



# AFRICA VENTURE GROUP

AVG BANKING SOLUTIONS - [www.banking.africaventuregroup.com](http://www.banking.africaventuregroup.com)

## CONVENTION DE CONFIDENTIALITÉ MUTUELLE

NDA pour institutions bancaires, partenaires financiers, entités réglementées et parties prenantes autorisées

Bien vouloir remplir et le retourner signer

### Objectif du document

Encadrer, de manière claire et rassurante, les échanges précontractuels et exploratoires entre Africa Venture Group et toute entité bancaire souhaitant discuter de projets liés à AVG Banking Solutions : transformation bancaire, agence phygitale, contrôle d'accès, gestion de files d'attente, parcours client, intégrations, cybersécurité, GED, SMS/WhatsApp business, données opérationnelles et solutions digitales connexes.

<b>Nature</b>	NDA mutuel / accord de confidentialité bilatéral
<b>Partie A</b>	Africa Venture Group / AVG Banking Solutions
<b>Partie B</b>	[Nom de la banque / institution financière]
<b>Date d'entrée en vigueur</b>	[dd/mm/aaaa]



## 0. Préambule et esprit de l'accord

Africa Venture Group, à travers sa business unit AVG Banking Solutions, avec ses partenaires internationaux propose une offre spécialisée d'accompagnement des institutions financières en Afrique centrale et en Afrique de l'Ouest, notamment au Cameroun, en Côte d'Ivoire, au Togo, au Congo, au Gabon, en RCA, au Tchad et bien d'autres.

Dans ce cadre, les Parties peuvent être amenées à échanger des informations stratégiques, techniques, commerciales, opérationnelles, financières, réglementaires, informatiques, documentaires ou organisationnelles, y compris des informations relatives aux parcours clients, flux agences, processus internes, solutions technologiques, architectures, besoins métiers, projets pilotes, intégrations et contraintes de sécurité.

Les Parties souhaitent établir un cadre de confiance permettant de protéger ces informations et de faciliter des échanges professionnels, responsables et sécurisés, sans créer à ce stade une obligation de conclure un contrat commercial, un partenariat ou un projet de déploiement.

La présente convention vise à permettre aux banques d'échanger avec AVG dans un cadre rassurant : les informations sensibles restent protégées, les usages sont limités aux objectifs convenus, les accès sont maîtrisés, et les discussions peuvent évoluer de manière progressive vers des diagnostics, démonstrations, pilotes ou propositions formelles.

## 1. Identification des Parties

Partie divulgateuse / réceptrice A	Partie divulgateuse / réceptrice B
<p>Africa Venture Group, agissant pour son compte et, le cas échéant, pour ses filiales, business units, représentants habilités, partenaires internationaux et équipes projet dûment autorisées.</p> <p>Adresse opérationnelle : Douala, Cameroun   Abidjan, Côte d'Ivoire   Lomé, Togo.</p> <p>Email : <a href="mailto:wecare@africaventuregroup.com">wecare@africaventuregroup.com</a></p>	<p>[Dénomination complète de la banque / institution financière]</p> <p>Adresse : [●]</p> <p>Représentée par : [●]</p> <p>Email institutionnel : [●]</p>

## 2. Définitions

Terme	Définition
Informations Confidentielles	toute information, donnée, document, conversation, démonstration, accès, note, schéma, proposition, modèle, fichier, prix, donnée client, information métier, technique, financière, opérationnelle, stratégique ou réglementaire, transmise oralement, par écrit, électroniquement, visuellement ou par tout autre moyen, avant ou après la signature du présent accord.
Partie divulgateuse	la Partie qui communique ou met à disposition une Information Confidentielle.
Partie réceptrice	la Partie qui reçoit, consulte ou accède à une Information Confidentielle.
Représentants autorisés	les dirigeants, administrateurs, salariés, consultants, conseils, auditeurs, prestataires, sous-traitants, partenaires techniques ou affiliés qui ont un besoin légitime de connaître l'information pour l'objectif prévu et sont soumis à une obligation de confidentialité au moins équivalente.



Objectif Autorisé	l'évaluation, la préparation, la négociation, le cadrage, la démonstration, le diagnostic, la conception, le pilotage ou la mise en œuvre éventuelle de services liés à AVG Banking Solutions ou à toute solution connexe d'intérêt pour l'entité bancaire.
-------------------	---

### 3. Objet et portée de la confidentialité

Le présent accord a pour objet de protéger les Informations Confidentielles échangées entre les Parties dans le cadre de discussions professionnelles relatives, directement ou indirectement, aux offres, projets, diagnostics ou services de AVG Banking Solutions.

Sont notamment concernés, sans limitation :

- les besoins métiers, parcours clients, flux d'agence, files d'attente, rendez-vous, canaux digitaux, processus de crédit, onboarding, gestion documentaire, cybersécurité, contrôle d'accès, sécurité physique et logique ;
- les architectures techniques, API, intégrations, environnements de test, exigences d'hébergement, modes de déploiement cloud, on-premise ou hybride ;
- les données ou informations relatives aux clients, collaborateurs, prestataires, agences, volumes, incidents, risques, contraintes réglementaires, projets internes et politiques de sécurité ;
- les propositions commerciales, conditions tarifaires, marges, modèles économiques, feuilles de route, roadmaps, plans de déploiement, stratégies de go-to-market ou scénarios de partenariat ;
- les informations échangées lors de réunions, appels, démonstrations, ateliers, visites de sites, partages d'écran, échanges par email, messagerie instantanée, formulaires web ou plateformes collaboratives.

### 4. Obligations principales de la Partie réceptrice

Chaque Partie, lorsqu'elle agit comme Partie réceptrice, s'engage à :

- utiliser les Informations Confidentielles exclusivement pour l'Objectif Autorisé ;
- ne pas divulguer, publier, transférer, reproduire ou mettre à disposition les Informations Confidentielles à des tiers non autorisés ;
- limiter l'accès aux seules personnes ayant un besoin professionnel légitime d'y accéder ;
- protéger les Informations Confidentielles avec un niveau de soin au moins équivalent à celui utilisé pour ses propres informations sensibles, et en tout état de cause avec un niveau de protection raisonnable et professionnel ;
- informer ses Représentants autorisés de la nature confidentielle des informations et veiller à ce qu'ils respectent des obligations au moins équivalentes ;
- ne pas contourner les finalités convenues pour exploiter les informations à des fins concurrentes, non autorisées ou préjudiciables ;
- notifier promptement l'autre Partie en cas d'accès non autorisé, perte, fuite, compromission ou suspicion raisonnable de compromission d'Informations Confidentielles.

### 5. Exclusions

Ne sont pas considérées comme Informations Confidentielles les informations que la Partie réceptrice peut démontrer par des éléments écrits raisonnables :

- étaient déjà légalement en sa possession avant leur divulgation ;
- étaient publiques ou deviennent publiques autrement que par violation du présent accord ;
- ont été reçues légalement d'un tiers non soumis à une obligation de confidentialité ;
- ont été développées indépendamment sans utilisation des Informations Confidentielles de l'autre Partie ;
- doivent être divulguées en vertu d'une obligation légale, réglementaire, judiciaire ou administrative, sous réserve de respecter l'article 10 lorsque cela est possible.

### 6. Protection renforcée des informations bancaires, données personnelles et secrets professionnels

Lorsque les informations échangées concernent une institution bancaire, un établissement financier, un client, un collaborateur, une agence, un dispositif de sécurité, une architecture informatique ou un processus réglementé, les Parties reconnaissent la sensibilité particulière de ces informations.

La Partie réceptrice s'engage notamment à :

- respecter les obligations applicables en matière de secret professionnel, secret bancaire, protection des données personnelles, cybersécurité, sécurité des systèmes d'information et conformité interne ;
- ne traiter aucune donnée personnelle au-delà de ce qui est nécessaire à l'Objectif Autorisé ;
- éviter, sauf accord écrit spécifique, l'échange de données clients nominatives, données d'authentification, informations de compte, secrets de sécurité, clés d'accès, mots de passe ou informations permettant d'identifier directement un client ;
- privilégier, lorsque possible, des données anonymisées, agrégées, fictives ou masquées pour les démonstrations, tests, ateliers et diagnostics ;
- prendre des mesures techniques et organisationnelles raisonnables pour éviter tout accès non autorisé, toute perte ou altération des informations sensibles.

Le présent modèle est conçu pour permettre des échanges préliminaires sécurisés sans exposer inutilement les données clients. Pour les phases plus avancées impliquant des données personnelles, systèmes de production ou accès techniques, un Data Processing Agreement, un protocole de sécurité, un cahier des charges ou un avenant dédié pourra être signé.

## 7. Modalités d'échange, de stockage et de sécurité

Les Parties conviennent que les échanges peuvent se faire par email professionnel, visioconférence, messagerie d'entreprise, plateforme sécurisée, formulaire web, dépôt documentaire, réunion physique ou atelier technique.

La Partie réceptrice doit éviter de stocker les Informations Confidentielles dans des environnements personnels, non sécurisés ou non maîtrisés. Les copies locales doivent être limitées au strict nécessaire. Les accès doivent être restreints, protégés par authentification appropriée et, lorsque possible, par authentification multifactorielle.

Tout accès à un environnement de test, démonstration, API, interface, système pilote ou document technique reste strictement limité aux finalités autorisées. Sauf autorisation écrite préalable, la Partie réceptrice ne doit pas effectuer de tests intrusifs, extraction massive, copie de base de données, scan de vulnérabilité, reverse engineering, contournement de sécurité ou tentative d'accès à des zones non expressément autorisées.

## 8. Démonstrations, pilotes et documents techniques

Dans le cadre de démonstrations, proofs of concept, ateliers, pilotes ou cadrages techniques, les Parties peuvent échanger des documents, captures d'écran, spécifications, comptes rendus, informations de configuration, fiches de cas d'usage, propositions d'architecture, maquettes ou accès temporaires.

Ces éléments restent confidentiels et ne peuvent être utilisés que pour l'évaluation ou la préparation du projet concerné. Aucun élément ne doit être réutilisé, reproduit, transmis à une autre entité ou intégré dans un appel d'offres, cahier des charges ou projet concurrent sans accord écrit préalable de la Partie divulgateuse, sauf lorsque l'information est devenue publique ou appartient légitimement à la Partie réceptrice.

## 9. Propriété intellectuelle et absence de licence

Chaque Partie conserve l'ensemble de ses droits, titres et intérêts sur ses Informations Confidentielles, marques, noms commerciaux, méthodologies, savoir-faire, documents, logiciels, plateformes, outils, supports, offres, modèles, architectures, propositions, données, éléments graphiques et droits de propriété intellectuelle.

Aucune disposition du présent accord ne peut être interprétée comme accordant une cession, licence, transfert de propriété, droit d'exploitation ou autorisation d'usage au-delà de l'Objectif Autorisé.

## 10. Divulgence contrainte par la loi, régulateur ou autorité compétente

Si une Partie est légalement tenue de divulguer une Information Confidentielle en vertu d'une obligation légale, réglementaire, judiciaire, administrative, prudentielle ou à la demande d'une autorité compétente, elle peut procéder à cette divulgation dans la limite strictement requise.

Dans la mesure légalement permise, elle devra informer préalablement l'autre Partie, coopérer raisonnablement pour limiter la portée de la divulgation et solliciter, lorsque possible, un traitement confidentiel des informations divulguées.



## 11. Restitution, destruction et conservation résiduelle

À la demande écrite de la Partie divulgateuse, ou à la fin des discussions si aucun projet ne se poursuit, la Partie réceptrice devra restituer ou détruire les Informations Confidentielles en sa possession, sous réserve des copies conservées pour répondre à des obligations légales, réglementaires, d'audit, de conformité, d'archivage automatique, de continuité informatique ou de preuve.

Toute copie résiduelle conservée conformément au paragraphe précédent reste soumise aux obligations de confidentialité du présent accord.

## 12. Durée

Le présent accord entre en vigueur à compter de la date de signature ou, en cas d'acceptation électronique, à compter de la date d'acceptation documentée. Il couvre également les Informations Confidentielles échangées avant cette date dans le cadre des mêmes discussions, sauf accord contraire écrit.

Sauf résiliation écrite, le présent accord est conclu pour une durée initiale de trois (3) ans. Les obligations de confidentialité survivent pendant cinq (5) ans après la fin de l'accord ou la dernière divulgation, selon la date la plus tardive. Les secrets d'affaires, secrets professionnels, secrets bancaires, informations de sécurité, informations d'architecture sensible et données personnelles restent protégés aussi longtemps que leur nature confidentielle ou les obligations légales applicables l'exigent.

## 13. Non-contournement et intégrité des discussions

Lorsque AVG présente une opportunité, une méthodologie, un cas d'usage, un partenaire technique, une architecture, une proposition ou une solution spécifique dans le cadre d'une discussion confidentielle, la Partie réceptrice s'engage à ne pas utiliser ces informations pour contourner AVG ou porter atteinte de manière déloyale à sa position dans l'opportunité concernée.

Cette clause ne limite pas le droit de la Partie réceptrice de poursuivre des relations déjà existantes, d'utiliser ses connaissances internes, de consulter le marché conformément à ses politiques d'achat ou de respecter ses obligations réglementaires et de mise en concurrence.

## 14. Absence d'obligation de conclure

Le présent accord ne crée aucune obligation pour l'une ou l'autre Partie de conclure un contrat, d'acheter une solution, d'attribuer un marché, de poursuivre une négociation, de lancer un pilote ou de formaliser un partenariat. Toute collaboration commerciale ou technique devra faire l'objet d'un contrat distinct dûment signé.

## 15. Communication externe et usage des noms

Aucune Partie ne peut utiliser le nom, le logo, la marque, les références, les visuels, les projets, les clients, les informations de collaboration ou les annonces relatives à l'autre Partie dans une communication externe, publication, communiqué, présentation commerciale, site web ou réseau social sans accord écrit préalable de l'autre Partie.

## 16. Limitation de responsabilité liée aux échanges précontractuels

Les Informations Confidentielles sont fournies dans le cadre d'échanges exploratoires et peuvent être incomplètes, évolutives ou sujettes à validation. Sauf stipulation contraire dans un contrat distinct, elles sont fournies sans garantie expresse ou implicite quant à leur exhaustivité, exactitude ou adéquation à un usage particulier.

Cette clause ne limite pas la responsabilité d'une Partie en cas de faute lourde, fraude, violation intentionnelle de la confidentialité, atteinte aux droits de propriété intellectuelle, violation de données personnelles ou manquement à une obligation légale impérative.

## 17. Signature électronique, acceptation en ligne et traçabilité

Le présent accord peut être signé manuscritement, électroniquement ou accepté via un processus en ligne permettant d'identifier raisonnablement le signataire, la date, l'entité représentée et la version du document acceptée.

Lorsque le document est téléchargé ou accepté depuis [www.banking.africaventuregroup.com](http://www.banking.africaventuregroup.com), la version mise à disposition à la date d'acceptation constitue la version applicable, sauf accord écrit contraire entre les Parties.



## 18. Droit applicable et règlement des différends

Les Parties privilégieront une résolution amiable de tout différend relatif à l'interprétation, l'exécution ou la validité du présent accord. À cette fin, elles s'engagent à organiser une réunion de bonne foi entre représentants habilités dans un délai raisonnable suivant notification du différend.

Sauf accord contraire dans un contrat ou avenant spécifique, le présent accord est régi par le droit applicable au siège opérationnel de la Partie AVG contractante et par les principes pertinents du droit des affaires applicable dans l'espace OHADA, sans préjudice des règles impératives applicables à la Partie bancaire, notamment en matière de secret bancaire, données personnelles, cybersécurité, conformité et supervision prudentielle.

Tout différend non résolu amiablement pourra être soumis, au choix convenu par les Parties : (i) aux juridictions compétentes de Douala, Cameroun ; ou (ii) à une procédure d'arbitrage ou de médiation convenue par écrit, notamment sous un règlement reconnu dans l'espace OHADA. Les Parties peuvent adapter cette clause selon le pays de la banque, la politique juridique interne et les exigences réglementaires applicables.

## 19. Dispositions diverses

- Aucune renonciation à un droit ne peut être présumée du simple fait de son non-exercice.
- Si une clause est déclarée nulle ou inapplicable, les autres clauses demeurent en vigueur et les Parties remplaceront la clause concernée par une disposition valide reflétant au mieux l'intention initiale.
- Le présent accord constitue l'intégralité de l'accord de confidentialité entre les Parties pour l'objet visé, sauf accord de confidentialité spécifique signé ultérieurement.
- Toute modification doit être faite par écrit et signée ou acceptée par des représentants habilités des Parties.
- Les obligations du présent accord bénéficient aux affiliés, business units, dirigeants, salariés, représentants et partenaires techniques autorisés des Parties lorsqu'ils interviennent dans le cadre de l'Objectif Autorisé.



## 20. Signatures

Pour acceptation et engagement :

Partie A - Africa Venture Group	Partie B - Entité bancaire / institution financière
<b>Dénomination :</b> Africa Venture Group / AVG	<b>Dénomination :</b> [Dénomination complète]
<b>Représentée par :</b> Yannick Kounga	<b>Représentée par :</b> [Nom du signataire habilité]
<b>Fonction :</b> CEO	<b>Fonction :</b> [Fonction]
<b>Adresse :</b> Douala, Cameroun   Abidjan, Côte d'Ivoire   Lomé, Togo	<b>Adresse :</b> [Adresse complète]
<b>Email :</b> <a href="mailto:wecare@africaventuregroup.com">wecare@africaventuregroup.com</a>	<b>Email :</b> [Email institutionnel]
<b>Date :</b> [dd-mm-aaaa]	<b>Date :</b> [dd-mm-aaaa]
<b>Signature :</b>	<b>Signature :</b>
<b>Cachet :</b>	<b>Cachet :</b>

## Annexe A. Catégories indicatives d'informations confidentielles

Catégorie	Exemples
Stratégie et gouvernance	Plans de transformation, priorités métiers, contraintes opérationnelles, feuilles de route, arbitrages de direction, organisation interne.
Banque et opérations	Flux d'agence, volumes, files d'attente, parcours clients, processus crédit, onboarding, réclamations, gestion documentaire, contrôle d'accès.
Technologie et sécurité	Architecture SI, API, schémas d'intégration, accès, comptes de test, configurations, journaux, vulnérabilités, exigences de sécurité.
Données et conformité	Données personnelles, données clients, informations réglementaires, exigences d'audit, contrôles internes, politiques de confidentialité.
Commercial et financier	Tarifs, marges, propositions, partenaires, conditions contractuelles, modèles économiques, opportunités de marché.
Propriété intellectuelle	Méthodologies, supports, modèles, présentations, maquettes, wireframes, documents de cadrage, livrables et contenus de démonstration.

## Annexe B. Fiche d'identification de la contrepartie

Champ	Informations à compléter
Dénomination légale	[•]
Pays / ville	[•]
Adresse complète	[•]
Nom du signataire habilité	[•]
Fonction	[•]
Email institutionnel	[•]
Téléphone / WhatsApp professionnel	[•]
Objet des discussions	[Transformation bancaire / contrôle d'accès / parcours agence / GED / cybersécurité / autre]
Personnes autorisées à participer	[Noms, fonctions, emails]
Niveau de sensibilité anticipé	[Faible / Moyen / Élevé / Réglementé]

## Annexe C. Règles pratiques recommandées pour les échanges

- Utiliser des adresses emails professionnelles, éviter les comptes personnels pour les échanges sensibles.
- Identifier les documents sensibles par la mention « Confidentiel » lorsque cela est possible.
- Limiter les destinataires au strict nécessaire et éviter les transferts non maîtrisés.
- Utiliser des données fictives, masquées ou anonymisées lors des démonstrations et tests.
- Éviter le partage de mots de passe, clés API, secrets d'authentification ou données clients réelles sans protocole dédié.
- Mettre en place un compte rendu des réunions clés afin de tracer les sujets abordés et les prochaines étapes.
- Signer un avenant technique ou un DPA avant toute manipulation significative de données personnelles ou tout accès à un environnement sensible.