

# LIGNES DIRECTRICES EN MATIERE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

## INTRODUCTION

OLEA est un leader panafricain du courtage en assurance et en réassurances qui accompagne ses clients dans la gestion de leurs risques sur le continent et déploie par ailleurs, une solution digitale de gestion maladie déléguée. Dans le cadre de ses missions, OLEA peut être amenée à accéder à des données à caractère personnel.

En tant que Responsable de Traitement, OLEA s'assure de la protection de toutes les données personnelles qui lui sont confiées dans le cadre de ses activités.

Les présentes lignes directrices en matière de protection des données à caractère personnel (ci-après les « **Lignes Directrices** ») définissent l'approche globale du Groupe OLEA en matière de protection des données à caractère personnel. Elles ont pour objet d'informer l'ensemble des collaborateurs et partenaires du Groupe OLEA sur les mesures de précautions que nous entendons respecter dans le traitement des données à caractère personnel qui nous sont confiées dans l'exercice de notre mission.

Fort de nos valeurs éthiques de respect de la vie privée, la protection des données est un enjeu majeur du Groupe OLEA. A ce titre, nous accordons la plus grande importance au respect de la vie privée, la confidentialité, la sécurité et l'intégrité de données.

La protection des données que nous confient nos clients engage également l'amélioration de notre efficacité commerciale grâce à l'exactitude et à la mise à jour régulière de nos bases clients et prospects. Cela participe au renforcement de notre image d'entreprise responsable et nous confère un avantage concurrentiel sur le continent.

Notre ambition est d'édicter des principes visant à garantir la conformité aux réglementations en vigueur en la matière dans nos différents pays d'implantation.

Ce dispositif de protection des données repose sur deux (2) piliers : (i) Le respect des droits des personnes vis-à-vis de leurs données et (ii) la mise en œuvre de mesures de sécurité.

Les principes et directives énoncés aux présentes sont appelés à être mis en pratique par l'ensemble des entités et collaborateurs du Groupe lorsqu'elles/ils interviennent dans le traitement ou le transfert des données.

## DEFINITIONS ET INTERPRETATION

« **Autorité(s) de Contrôle** » désigne les autorités publiques compétentes pour le suivi de l'application de toutes législations applicables en matière de protection des données.

« **Collaborateur(s)** » désigne tous les salariés du Groupe OLEA, actuels ou futurs, incluant les travailleurs intérimaires et les stagiaires ;

« **Délégué à la protection des données** » désigne la personne nommée au sein du Groupe OLEA, responsable de la protection des données à caractère personnel, afin de définir et transmettre les bonnes pratiques relatives à la protection des données à caractère personnel, et de garantir leur mise en œuvre.

« **Données à caractère personnel** » ou « **Donnée** » désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, à l’instar d’un nom, d’un numéro d’identification ou de données de localisation.

« **Employeur** » désigne toute société du Groupe OLEA qui embauche régulièrement toute personne physique, en application de toute loi sociale, et à qui elle assigne une tâche à exécuter et sur qui elle exerce une autorité hiérarchique.

« **Personne Concernée** » désigne une personne identifiée ou identifiable dont les données à caractère personnel font l’objet d’un traitement.

« **Responsable de Traitement** » désigne toute entité du Groupe OLEA qui seule ou conjointement avec d’autres entités, détermine les finalités, conditions et moyens affectés au traitement des données à caractère personnel.

« **Sous-Traitant** » désigne la personne physique ou morale, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du Responsable de Traitement.

« **Traitement des Données** » désigne toute opération ou ensemble d’opérations manuelles et/ou automatisées, effectuées ou non à l’aide de procédés automatiques, sur des données, comme la collecte, l’enregistrement, l’organisation, le stockage, l’adaptation ou la modification, l’extraction, la consultation, l’utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition ou de transfert, l’alignement ou la combinaison, le verrouillage, l’effacement ou la suppression.

## 1. LE RESPECT DES DROITS DES PERSONNES VIS-A-VIS DE LEURS DONNEES

### FINALITE DU TRAITEMENT DES DONNEES

Les présentes lignes directrices s’appliquent aussi bien aux traitements automatisés que manuels.

En qualité de Responsable de Traitement, les données traitées par OLEA sont celles collectées auprès des personnes concernées.

Les données doivent être collectées pour des finalités déterminées et légitimes et ne pas être traitées ultérieurement de manière incompatible avec lesdites finalités. En effet, un traitement doit avoir un objectif défini et précis, les Données traitées doivent être cohérentes au regard de l’objectif de la collecte. En conséquence, elles ne doivent pas être utilisées, transférées ou traitées ultérieurement pour des finalités autre que celles pour lesquelles elles ont été collectées.

Les données à caractère personnel doivent être recueillies de manière loyale, licite et transparente et en respect du droit à l’information de la personne concernée, sauf exceptions légales.

En conséquence, le traitement des données doit reposer sur l'un des motifs légaux suivants :

- Le consentement explicite de la personne concernée par le traitement ; ou
- Le respect d'une obligation légale ;ou
- L'exécution d'un contrat auquel la personne concernée est partie ou avant la conclusion d'un contrat à la demande de la personne concernée ; ou
- La protection des intérêts vitaux de la personne concernée ; ou
- L'exécution d'une mission d'intérêt public ; ou
- s'agissant de données de santé, si le traitement des données est nécessaire aux fins de la médecine préventive, du diagnostic médical, de l'administration de soins ou de traitements ou de la fourniture de services de santé, et doit être effectué dans des lieux où lesdites données sont traitées par un professionnel de la santé ou toute autre personne tenue au secret professionnel ou soumise à une obligation de secret équivalente en vertu de la réglementation en vigueur.
- Le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à la réglementation en vigueur.

Dans le cadre de notre activité de courtage en assurance et de gestion maladie déléguée, nous traitons les données de nos clients, prestataires et partenaires aux fins de suivi de notre relation commerciale. Le traitement nous permet notamment de procéder à :

- La gestion des contrats;
- La gestion des risques;
- La gestion et le suivi des demandes clients;
- La gestion des remboursements;
- La gestion de la comptabilité;
- Le suivi statistique ;
- Tout autre fonction support (communication, assistance juridique, audit interne).

Nous traitons également les données à des fins de développement et de gestion des ressources humaines.

### **CATEGORIES DES DONNEES**

Lorsque nous interagissons avec les personnes concernées, par voie physique ou électronique, ils peuvent être amenés à nous confier leurs données :

- Identité, état civil, données d'identification;
- Coordonnées personnelles ou professionnelles;
- Numéros de sécurité sociale ou informations d'identification sociale;
- Informations bancaires ou de facturation;
- Information d'ordre économique et financier;
- Informations de connexion à notre site et application;
- Informations relatives à l'employeur;
- Données de santé, physique ou mentale;
- Données de l'assurance maladie;
- Infractions, condamnations et mesures de sûreté;

- Informations de localisation ou de navigation sur notre application « OLEA Santé ».

A cette occasion, nous pouvons également être amenés à créer des données les concernant, à l'instar des registres ou de l'historique de navigation sur notre application.

Conformément au principe de minimisation, nous ne collectons que les données nécessaires à la réalisation de nos missions de courtage et de gestion maladie déléguée.

## **DROITS DES PERSONNES CONCERNEES**

Le Groupe OLEA garantit le plein exercice des droits des Personnes Concernées. En conséquence, chaque Collaborateur veillera au respect des obligations requises par la législation en vigueur et par l'Autorité de Contrôle compétente.

OLEA reconnaît aux personnes concernées les droits suivants :

- Le droit d'information sur la finalité du traitement de leurs données;
- Le droit d'obtenir sans limitations, à intervalles raisonnables, et sans délai ou frais excessifs, une copie de leurs données à caractère personnel traitées;
- Le droit d'obtenir la rectification, l'effacement ou le verrouillage de leurs données à caractère personnel;
- Le droit de s'opposer, à tout moment et pour des motifs impérieux légitimes et pertinents, au Traitement de leurs Données à caractère personnel, sauf si ledit Traitement est exigé par la loi. Si l'objection est justifiée, le Traitement doit être arrêté;
- le droit de s'opposer, sur demande et gratuitement, au Traitement de leurs Données à caractère personnel à des fins de prospection.

Le Délégué à la Protection des Données est le contact privilégié pour toute problématique relative au traitement des données. Il s'assure du respect des politiques mises en place en matière de protection des données, veille à la sécurité des données et aux conditions d'exercice des droits des personnes concernées.

Toute réclamation d'une personne concernée relative au traitement de ses données doit être transmise par courrier à l'adresse [dpo@olea.africa](mailto:dpo@olea.africa)

Par ailleurs, la personne concernée conserve le droit de déposer directement une plainte auprès de toute Autorité de Contrôle compétente.

## **2. LA MISE EN ŒUVRE DES MESURES DE PROTECTION**

### **MESURES DE PROTECTION DES DONNEES**

Le Groupe OLEA met en place les mesures permettant de protéger les données à caractère personnel des personnes concernées contre tout risque d'accès non autorisé et accidentel, tout traitement illégal, toute divulgation involontaire ou illégale, toute perte, toute destruction ou tout dommage.

En effet, des cas d'intrusions pourraient affecter durablement la vie personnelle des personnes concernées et entraîner des conséquences graves comme une perte des données ou une usurpation d'identité.

En conséquence, le Groupe OLEA s'emploie à mettre en œuvre des mesures de protection et, en particulier, des mesures de sécurité physiques, techniques et organisationnelles visant à garantir de manière adéquate la sécurité et la confidentialité des données des personnes concernées.

Ces mesures sont proportionnelles au risque existant et des conséquences éventuelles sur la personne concernée ainsi qu'au niveau de sensibilité des données.

### **La stricte confidentialité**

Tous les collaborateurs qui ont accès aux données doivent se conformer à la plus stricte confidentialité. En effet, chaque collaborateur joue un rôle crucial pour empêcher tout accès illicite aux données et autres informations sensibles que ce soit au niveau de l'accès aux systèmes d'information et d'applications qu'au niveau de l'accès physique aux locaux ou aux documents. La collaboration de l'ensemble des collaborateurs est essentielle à la sécurité de l'information et au respect de la vie privée des personnes concernées.

Ainsi, dès lors que les données ne sont plus utilisées par le collaborateur, ce dernier doit en assurer l'archivage ou la destruction.

### **Les règles de sécurité informatique**

Les risques d'intrusion dans les systèmes informatiques sont importants et peuvent affecter l'intégrité des données, leur perte ou leur utilisation frauduleuse. Le Groupe favorise la mise en place des précautions suivantes par les collaborateurs :

- Utiliser des antivirus régulièrement mis à jour;
- Éviter les connexions de supports mobiles à l'instar des clés USB ou disques durs externes ;
- Stocker des Données sur un espace de stockage régulièrement sauvegardé plutôt que sur les postes de travail;
- Éviter l'exécution d'applications téléchargées ne provenant pas de sources sûres ;
- Prévenir, sans délai, le département informatique en cas d'incident de sécurité ou de survenance d'un événement inhabituel touchant aux systèmes d'information et de communication de l'organisme.

### **Le poste de travail (Clean desk)**

Chaque collaborateur peut être amené à traiter des données à caractère personnel dans le cadre de l'exercice de ses fonctions. A ce titre, il est responsable de l'intégrité des données auxquelles il a accès. Afin de réduire les risques d'accès non autorisé ou d'endommagement des supports, papiers ou autres moyens physique de traitement des données, le collaborateur devra se conformer aux pratiques de « clean desk » ou « bureau propre et écran vide » suivantes :

- Ranger les espaces de travail qui doivent rester libres de papier et de désordre;
- Ranger les ordinateurs portables dans un lieu sûr à la fin de la journée de travail;
- Préserver les documents contenant les données ou toute autre information sensible de tout accès non autorisés;
- Protéger les impressions de documents contenant les Données ou toute autre information sensible;
- Ranger en lieu sûr les médias sur lesquels sont enregistrées les données tels les CD, les DVD, les disques durs externes ou les clés USB;

- Procéder, lorsque cela est requis, à la destruction sécurisée, avec broyeur, des documents contenant les données ou toute autre information sensible;
- Fermer systématiquement à clé les locaux d'archives à la fin de la journée de travail.

### **La sécurisation des locaux**

Nos lieux de travail, dans chacun de nos pays d'implantation, doivent être sécurisés et préservés de toute intrusion non-autorisée.

L'accès aux locaux doit être contrôlé pour éviter un accès non autorisé, que ce soit aux fichiers papiers ou aux matériels informatiques. A cette fin, les directions générales mettront en place des moyens de contrôle d'accès des visiteurs et des zones spécifiques d'accueil du public.

### **Le mécanisme de notification**

En cas d'altération des données ou de suspicion de tout cas d'intrusion ou de violation des principes établis par les lignes directrices, tout collaborateur pourra alerter le Délégué à la protection des données par courriel adressé à [dpo@olea.africa](mailto:dpo@olea.africa).

Le Délégué à la protection des données répondra dans les meilleurs délais en précisant les recommandations et mesures correctives à mettre en place. Il pourra faire intervenir le département informatique, le cas échéant.

### **La sensibilisation**

Le Délégué à la protection des données procédera, annuellement, à une session de sensibilisation des collaborateurs sur la sécurité des données et le respect de la vie privée.

L'objectif étant d'attirer l'attention des collaborateurs sur les exigences de la protection des données et d'assurer la mise en œuvre des principes édictés aux présentes.

## **SECURITE ET TRANSFERT DES DONNEES**

En qualité de Responsable de Traitement, OLEA met tout en œuvre pour préserver l'intégrité des données et assurer leur sécurité la plus maximale.

En conséquence, les données des personnes concernées sont susceptibles d'être transférées à un prestataire informatique externe, basé en France, offrant les garanties de sécurité et de confidentialité les plus strictes. OLEA s'assure que le sous-traitant offre les garanties suffisantes quant aux mesures de sécurité techniques et organisationnelles régissant le traitement, et s'assure que le sous-traitant respecte lesdites mesures.

Au regard du niveau de protection garanti par le sous-traitant, les données sensibles, à l'instar des données de santé, sont systématiquement hébergées par le sous-traitant.

Lorsqu'un cadre légal adéquat doit être mis en place pour que le transfert soit conforme aux législations applicables en matière de protection des données personnelles, OLEA s'assure de mettre en œuvre les démarches requises auprès de l'Autorité de Contrôle et de lui communiquer la nécessaire information sur les modalités de transfert et les mesures de sécurité garantissant l'intégrité des données hébergées à l'étranger.

## **DUREE DE CONSERVATION DES DONNEES**

La durée de conservation des données à caractère personnel traitées doit être définie selon la finalité prévue de la collecte, du transfert et du traitement des données à caractère personnel.

Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la période nécessaire à la réalisation des finalités pour lesquelles elles sont collectées. Si les données à caractère personnel collectées ne sont plus nécessaires aux fins de leur traitement, lesdites données doivent être restituées, effacées ou rendues anonymes, comme requis par la législation locale applicable en matière de protection des données.

OLEA pourra ainsi instruire tout sous-traitant de procéder à la destruction définitive des données hébergées.