément aux instructions documentées figurant dans le contrat de service conclu avec l'Institution Financière. Mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir la sécurité des données.

4. Conservation et Suppression des Données

4.1. Durées de Conservation

- Les données stockées par Bankingly sont conservées strictement pendant les périodes définies dans :
- Les contrats de service (MSA) signés avec l'Institution Financière.
- Les exigences légales applicables en matière de journaux d'audit et de sécurité.
- Si l'Institution Financière souhaite appliquer une durée de conservation spécifique, celle-ci devra être expressément prévue dans le contrat.
- L'Institution Financière peut demander des sauvegardes complètes de la base de données et appliquer sa propre politique de conservation des données.

4.2. Suppression et Restitution

À l'issue de la relation contractuelle ou sur demande spécifique de l'Institution Financière :

- L’Institution Financière peut demander la suppression sécurisée (sanitisation) des données de ses utilisateurs stockées par Bankingly.
- L’Institution Financière peut demander des sauvegardes complètes des informations afin d’appliquer ses propres politiques de conservation.

Bankingly certifiera la destruction des données une fois la période de conservation écoulée ou la demande traitée, sauf si la législation applicable impose leur conservation.

5. Sécurité de l’Information (SOC 2)

Bankingly met en œuvre des contrôles de sécurité alignés sur les standards SOC 2 afin de garantir la confidentialité et l’intégrité des données :

Chiffrement :
Toutes les données sont chiffrées en transit (TLS 1.2 ou version supérieure) et au repos (AES-256) pour les informations stockées.

- **Contrôle d’accès :**
  L’accès aux données par le personnel de Bankingly est strictement limité selon le principe du « moindre privilège » et requiert une authentification multifacteur (MFA).
- **Authentification des utilisateurs :**
  L’accès aux informations financières nécessite l’identification de l’utilisateur, une session active, ainsi que des facteurs de sécurité définis.

6. Droits des Personnes Concernées (Utilisateurs Finaux)

Étant donné que Bankingly n’est pas propriétaire des données :

- Toute demande d’accès, de rectification, d’effacement ou d’opposition (droits ARCO / RGPD) formulée par un utilisateur final doit être adressée à l’Institution Financière.

- Bankingly assistera l'Institution Financière dans le traitement de ces demandes lorsque celle-ci en fera la demande formelle, en veillant à ce que ladite demande soit conforme aux stipulations contractuelles applicables.

7. Transferts et Sous-traitants Ultérieurs

Bankingly ne partagera pas les données avec des tiers, sauf dans les cas suivants:

- Avec des fournisseurs d'infrastructure (par exemple AWS, Azure) nécessaires à l'exploitation des services, lesquels sont également tenus de respecter des standards de sécurité appropriés.
- En cas d'obligation légale ou de réquisition judiciaire, après notification préalable à l'Institution Financière, lorsque la loi l'autorise.

Version	Date	Description	Auteur	**Approbateur**	Notes
1.0	7 janvier 2026	Première version	Pedro Crosta	Martin Naor	Première version