GUIDELINES FOR THE PROTECTION OF PERSONAL DATA

INTRODUCTION

OLEA is a Pan-African leader in insurance and reinsurance brokerage that assists its clients in managing their risks on the continent and deploys a digital solution for delegated health management. In the course of its business, OLEA may have access to personal data.

As Data Controller, OLEA ensures the protection of all personal data entrusted to it as part of its activities.

These personal data protection guidelines (hereinafter the "**Guidelines**") define the OLEA Group's global approach to the protection of personal data. Their purpose is to inform all OLEA Group employees and partners of the precautions that we intend to observe when processing the personal data entrusted to us in the performance of our mission.

Based on our ethical values of respect for privacy, the protection of Data is a major issue for the OLEA Group. As such, we attach the utmost importance to the respect of privacy, confidentiality, security and integrity of Data.

The protection of the data entrusted to us by our customers also involves improving our commercial efficiency through the accuracy and the regular updating of our customer and prospect databases. This contributes to strengthening our image as a responsible company and gives us a competitive advantage on the continent.

Our ambition is to establish principles aimed at guaranteeing compliance with the regulations in force in our various countries of operation.

This Data protection system is based on two (2) pillars: (i) the respect of the rights of individuals regarding their Data and (ii) the implementation of security measures.

The principles and guidelines set forth herein are intended to be applied by all Group entities and employees when they are involved in the processing or transfer of Data.

DEFINITIONS ET INTERPRETATION

"Data" or **"Personal Data"** means any information relating to an identified or identifiable natural person, directly or indirectly, such as a name, an identification number or location data.

"Data Controller" means any entity of the OLEA Group which, alone or jointly with other entities, determines the purposes, conditions, and means assigned to the Processing of Personal Data.

"Data Processing" means any manual and/or automated operation or set of operations, whether performed using automatic processes, on Data, such as collection, recording, organization, storage, adaptation or modification, extraction, consultation, use, communication by transmission, diffusion, or any other form of making available or transfer, alignment or combination, blocking, deletion or suppression.

"Data Processor" means the natural or legal person, the department or any other body which processes Personal Data on behalf of the Data Controller.

"Data Protection Officer" means the person appointed within the OLEA Group, responsible for the Protection of Personal Data, in order to define and relay good practices relating to the protection of Personal Data, and to guarantee their implementation.

"**Employee(s)**" means all current or future employees of the OLEA Group, including temporary workers and interns;

"Employer" means any company of the OLEA Group which regularly hires any natural person, in application of any social law, and to whom it assigns a task to be performed and over which it exercises hierarchical authority.

"Person(s) Concerned" means an identified or identifiable person whose personal data is being processed.

"**Supervisory Authority(ies)"** means the public authorities competent to monitor the application of any applicable data protection legislation.

1. THE RESPECT FOR THE RIGHTS OF INDIVIDUALS CONCERNING THEIR DATA

PURPOSE OF DATA PROCESSING

These Guidelines apply to both automated and manual Processing.

As Data Controller, the Data processed by OLEA are those collected from the Persons Concerned.

The Data must be collected for specified and legitimate purposes and not be further processed in a manner incompatible with those purposes. Actually, a Processing must have a defined and precise objective, the Data processed must be consistent with the objective of the collection. Consequently, they must not be used, transferred or further processed for purposes other than those for which they were collected.

Personal Data must be collected in a fair, lawful and transparent manner and in compliance with the Person Concerned right to information, unless legal exceptions.

Accordingly, the Data Processing must be based on one of the following legal grounds:

- The explicit consent of the Person Concerned to the Processing; or
- Compliance with a legal obligation; or
- The performance of an agreement to which the Person Concerned is a party or prior to entering an agreement at the request of the Person Concerned; or
- The protection of the vital interests of the Person Concerned; or
- Carrying out of a mission of public interest; or
- In the case of health Data, Data Processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the supply of health services and must be carried out in places where the Data is processed by a health professional or any other person bound by professional secrecy or subject to an equivalent obligation of secrecy under the regulations in force.

- Processing for archival purposes in the public interest, for scientific or historical research or for statistical purposes, in accordance with the regulations in force.

As part of our insurance brokerage and delegated health management activity, we process the Data of our customers, service providers and partners for the purpose of monitoring our commercial relationship. The Processing allows us to deal with:

- Contract management;
- Risk management;
- Management and follow-up of customer requests;
- Management of reimbursements;
- Accounting management;
- Statistical monitoring;
- Any other support function (communication, legal assistance, internal audit).

We also process Data for human resources development and management purposes.

DATA CATEGORIES

When we interact with Persons, physically or electronically, they may entrust us with their Data:

- Identity, civil status, identification data's;
- Personal or professional contact details;
- Social security number or social identification information's;
- Banking or billing information's;
- Economic and financial information's;
- Connection information to our site and application;
- Employer information's;
- Physical or mental health data's;
- Health insurance data's;
- Offences, convictions and safety measures;
- Location or browsing information's on our *"Olea Santé"* Apps.

On this occasion, we may also be required to create Data concerning them, such as registers or browsing history on our application.

In accordance with the principle of data minimization, we only collect the Data necessary to carry out our brokerage and delegated health management missions.

RIGHTS OF PERSONS CONCERNED

The OLEA Group guarantees the full exercise of the rights of the Person Concerned. Consequently, each Employee will ensure compliance with the obligations required by the legislation in force and by the competent Supervisory Authority.

OLEA recognizes the following rights to the Person Concerned:

- The right of information on the purpose of the Processing of their Data;
- The right to obtain without limitations, at reasonable intervals, and without excessive delay or expense, a copy of their processed Personal Data;
- The right to obtain the rectification, erasure or blocking of their Personal Data;
- The right to object, at any time and for compelling legitimate and relevant reasons, to the Processing of their Personal Data, unless said Processing is required by law. If the objection is justified, the Processing must be stopped;
- The right to object, on request and free of charge, to the Processing of their Personal Data for prospecting purposes.

The Data Protection Officer is the main contact for any question relating to Data Processing. He/she ensures compliance with the policies implemented in terms of Data protection, monitors the security of the Data and the conditions for exercising the rights of the Persons Concerned.

Any complaint from a Person relating to the Processing of their Data must be sent by mail to the address dpo@olea.africa

Furthermore, the Person Concerned retains the right to file a complaint directly with any competent Supervisory Authority.

2. THE IMPLEMENTATION OF PROTECTION MEASURES

DATA PROTECTION MEASURES

The OLEA Group implements measures to protect the Personal Data of the Person Concerned against any risk of unauthorized and accidental access, any illegal Processing, any involuntary or illegal disclosure, any loss, any destruction or any damage.

Actually, cases of intrusion could permanently affect the personal life of the Persons Concerned and lead to serious consequences such as loss of data or identity theft.

Consequently, the OLEA Group is committed to implementing protective measures, in particular, physical, technical and organizational security measures aimed at guaranteeing the security and confidentiality of the Data of the Person Concerned.

These measures are proportionate to the existing risk and possible consequences for the Person Concerned and the level of sensitivity of the Data.

The strict confidentiality

All Employees who have access to the Data must comply with the strictest confidentiality. Indeed, each Employee plays a major role in preventing any illicit access to Data and other sensitive information's, whether at the level of access to information systems and applications and at the level of physical access to premises or to documents. The collaboration of all Employees is essential to the security of information and respect for the privacy of the Persons Concerned.

Thus, when the Data is no longer used by the Employee, he/she must ensure its archiving or destruction.

Computer security rules

The risks of intrusion into computer systems are significant and may affect the integrity of Data, their loss or their fraudulent use. The Group promotes the implementation of the following precautions by Employees:

- Use regularly updated anti-virus software;
- Avoid connecting mobile devices such as USB keys or external hard drives;
- Store Data on a regularly backed up storage space rather than on workstations;
- Avoid running applications downloaded from untrusted sources;
- Notify the IT department without delay in the event of a security incident or the occurrence of an unusual event affecting the organization's information and communication systems.

The workstation (Clean desk)

Each Employee may be required to process Personal Data in the performance of their duties. As such, he/she is responsible for the integrity of the Data to which he has access. In order to reduce the risk of unauthorized access or damage to media, paper or other physical means of processing Data, the Employee must comply with the following "clean desk" or "clean desk and blank screen" practices:

- Tidy the workspaces which must remain free of paper and clutter;
- Put laptops in a safe place at the end of the working day;
- Preserve the documents containing the Data or any other sensitive information from any unauthorized access;
- Protect printouts of documents containing the Data or any other sensitive information;
- Store in a safe place the media on which the Data is recorded, such as CDs, DVDs, external hard drives or USB keys;
- Proceed, when required, to the secure destruction, with a shredder, of the documents containing the Data or any other sensitive information;
- Systematically lock the archive premises at the end of the working day.

Securing the premises

Our workplaces, in each of the countries where we operate, must be secure and protected from any unauthorized intrusion.

Access to the premises must be controlled to prevent unauthorized access, whether to paper files or computer equipment. To this end, the general managements will set up visitor access control systems and specific areas for welcoming the public.

The notification mechanism

In the event of alteration of the Data or suspicion of any case of intrusion or violation of the principles established by the Guidelines, any Employee may alert the Data Protection Officer by email addressed to dpo@olea.africa

The Data Protection Officer will respond as soon as possible, specifying the recommendations and corrective measures to be put in place. The IT department will be involved, if necessary.

Awareness

The Data Protection Officer will conduct an annual session to raise awareness among Employees on Data security and respect for privacy.

The objective is to draw the attention of Employees to the requirements of Data protection and to ensure the implementation of the principles set out herein.

DATA SECURITY AND TRANSFER

As Data Controller, OLEA makes every effort to preserve the integrity of the Data and ensure its maximum security.

Consequently, the Data of the Persons Concerned may be transferred to an external IT service provider, based in France, offering the strictest guarantees of security and confidentiality. OLEA ensures that the Data Processor offers sufficient guarantees as to the technical and organizational security measures governing the Processing and ensures that the Data Processor complies with said measures.

Regarding the level of protection guaranteed by the Data Processor, sensitive Data, like health Data, is systematically hosted by the Data Processor.

When an adequate legal framework must be put in place so that the transfer complies with the applicable legislation on the protection of Personal Data, OLEA ensures that it implements the required procedures with the Supervisory Authority and communicates to it the necessary information on the transfer methods and the security measures guaranteeing the integrity of the Data hosted abroad.

DATA STORAGE DURATION

The duration period of the Personal Data Processed must be defined according to the intended purpose of the collection, transfer and Processing of the Personal Data.

Personal Data must be kept in a form allowing the identification of the Persons Concerned for a period that does not exceed the period necessary to achieve the purposes for which they are collected. If the Personal Data collected is no longer necessary for the purposes of its Processing, such Data must be returned, erased, or made anonymous, as required by applicable local data protection legislation.

OLEA may thus instruct any Data Processor to permanently destroy the hosted Data.