



ONGEZA LIFE (PTY) LTD

TRADING AS

ONGEZA LIFE

RETENTION & DESTRUCTION POLICY

Retention and Destruction Policy

1. PURPOSE

This policy defines Ongeza Life (Pty) Ltd's ("Ongeza Life") obligations regarding the retention of personal information and data collected, held and processed by Ongeza Life in accordance with POPI and other relevant legislation.

Ongeza Life only maintains records and information for legal or legal business reasons and always adheres to the laws, standards and best practices of SA.

The question of how long personal information should be kept from a specific entity is not clear in South Africa. This policy therefore describes the types of personal data held by Ongeza Life, the period for which that personal information is to be retained, the criteria for determining and reviewing such period, and when and how it was removed or otherwise disposed of.

2. SCOPE

This policy applies to all Ongeza Life employees, contractors, vendors and agents. This policy applies to remote access connections used to do work on behalf of Ongeza Life including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Ongeza Life networks.

3. PRINCIPALS

- Ongeza Life must collect personal information about employees, workers or individuals we have a business relationship with in order to carry out our daily business functions and activities efficiently and with satisfaction, and to provide the services determined by our business type. This information may include, but is not limited to, name, address, email address, date of birth, identification number, private and confidential information, sensitive information and banking details.
- In addition, it may sometimes be necessary for Ongeza Life to collect certain types of personal information to comply with the requirements of the law and / or regulations.
- Ongeza Life is committed to the secure processing and retention of any confidential and information assets in accordance with contractual and legal obligations and that Ongeza Life does so in an ethical and consistent manner. Ongeza Life confirms that its approach and procedures comply with POPI laws and regulations and that staff are trained and advised accordingly on the procedures and controls in place.

3.1 RETENTION OF PERSONAL INFORMATION

- Protection Of Personal Information Act No.4 of 2013 "POPI" obliges the companies as a data controller to process personal data fairly and not to hold the data for a longer period than is necessary to achieve those goals.
- Furthermore, records will be retained to provide information on, and proof of Ongeza Life's transactions, customers, employment and activities.
- Ongeza Life's data retention objectives and principles are to:

Retention and Destruction Policy

- set boundaries for retaining personal data and ensuring compliance;
 - ensure that Ongeza Life fully meets its obligations and rights of data under POPI;
 - secure protection of confidential data and its information assets;
 - ensure that records and documents are retained for the legal, contractual and regulatory period set in accordance with the rules of terms of each body.
- Ongeza Life systematically maintains data records in a manner that meets POPI's requirements. This policy is widely disseminated to ensure a standardized approach to data retention and record management.
 - Records will be retained to provide information on, and proof of, Ongeza Life's transactions, customers, employment and activities.
 - Documents are always stored in a secure platform and server with authorised personnel being the only people who have access to it.

3.2 DESTRUCTION OF PERSONAL INFORMATION

Retention and destruction rules applies to both hard copies/documents, as well as electronic versions Ongeza Life must consciously think about, and in some instances completely overhaul, how and in what manner they destroy or delete personal information and whether such processes meet muster as required by the test established by POPIA in terms of section 14(5).

In certain instances, Ongeza Life may consider taking the easy route out and hire a reputable company to destroy the hard copy or electronic data for them. Ongeza Life should exercise caution on this approach as in such instances it is the organisation's responsibility to ensure that such a company is compliant with POPIA when such data is destroyed and deleted, as in instances of a data beach, both the company providing the service and the organisation could be held liable in terms of POPIA.

In light of POPIA, the onus is on Ongeza Life to ensure that personal information is sufficiently destroyed and deleted.

Any actions undertaken by Ongeza Life to destroy or delete personal information will be under scrutiny should such processes not at a minimum ensure that the personal information is destroyed or deleted in a manner that prevents its reconstruction in an intelligible form.

So therefore, disposing of personal information by recycling or deleting a file electronically may not in the face of POPIA be enough as some remanence of that personal information may be retained. It is therefore incumbent upon Ongeza Life to take control of the manner in which personal information is disposed of and to ensure that appropriate mechanisms within Ongeza Life established to address potential risks.

Retention and Destruction Policy

- All information of a confidential or sensitive nature on paper or electronic media must be destroyed when it is no longer needed. This ensures compliance with POPI and the duty of confidentiality that Ongeza Life owes to its employees, customers and members.
- Shredding machines and confidential waste disposal units are made available throughout the building and where Ongeza Life uses service providers, regular collection takes place to ensure that confidential data is disposed of properly.
- Personal or sensitive paper-based information should not only be discarded in a trashcan. Such documents must first be processed in a specific way by shredding method. Documents that do not contain confidential information can be destroyed in the usual way.
- Under certain circumstances, data subjects have the right to request that their personal data be deleted. Data subjects have the right to delete personal data only and to prevent processing if any of the following conditions apply:
 - where the personal data is no longer needed for the purpose for which it was originally collected;
 - when the individual withdraws consent;
 - when there is no relevant legitimate interest in the continued processing;
 - the personal data has been processed illegally; or
 - extermination is required by law.

The following table serves as a guide to facilitate the decision-making of retention periods for the types of information. The data subject is the original source of, and the subject of the information, and thus also owns it.

| DATA SUBJECT | TYPE OF INFORMATION | RETENTION PERIOD |
|---|---|--|
| Company information | Agendas of Board meetings | Indefinite period |
| Clients or Service Provider Data including FICA documents | All information from customers, business contacts and suppliers | At least (5) years and maximum (7) years after termination of service As set out in applicable law |
| Financial Data | Financial information related to and owned by Ongeza Life | As set out in applicable law |
| Electronic Documents | Email | Not all emails need to be retained depending on the topic |

Retention and Destruction Policy

| | | |
|------------------|--|---|
| Employees data | PDF documents | Must be based on the contents of the file. |
| Job seekers data | personnel records (attendance records, application forms, job or status change records, evaluations, termination documents, test results, training, qualification records) | At least (5) years and a maximum of (7) years after termination of service contract |
| | Service contracts - individually | Indefinite |
| | CV, cover letter, qualifications, work history, references | A maximum of 6 months, after which the job seeker must give permission again |

By law, all information stored under this policy must be non-encrypted. Encryption and decryption keys must be kept secure for as long as the information is retained.

4. ROLES AND RESPONSIBILITIES

Employees Must:

- ensure that all information held by Ongeza Life is destroyed in accordance with this policy.
- Incorrect or unnecessary data retention devices (HARD DISK, FLASH, CD, etc.) pass to the IT Department for safe destruction.
- Make regular backups of all sensitive information.

Heads of departments and information asset owners

- have overall responsibility for the management of records and data generated by their department's activities, namely, to ensure that records created, received and controlled within the scope of their department, and the systems (electronic or otherwise) and procedures that they are adopted to manage in a manner that meets the objectives of this policy.

Where an information officer has been appointed, he must be involved in any data retention processes and records or all archives and the destruction of certain information.

IT Department

- The IT department is responsible for archiving, destroying information and sanitizing hardware and software. Any hardware that can store sensitive information must be destroyed by the IT department.

Retention and Destruction Policy

- Only the IT department may authorize the disposal of any IT equipment and must personally accept and authorize such assets of the department.
- In all cases, the IT department must confirm the successful deletion and destruction of each asset.

Prohibited Activities

Employees may not:

- get rid of Ongeza Life's clients and business related information by throwing it in the trash;
- get rid of Ongeza Life clients, and business related information anywhere other than Ongeza Life's business premises;
- use a memory device (FLASH) Ongeza Life's clients and business related information;
- open and / or reuse a flash disk, hard drive or CD-ROM for personal reasons, initially containing Ongeza Life's clients and business related information; and
- donate or sell any mobile, portable, wireless device capable of retaining sensitive information issued to Ongeza Life by any other person.

Employees must:

- at all times destroy Ongeza Life 's clients and business information in accordance with this policy;
- delete any paper-based information related to Ongeza Life, its clients in accordance with this policy;
- transmit any hard drive to the IT Department in accordance with this policy.
- Use CLOUD REVIEW (like OneDrive accounts)
- Use FILE-DROP technologies such as OneDrive accounts are included in this policy. OneDrive accounts are provided to Ongeza Life employees. This platform (like Dropbox or Google Drive) can be an easy solution for employees in terms of backup and secure file transfer. Your OneDrive Account and therefore all information stored on it is the property of Ongeza Life and is still subject to this policy.
- Backup - For a user's email, calendar and other items, a retention policy is applied at the level of the mailbox. For public files, the retention policy is applied at the file level.
- File Transfer - Cloud technology can provide an easy way to transfer information to other parties. If you decide to process sensitive information in this way, it must be encrypted, and must be properly maintained as explained in this policy.

Heads of departments and information asset owners - have overall responsibility for the management of records and data generated by their department's activities, namely to ensure that records created, received and controlled within the scope of their department, and the systems

Retention and Destruction Policy

(electronic or otherwise) and procedures that they are adopted to manage in a manner that meets the objectives of this policy.

Where an information officer has been appointed, he must be involved in any data retention processes and records or all archives and the destruction of certain information.

IT Department

- The IT department is responsible for archiving, destroying information and sanitizing hardware and software. Any hardware that can store sensitive information must be destroyed by the IT department.
- Only the IT department may authorize the disposal of any IT equipment and must personally accept and authorize such assets of the department.
- In all cases, the IT department must confirm the successful deletion and destruction of each asset.

5. POLICY COMPLIANCE

5.1 COMPLIANCE MEASUREMENT

The Information Security team will verify compliance to this policy through various methods, including but not limited to, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 EXCEPTIONS

Any exception to the policy must be approved by the Chief Information Officer/ Head of IT in advance.

5.3 NON-COMPLIANCE

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. RELATED STANDARDS AND POLICIES

- Acceptable Internet use Policy
- Email Policy
- Incident response Policy
- Notice of Security Incident Policy
- Mobile and Portable Devices Policy
- Access to Information Policy