PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013 ("POPIA")

AWCAPE & APPLICO POPIA POLICY

INDEX

1. GENERAL

AWCape & Applico are committed to fulfil their obligations in terms of the Protection of Personal Information Act no 4 of 2013 ("POPIA"). Any personal information that is collected and processed will be done fairly and in accordance with the requirements of POPIA.

This Policy will be binding between the Company and customers where services are provided by the Company and where Personal Information is processed on behalf of the customer.

2. DEFINITIONS

2.1 **Consent**", means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information

2.2 "**Confidential information**" means any information or data….

2.3 "**Data subject**", means the person to whom Personal Information ("PI") belongs

2.4 "**De-identify**", in relation to personal information means to delete any information that –

2.4.1 Identifies the data subject,

2.4.2 Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

2.4.3 Can be linked by a reasonably foreseeable method to other information that identifies the data subject.

2.5 "**Operator**" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

2.6 "**Person**" means a natural or a juristic person

2.7 "**Personal Information**" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

2.7.1 Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person;

2.7.2 Information relating to the education or the medical, financial, criminal or employment history of the person

2.7.3 Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other assignment to the person;

2.7.4 Biometric information of the person;

2.7.5 Personal opinions, views, or preferences of the person.

2.8 **"POPIA**" means the Protection of Personal Information Act No 4 of 2013, as amended from time to time

2.9 "**Processing**" means any operation or activity or any set of operations, whether by automatic means or not, concerning personal information, including-

2.9.1 The collection, receipt, recording, collation, storage, updating or modification, retrieval, alteration, consultation, or use

2.9.2 Dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure, or destruction of information.

2.9.3 Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.

2.9.4 The views or opinions of another individual about the person; and

2.9.5 The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would revel information about the person.

2.10 "**restriction**" means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information.

2.11 "**Services**" means any supply or rendering of services by AWCape & Applico to its customers in terms of a Contract of Service whereby AWCape & Applico processes personal information of data subjects.

3. INFORMATION OFFICER

AWCape & Applico (hereinafter referred to as "the Company") have formally appointed an Information Officer and Deputy Information Officer with clearly defined responsibilities. Their contact details are disclosed at the bottom of this document.

4. COMPLIANCE COMMITTEE

4.1 The Company has established a Compliance Committee and members are responsible for information security / privacy. Regular meetings are held to ensure compliance of POPIA as well as the Promotion of Access to Information Act no 2 of 2002, as amended from time to time. The committee handles any security and privacy event that may occur and performs regular compliance evaluations on processes and systems that may impact on the business and customers.

4.2 Non-compliance is addressed and the necessary remedial actions put in place to address any problem areas.

5. CONFIDENTIALITY AGREEMENTS / NON-DISCLOSURE AGREEMENTS

5.1 Third parties are required to sign Confidentiality / Non-disclosure agreements, as per clause 7 below.

6. EMPLOYEES & CONTRACTORS

6.1 Employees and contractors are trained and kept updated of information security and privacy policies, which policies are readily available on the internal share point system.

6.2 Employees & contractors sign agreements which clearly set out the terms of the Company Policies and strict adherence thereto.

6.3 Background screenings of new employees / contractors are conducted prior to employment and access to Personal Information is restricted to those employees / contractors who are actively involved in Services for a particular data subject.

6.4 Access to such Personal Information is removed once employees / contractors leave the organization or upon finalization of a specific contract which they were involved with.

7. THIRD PARTIES / VENDORS / OPERATORS

7.1 It is mandatory for third parties / vendors / operators to sign confidentiality / non-disclosure agreements which specifically state that they are required to adhere to the Companies' policies or standards or that they have similar or stronger information security and privacy controls. The agreements describe the nature of the information that they will process and limits the processing according to the specific nature of the contract.

7.2 Should it be necessary that third parties / vendors / operators process Personal Information, written permission will be obtained from customers prior to disclosing any information to such third party / vendor / operator.

7.3 The Company constantly monitor security alerts and notifications from third parties for technologies in use within its environment.

8. SECURITY POLICIES

8.1 Physical Security Policy

8.1.1 The Company has an approved Physical Security Policy which establishes the rules for the granting, control, and monitoring of physical access.

8.1.2 The Company has identified sensitive areas within the office building and the offices are protected by security cameras, after-hour entry and logbooks. Security is monitored on an ongoing basis and there are measures in place to prevent unauthorized access to its offices, such as access codes and alarm systems with 24/7 camera monitoring.

8.2 Network Security Policy

8.2.1 Strict guidelines for computer network access are in place. Workstations are connected to Cloud servers with access control, security policy and automated backup.

8.2.2 The Company supplies and maintains Cloud Services ("Managed Cloud Services") with automated backup services. The terms and conditions of these services are regulated by a Service Level Agreement (SLA). The services and backup storage are hosted by an outside premium Internet hosting service and managed on behalf of the customer by the Company.

8.2.3 The server infrastructure is supplied as follows:

8.2.3.1 All servers come with Microsoft Windows Server 2012 R2 or 2016 Standard with Anti-Virus, Anti-Malware & Server Monitoring software included, unless otherwise specified.

8.2.3.2 Cloud Services are deployed on physical hardware. When the application software is due for a major upgrade, AWCape will, as a preventative measure, migrate the current installation to a new server to ensure a clean and fresh environment that is deployed on new hardware, thereby ensuring improved efficiencies.

8.3 Backup Services (Personal Information)

All relevant and required data is backed up from servers using two off-site backup service providers. This includes Sage related data. Data stored on OneDrive and Sharepoint is automatically backed up by Microsoft.

8.4 Backup Services (Managed Cloud Servers)

8.4.1 Online off-site backup services are supplied as mandatory and may be expanded to include all PCs in the organization. This backup option has a high Recovery Time Objective (estimated 6 days) as Disaster Recovery involves rebuilding the Managed Cloud Server from a blank slate.

8.4.2 Customers are solely and exclusively responsible for the selection of data to backup and for verifying that the correct data is being backed up on an on-going basis. Any actions of Company employees in selecting data will be deemed to have been on instruction from the Managed Cloud Subscriber and in assisting the Managed Cloud Subscriber in setting up a valid back up selection.

8.5 Additional Backup Services (Managed Cloud Servers)

8.5.1 Additional backup service options are also available, i.e.

8.5.1.1 Daily Full System Backup (FSB) to capture current state of the system, which can be restored to a new server; and

8.5.1.2 Estimated 2 hourly SQL transaction log (TL) backups to backup transactions being done between daily backups.

8.6 Passwords

The Company has an approved Password Security Policy, which is constantly enforced. Due to the size of the Company, there is no need for a formal Service Desk to assist with resetting passwords.

8.7 Passwords (Managed Cloud Services)

8.7.1 Passwords and encryption keys (for backups) will be automatically allocated to the customers' account, alternatively the customer may assign the required password and encryption key. It is required from Cloud Subscribers that they keep passwords confidential and immediately notify the Company if any unauthorized third party becomes aware of a password or if they become aware of any unauthorized use of the password and breach of security.

8.7.2 Managed Cloud Subscribers certify that any person to whom its password and encryption key is disclosed is authorized to act as its agent for purposes of using the service.

8.7.3 Passwords / Access passwords to Managed Cloud Services are periodically changed and recorded by the Company.

8.7.4 Managed Cloud Subscribers are responsible for any loss or damage they may suffer resulting from loss of confidentiality/access to MCS Account and the Company shall not be responsible for any unauthorized access to or alteration of transmissions or data, any material or date sent or received, or any transactions or agreements entered into through the use of the Managed Cloud Services.

8.8 Firewalls

Servers all run the latest MS Windows firewalls. No additional network firewalls and all software, i.e. Windows firewall, Defender, and others, are routinely updated. This does not link to third parties.

8.9 Remote access

The Company uses secure remote access mechanisms to allow access for remote users into the internal network.

8.10 Logical Access Control Policy

The Company has an approved Logical Access Control Policy, which regulates interactions with computer systems and data through access control systems. This entails identification, authentication, and authorisation protocols.

8.11 Application Security Policy

8.11.1 The Company has an approved Application Security Policy even though application / development is limited within the Company. User roles and access to development tools are limited and controlled through admin users. The separation of quality assurance, development, pre-production, and production environments is limited by customers' development standards provides.

8.11.2 Systems and processes are in place to update the patch levels of all infrastructure relevant to information assets, as well as to secure configuration standards for all infrastructure relevant to information assets.

8.12 Malware & Vulnerability scans

8.12.1 The Company sells and supports only packaged solutions with no development or production line.

8.12.2 As only Sage & Microsoft software are sold and supported, there is no requirement for security coding techniques, Application Security Assessments or Security testing.

8.12.3 Systems and processes to detect and prevent malware on infrastructure is part of the Cloud Services Supplier agreement.

8.12.4 Apart from keeping security software up to date, there are no further processes and steps regarding vulnerability scans on external and internal networks.

8.13 Security Information and Event Management (SIEM)

The Company has never done client integration with the customer's SIEM.

8.14 Business continuity and disaster recovery plans

8.14.1 The Company has RAID functionality for all servers. For issues beyond RAID backups, there are daily off-site backups of all important data which can be brought back online immediately.

8.14.2 For catastrophic failures, all new hardware, OS & system software as well as backups can be brought up in 24-48 hours. Xneelo can provide new hardware in a new location if it is a site wide failure.

8.14.3 Daily backups are done of all nominated servers' data, which would usually include Sage and customers' private information. Randomized backup restores are tested monthly.

8.15 Disaster Recovery (Managed Cloud Services)

Disaster recovery is dependent on the environment and backup service that is chosen. It entails the restoration of functionality to a previous state in time. The Recovery Time Objective is the time taken from the disaster to the system being functional. The Recovery Point Objective is the point in time to which the system should be restored and defines what the "acceptable loss" is.

9. PROTECTION OF PERSONAL INFORMATION

The Company has measures in places to protect the confidentiality and integrity of personal Information, as well as to review information security of a third party and evaluate their level of privacy.

9.1 Privacy of Personal Data

9.1.1 Customers consent to the processing of Personal Data by the Company and their respective employees, subcontractors, and third parties as provided in this Policy. Before providing Personal Data to the Company, Customers will obtain all required consents from third parties (including Customer's contacts, Partners, distributors, administrators, and employees) under applicable privacy and data protection laws.

9.1.2 Necessary security controls are in place when the Personal Information is transferred.

9.1.3 The Company will only process Personal Information of customers in connection with specific, explicitly defined, and lawful purposes related to a Service rendered for a specific Customer.

9.1.4 For purposes of the provision of such services, the Company will act as its customers' Operator, as defined in clause 2 above.

9.2 Incident Management Plan

9.2.1 The Company has a formal documented incident management plan in place and, should any security or privacy event occur involving customers' Personal Information, it will be possible to identify the individual(s) whose personal information may have been compromised.

9.2.2 The Plan is reviewed on a regular basis to ensure that requirements in terms of the Protection of Information Act (POPI) are complied with.

9.3 Customer contracts

9.3.1 Contracts describe the nature of the customer Personal Information that it retains or will process, including the limitations of such processing. The nature of the Personal Information varies between different customer requirements.

9.3.2 Inventories are kept of personal information in the Company's possession and no personal information is transferred to third parties without the necessary security controls.

9.3.3 Written permission is obtained from customers prior to processing / storing their personal information in countries outside of South Africa.

9.3.4 Daily backups are made of all nominated servers' data, which would include customers' Personal Information. Randomized backup restores are done monthly.

9.3.5 By virtue of nature of the business, the Company implements systems on behalf of clients. Client Personal Information is stored on the Company environment before moving this to live. The Personal Information is de-identified once the project is completed.

9.3.6 Once a contract with a customer is terminated, any Personal Information in Company possession will either be de-identified or handed back to the customer, depending on the customer's choice.

9.3.7 Personal Information in the possession of third parties are de-identified.

9.4 **Breaches**

9.4.1 Any detected breaches will be reported to the Information Officer or Deputy Information Officer and managed appropriately in accordance with POPIA.

9.4.2 Customers will be informed as soon as possible of any breach or incident involving their Personal Information if it may reasonably believe that any unauthorized person has accessed or acquired any Personal Information.

9.4.3 Customers will be kept abreast of investigations into such breach or incident and subsequent steps taken to remedy such breach or incident.

9.4.4 The Company will inform the Information Regulator about such breach or incident as well as remedial steps taken.

9.4.5 Inventories are kept of personal information in the Company's possession and no personal information is transferred to third parties without the necessary security controls.

9.4.6 The Company ensures that written permission is obtained from customers prior to processing / storing their personal information in countries outside of South Africa.

9.5 Requests and complaints

9.5.1 The Company has formal procedures in place regarding processing of questions, complaints, and requests for access to / correction and processing of Personal Information.

9.5.2 Upon request from a data subject, the request / complaint is forwarded to the Information Officer / Deputy Information Officer and escalated to the Compliance Committee.

9.5.3 The legal representative, a member of the committee, will take control of the request / complaint and follow the formal procedures, once the identity of the person requesting the information is confirmed by proof in the form of the identity document / passport.

9.5.4 The Company will thereafter follow the instructions from the data subject regarding the processing / further processing of the personal information.

10. INDEMNITY

The Company will hold its customers harmless from any and all losses arising from, or in connection with, any claim or action arising from the Company's negligent breach of its obligations with respect to Confidential and Personal Information.

11. CONTACT US

For further information, please contact:

Information Officer
Henri Hattingh
Henri.hattingh@awcape.co.za
Tel: 082 371 3127

Deputy Information Officer
Jeff Ryan
Jeff.Ryan@awcape.co.za
Tel: 079 138 1442