POLITIQUE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

TABLE DES MATIERES

I. PRESENTATION DE MOOV AFRICA CÔTE D'IVOIRE

Moov Africa Côte d'Ivoire est une société de télécommunications exerçant ses activités en vertu d'une Licence d'exploitation des services de télécommunication. Elle opère sous le nom commercial de Moov Africa. En vue de se positionner comme un acteur majeur de l'inclusion financière, Moov Africa a créé une filiale la société Moov Money Côte d'Ivoire. Ladite filiale est agréée par la Banque Centrale des Etats de l'Afrique de l'Ouest en vertu de la décision 210-07-2019.

Dans le présent document, Moov Africa CI et sa filiale sont référencées sous le terme « l'institution ». Le nom commercial "Moov Africa", toutes les fois qu'il est employé, fait référence à la société de télécommunications et sa filiale ci-dessus citée.

II. OBJET ET CHAMP D'APPLICATION

Les enjeux de la protection des données à caractère personnel mis en place par la loi n°2013-450 relative à la protection des données à caractère personnel du 19 juin 2013 impliquent que l'institution, marque son engagement à tous les niveaux de l'organisation pour le respect de sa stratégie de traitement de données à caractère personnel.

La présente Politique établit les principes et lignes directrices en matière de conformité des traitements et des données personnelles à la législation de Côte d'Ivoire. Elle décrit également les méthodes que Moov Africa et ses filiales utilisent pour recueillir, gérer et utiliser les données personnelles. Elle s'applique à toutes les données traitées par ses différentes entités. Elle s'applique à toutes les données traitées sous la responsabilité de l'institution et pour l'exécution des produits et services qu'elle propose.

Une donnée à caractère personnel est toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique. Une donnée à caractère personnel est donc toute information permettant d'identifier directement ou indirectement une personne physique.

Elle s'adresse et est opposable à tous ceux qui rentrent ou entretiennent une quelconque relation avec l'institution dans le cadre de ses activités et notamment aux :

- Clients ;
- Distributeurs ;
- Marchands et accepteurs ;
- Détaillants ;
- Partenaires divers ;
- Sous-traitants ;
- Prospects ;

- L'ensemble des collaborateurs, dirigeants et administrateurs.

Cette politique se réfère à la politique de sécurité du système d'information de l'institution ainsi qu'au guide de sécurité des données à caractère personnel ainsi qu'à toute politique et procédure interne en vigueur susceptible d'engager la sécurité des données à caractère personnel.
Elle est susceptible d'être mise à jour, modifiée ou complétée pour prendre en compte les évolutions législatives et réglementaires, et tout changement dans l'organisation de l'institution ou dans les offres et services proposés dans le but d'en renforcer l'efficacité.

Cette Politique témoigne de l'engagement de l'institution à protéger ses clients et partenaires et à empêcher l'utilisation d'une donnée à caractère personnel à des finalités autres que celles nécessaires à ses activités, ou d'autres activités illégales.

III. CADRE REGLEMENTAIRE

La présente Politique est élaborée conformément aux normes règlementaires et légales suivantes :

- Loi N°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- Décret N° 2015-450 du 04 février 2015 fixant les modalités de dépôt des déclarations de présentation des demandes, d'octroi et de retrait des autorisations pour le traitement des données à caractère personnel ;
- Arrêté N° 511/MPTIC/CAB du 11 novembre 2014 portant définition du profil et fixant les conditions d'emploi du correspondant à la protection des données à caractère personnel.

IV. L'IDENTIFICATION DU RESPONSABLE DU TRAITEMENT

Le responsable de traitement est la personne physique ou morale, publique ou privée, tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités.
L'institution a la qualité de Responsable de traitement. En application des dispositions réglementaires, l'institution à travers son activité s'est dotée de dispositifs opérationnels efficaces et fiables pour protéger les données à caractère personnel. Pour ce faire, le dispositif se fonde sur les grands principes suivants :

- Le principe de la finalité ;
- Le principe de licéité ;
- Le principe de la transparence ;
- Le principe de la proportionnalité ;
- Le principe de la durée de conservation ;

- Le principe de la sécurité ;
- Le principe de la confidentialité ;
- Le principe de l'exactitude ;
- La désignation d'un correspondant à la protection des données à caractère personnel.

V. LES DONNEES COLLECTEES

L'institution collecte et utilise uniquement les données à caractère personnel qui sont nécessaires à son activité.
Les données qu'elle traite, sont en principe recueillies directement auprès des personnes concernées.
Toutefois, certaines données peuvent être recueillies de manière indirecte auprès des tiers.

Les différentes catégories de données que l'institution est amenée à traiter sont :

1. Les données d'identification, administratives et de contact (nom et prénoms, genre, date et lieu de naissance, photo, numéro de carte d'identité et de passeport, adresse postale, numéro de téléphone, email professionnel et/ou personnel) ;
2. Les données de localisation ;
3. Les données techniques d'identification et d'authentification notamment lors de l'utilisation des services à travers les plateformes de l'institution (logs techniques, traces informatiques, informations sur la sécurité et l'utilisation du terminal, adresse IP)
4. Les données nécessaires à la lutte contre le blanchiment d'argent et le financement du terrorisme.

Dans le cadre spécifique de la gestion des ressources humaines :

5. , les informations relatives à la situation personnelle et familiale (régime matrimonial, nombre d'enfants, situation maritale) ;

6. Les informations relatives à la formation, à l'emploi et au poste de travail (diplômes, niveau d'étude, emploi, nom de l'employeur, type de contrat de travail, date d'entrée dans l'entreprise, et Catégorie professionnelle, conditions de travail, risques professionnels) ;

7. Les dossiers de santé : coordonnées du médecin traitant, attestations médicales, feuilles de soin, dossiers médicaux, dates d'arrêt et de reprise du travail, motif de l'arrêt ;

L'institution peut être amenée à collecter des données sensibles sous réserve du

consentement explicite du client. De même, elle peut être amenée à collecter des données personnelles concernant un tiers alors qu'il n'est pas un client. Les personnes non-clientes auprès de qui l'institution est susceptible de collecter des informations sont les prospects, les mandataires, les représentants légaux, les bénéficiaires effectifs et actionnaires d'une personne morale cliente ou partenaire d'affaires, les curriculums vitae des candidats aux postes à pourvoir au sein de de l'institution.

Des notes d'information seront régulièrement adressées aux salariés et personnel prêté, sous-traitants et partenaires ayant accès aux données dans le cadre de leurs attributions, missions et prestations, en vue de leur sensibilisation.

VI. LES FINALITES DE LA COLLECTE

Les informations collectées sont utilisées pour les finalités suivantes :

- Assurer la conformité à des obligations légales et réglementaires, le respect des réglementations financières et sociales ainsi que les réponses aux demandes officielles d'autorités publiques ou judiciaires dûment autorisées ;

- Exécuter les contrats conclus avec les clients ou leur fournir des informations précontractuelles relatives aux produits et services, les assister lors de demandes de souscription, ou lors de la souscription à une offre et dans le cadre de la gestion de relation client ;

- Servir les intérêts légitimes de l' institution, afin de mettre en place et développer les produits ou services, garantir la sécurité des réseaux et des informations, optimiser la gestion des risques et défendre les intérêts de l'institution en justice, y compris à des fins de preuve de transactions ou d'opérations, prévention de la fraude et des abus et de recouvrement, enregistrement des appels téléphoniques, transmission de données à caractère personnel au sein de l'institution à des fins administratives ;

- Sauvegarder les intérêts de la personne concernée par la collecte, pour permettre de fournir des prestations complémentaires à l'initiative de l'Institution au plan social

- Personnaliser des offres commerciales (propositions commerciales) et pour proposer aux clients des produits ou services correspondant à leur situation et à leur profil.

Les données à caractère personnel ne seront utilisées qu'aux finalités pour lesquelles elles ont été recueillies.

VII. PRINCIPES DE LA POLITIQUE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Tout traitement de données à caractère personnel doit remplir certains prérequis de licéité et de finalité définis par la Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, en vue de garantir une bonne protection de la vie privée des personnes concernées.

La mise en œuvre d'un traitement de données à caractère repose sur un certain nombre de principes directeurs. La présente politique de protection des données personnelles se base sur les principes ci-après identifiés.

A- LE PRINCIPE DE LA FINALITE

La détermination d'une finalité est un critère indispensable dans le traitement d'une donnée à caractère personnel. Les données sont collectées pour des objectifs précis (finalités), portés à la connaissance des personnes concernées. Ces données ne peuvent être utilisées ultérieurement de manière incompatible avec ces finalités.
Les finalités doivent être déterminées, légitimes et explicites. Le principe de finalité permet de déterminer la pertinence des données à caractère personnel collectées. Elle permet également de fixer la durée de conservation.

B- LE PRINCIPE DE LICEITE

Le traitement de la donnée à caractère personnel doit reposer sur un fondement juridique, lequel permet au responsable de traitement de justifier l'utilisation des données à caractère personnel. En outre, la licéité est effectuée par le recueil du consentement de la personne concernée. Le traitement est considéré légitime si la personne concernée donne expressément son consentement préalable. Un traitement ne peut être mis en œuvre que s'il respecte le principe de licéité y compris la loyauté et de manière non frauduleuse. Pour ce faire, tous les traitements au sein de l'institution remplissent au moins l'une des conditions alternatives suivantes :

1. **La personne concernée a consenti au traitement** : Si le consentement est le fondement du traitement, l'institution prouvera que la personne concernée a effectivement consenti à l'opération de traitement.
2. **Le traitement est nécessaire à l'exécution d'un contrat ou de mesures précontractuelles prises à sa demande**.
3. **Le traitement est nécessaire au respect d'une obligation légale à laquelle l'institution est soumise ou à l'exécution d'une mission d'intérêt public ou relevant d'une instruction de l'autorité publique** : Le traitement a dans ce cas, son fondement dans la loi en vigueur.
4. **Le traitement est nécessaire à la sauvegarde des intérêts ou des droits fondamentaux de la personne concernée ou d'une autre personne physique**.

5. **<u>Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement ou par le destinataire</u>**, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée (par exemple : vidéosurveillance, facturation, ...).

C- LE PRINCIPE DE TRANSPARENCE

Le principe de transparence a pour objet d'informer les personnes concernées sur les modalités de traitement de leurs données à caractère personnel. Par conséquent celles-ci sont informées de : l'identité du responsable du traitement, la finalité du traitement, et les destinataires des données traitées.
Il importe également de porter à la connaissance des personnes concernées, les droits que la loi leur octroie ainsi que les modalités pratiques de l'exercice de ces droits.

Moov Africa encourage la transparence au sujet des données à caractère personnel qu'elle traite et de la finalité du traitement, tant envers la personne concernée que des autorités de surveillance. La communication menée est honnête, facilement accessible et compréhensible. Le principe de transparence est appliqué également lorsque les données à caractère personnel sont échangées avec des tierces parties.

Dans ce contexte, la présente politique sera publiée partout où besoin sera, en particulier sur le site internet de Moov Africa.

D- LE PRINCIPE DE PROPORTIONNALITE

Les données manipulées chez Moov Africa sont proportionnelles à la finalité déclarée : le principe de proportionnalité permet de s'assurer que les données traitées sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et leurs traitements ultérieurs est fermement appliqué dans les agences et autres lieux de distribution ou de ventes des produits et/ou des services de l'institution. Il s'agit des situations où ces données sont seulement utiles, mais aussi nécessaires pour l'institution de les traiter.

Moov Africa traite uniquement les données à caractère personnel strictement nécessaires ou indispensables pour l'exécution de ses activités.

E- LE PRINCIPE DE LA DUREE DE CONSERVATION

Les données collectées au sein de l'institution sont conservées conformément aux principes suivants :

- Les données doivent être conservées conformément à toutes les exigences légales, réglementaires et contractuelles applicables ;
- Les données ne doivent pas être conservées plus longtemps que nécessaire ;
- La protection des données suivant leur criticité, confidentialité, intégrité et disponibilité

doit être conforme à la classification des données.

F- LE PRINCIPE DE SECURITE

Ce Principe s'applique aux données traitées par des moyens automatisés (bases de données informatiques des Clients, etc.) ainsi qu'aux données contenues ou appelées à figurer dans un fichier non automatisé (papiers traditionnels, fichiers Word, Excel, etc.).

Les données à caractère personnel sont traitées de manière confidentielle et stockées à des endroits sécurisés.

En sa qualité de responsable de traitement, l'institution met en œuvre les mesures de sécurité logique et physique appropriées prévues lors de la mise en œuvre d'un traitement pour :

a. Empêcher l'accès de toute personne non autorisée aux bureaux et espaces de stockage utilisés pour le traitement des données sensibles (**contrôle de l'accès aux locaux avec les codes**) ;

b. Empêcher que les supports de données puissent être lus, copiés, modifiés ou retirés par des personnes non autorisées (**codes d'accès des supports de données**) ;

c. Empêcher l'introduction non autorisée ainsi que la prise de connaissance, la modification ou l'élimination non autorisées des données à caractère personnel introduites (**contrôle de l'insertion**) ;

d. Empêcher que les systèmes de traitement automatisés de données puissent être utilisés par des personnes non autorisées au moyen d'installations de transmission de données (**contrôle de l'utilisation**) ;

e. Empêcher que lors de la transmission de données à caractère personnel et du transport des supports, les données puissent être lues, reproduites, modifiées ou éliminées sans autorisation (**contrôle du transport**) ;

f. Empêcher que des systèmes de traitement de données soient utilisés à des fins de blanchiment de capitaux et de financement du terrorisme ;

g. Garantir que seules les personnes autorisées puissent avoir accès aux données visées par l'autorisation (**contrôle d'accès**) ;

h. Garantir que puisse être vérifiée et constatée l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission ;

i. Garantir qu'il soit possible de vérifier a posteriori, dans un délai approprié, en fonction de la nature du traitement à fixer dans la réglementation applicable à chaque secteur particulier, quelles données à caractère personnel sont introduites, quand elles l'ont été et pour qui (**contrôle de l'introduction**) ;

j. Assurer la sauvegarde des données par la constitution de copies de sécurité protégées.

G- LE PRINCIPE DE CONFIDENTIALITE

Toute personne agissant sous l'autorité de l'institution ou celle d'un sous-traitant de l'institution, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable hiérarchique de l'institution.

Par ailleurs, l'institution a mis en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre leur destruction accidentelle ou illicite, leur perte accidentelle, leur altération, leur diffusion ou des accès non autorisés.

Ces mesures sont assurées, compte tenu de l'état et des coûts liés à leur mise en œuvre avec un niveau de sécurité et de confidentialité approprié au regard des risques présentés par les traitements et de la nature des données à protéger.

Tout collaborateur, dirigeant, administrateur ou partenaire d'affaires de l'institution est tenu au respect de la confidentialité des données à caractère personnel en ne les divulguant pas. Toutefois, le devoir de confidentialité ne fait obstacle ni au signalement d'une alerte dans les conditions prévues par les procédures dédiées, ni aux réquisitions émanant des autorités compétentes.

H- LE PRINCIPE D'EXACTITUDE

Le principe d'exactitude implique que les données collectées en vue d'un traitement soient toujours, au-delà de leur pertinence, en faisant référence à la finalité du traitement, exemptes de toutes erreurs. L'institution met en œuvre toutes les mesures afin de s'assurer que les données sont exactes et à jour avant toute utilisation. **Toutes les données inexactes ou incomplètes, au regard des finalités pour lesquelles, elles ont été recueillies sont complétées, rectifiées ou mises à jour.**

VIII. TRANSFERT DES DONNEES VERS L'ETRANGER

Afin d'assurer la sécurité des données et de veiller à leur traitement dans des conditions conformes à la législation en vigueur, les transferts de celles-ci vers des pays étrangers sont réglementés et restreints à certaines conditions d'application, notamment le niveau de protection qu'offre le pays destinataire par rapport aux données. **Tous les transferts de données vers un pays étranger font l'objet d'une demande d'autorisation de transfert détaillée adressée à l'autorité compétente** et doivent toujours faire l'objet de clauses contractuelles imposant à la société étrangère, d'offrir à l'institution dans le cadre du transfert, des garanties de protection équivalentes à celles que la loi ivoirienne prévoit si non des garanties supérieures.

IX. LES DROITS DES PERSONNES CONCERNEES

L'institution veille au respect des droits des personnes concernées et prend toutes les mesures facilitant l'exercice de leurs prérogatives notamment des procédures intégrant le respect de ces divers droits.

A. LE DROIT A L'INFORMATION

Cette exigence est rattachée au principe de transparence en matière de traitement des données à caractère personnel, Il est le premier droit fondamental reconnu à la personne concernée. Ainsi, l'institution s'oblige à informer les personnes concernées de la finalité du traitement, des destinataires des données, du caractère obligatoire ou facultatif des réponses aux questions posées ainsi que des conséquences éventuelles d'un défaut de réponse. Cette information est faite de façon expresse et précise dans les agences et ses partenaires commerciaux.

B. LE DROIT D'ACCES

Toute personne concernée par le traitement de ses données personnelles peut interroger l'institution à ce propos et en demander, la communication sous une forme intelligible. Cependant, l'institution peut s'opposer aux demandes abusives de la même personne, notamment en raison de leur nombre, leur caractère répétitif ou systématique.

C. LE DROIT DE RECTIFICATION

La personne concernée par le traitement peut également exiger de l'institution que ses données soient actualisées, rectifiées, effacées, mises à jour ou même verrouillées dans les cas où les informations ne seraient pas correctes ou que le traitement ne serait pas conforme à la loi. L'exercice du droit de rectification permet à la personne de veiller à l'exactitude des informations la concernant.

D. DROIT D'OPPOSITION

Le droit d'opposition signifie le droit pour une personne de refuser que les données la concernant soient collectées et traitées. Le droit d'opposition pourra être mis en œuvre par la personne concernée sauf en cas de dispositions légales prévoyant expressément le traitement.

E. DROIT D'EFFACEMENT DES DONNÉES

La personne concernée dispose du droit de demander que ses données personnelles soient effacées, sans préjudice aux obligations de l'institution en termes de conservation des données. Les données à caractère personnel concernées sont celles que la personne concernée avait rendu disponible lorsqu'elle était mineure, ou pour l'un des motifs suivants :

- Les données ne sont plus nécessaires au regard de la finalité du traitement ;
- Le retrait du consentement de la personne concernée ;
- L'expiration du délai de conservation des données ;
- L'opposition légitime au traitement des données ;
- Non-conformité avec les dispositions de la loi ;
- Tout autre motif légitime.

X. LE RECOURS A LA SOUS TRAITANCE

Lorsque l'Institution recourt à un tiers pour mettre en œuvre les traitements de données à caractère personnel, ce tiers agit en qualité de sous-traitant et celui-ci doit apporter les garanties suffisantes pour la protection et la confidentialité des données pour lesquels il contracte avec elle. La vérification de l'existence de ces garanties incombe à l'Institution.

XI. DESIGNATION D'UN CORRESPONDANT A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

L'institution est organisée et prend directement en charge la surveillance ou le contrôle de l'application stricte des règles et procédures en matière de protection des données personnelles. Elle a désigné un Correspondant à la protection des données personnelles qui met en œuvre la politique de protection des données personnelles avec le support de plusieurs entités de supervision et des entités opérationnelles.
Ces entités apportent leurs ressources et compétence au correspondant à la protection des données à caractère personnel, chargé de suivre le respect des obligations en matière de protection des données à caractère personnel.

XII AUDIT ET REVUE DE LA POLITIQUE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Dans le cadre du dispositif de contrôle et d'amélioration continue, des travaux de revue sont effectués selon les plans de revue et d'audit interne annuels pour s'assurer de la pertinence et de l'adéquation de la présente Politique. Cette revue permettra de vérifier que la politique de protection des données à caractère personnel est :

a. **Complète et à jour ;**
b. **En phase avec l'évolution des lois et textes réglementaires applicables ;**
c. **Largement diffusée ;**
d. **Mise en place et en conformité avec les principes de sécurité et de confidentialité édictés par la législation en vigueur en matière de protection des données à caractère personnel.**

La revue de cette Politique de protection de données à caractère personnel a pour but de s'assurer que les principes et pratiques imposés par la loi sont bien appliqués et que l'ensemble du personnel de l'institution est bien responsabilisé.

Fait à Abidjan, le 1er octobre 2023

SIGNATURES

Le Rédacteur

Nom : Hermance GNEBLE

Fonction : Correspondant à la protection des données à caractère personnel.

Signature :

Le Responsable de traitement

Le Directeur Général

Lhoussaine OUSSALAH