

Politique de Protection des Données Personnelles (Version abrégée)

UBA Conhgo s'engage à garantir la confidentialité des informations personnellement identifiables collectées et traitées par ou pour le compte de la Banque. À cet effet, la Banque a mis en place un **Système de Management de l'Information sur la Vie Privée (PIMS)** conforme à la norme **ISO/IEC 27701**. Ce système permet à UBA Congo de veiller à la **protection et à la confidentialité** des données personnelles collectées et traitées.

La haute direction de la Banque démontre son engagement envers la protection des données personnelles en définissant des **objectifs** et des **politiques de confidentialité**, et en fournissant les ressources nécessaires pour maintenir et améliorer en continu la confidentialité au sein de la Banque.

La Banque garantit la **conformité** avec toutes les réglementations, normes et exigences contractuelles applicables en matière de sécurité de l'information.

Déclarations de la politique de confidentialité

- Toutes les **données personnelles** détenues ou contrôlées par la Banque seront traitées avec le **plus haut niveau de confidentialité et de protection**.
- UBA Congo s'engage à se conformer à **toutes les lois et réglementations applicables** à ses activités et opérations concernant la protection et la confidentialité des données.
- Toutes les données personnelles seront **classifiées** conformément à la **Politique de Classification de l'Information** de UBA Congo.

Objectifs en matière de sécurité de l'information et de protection des données personnelles

- Assurer une **gestion efficace** de la sécurité de l'information et de la protection des données personnelles au sein de la Banque, à travers un **cadre de gouvernance adapté** pour initier, piloter et contrôler leur mise en œuvre.
- Garantir que la **Direction** soutienne activement la gestion de la sécurité et de la confidentialité des données à travers :
 - l'**attribution de rôles** liés à la sécurité et à la vie privée,
 - la **coordination et l'évaluation** de la mise en œuvre des mesures de sécurité et de confidentialité à travers la Banque,
 - et la **présentation des politiques** au Conseil d'Administration pour approbation via le **Comité de Gestion des Risques**.
- Établir des **liens avec des spécialistes de la sécurité ou groupes externes**, y compris les autorités compétentes, pour :
 - suivre les **tendances du secteur**,
 - surveiller les **normes et méthodes d'évaluation**,
 - et garantir des **points de contact efficaces** lors de la gestion d'incidents.
- Favoriser une approche **pluridisciplinaire** de la sécurité de l'information et de la protection des données.

- Maintenir la **sécurité des données personnelles**, des **informations de la Banque** et des **installations de traitement de l'information**, lorsqu'elles sont accédées, traitées, communiquées ou gérées par des tiers.
- Garantir que l'introduction de **produits ou services de tiers** ne compromette pas la sécurité des données personnelles, des informations de la Banque, ni celle de ses systèmes de traitement de l'information.
- S'assurer que **l'accès aux données personnelles**, le **traitement**, ainsi que la **communication** des informations de la Banque par des tiers soient **strictement contrôlés**.
- S'assurer que toute **interaction commerciale avec des tiers**, impliquant :
 - l'accès aux données personnelles,
 - l'utilisation des systèmes ou informations de la Banque,
 - ou la fourniture ou la réception de produits/services,

fasse l'objet d'une **évaluation rigoureuse des risques**, afin d'identifier les implications sécuritaires et les exigences de contrôle associées.