EMMAUS MINISTRY SOUTH AFRICA – POPIA POLICY 2022 (DRAFT)

TABLE OF CONTENT:

1. Purpose

The purpose of the Act is to:

- Give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at –
  (a) Balancing the right to privacy against other rights, particularly the right of access to information; and
  (b) Protecting important interests, including the free flow of information within the Republic and across international borders.
- Regulate the way personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information.
- Provide persons with rights and remedies to protect their personal information from processing that is not in accordance with the Act; and
- Establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for, and to promote, enforce and fulfil the rights protected by the Act.

The purpose of this document is to ensure that EMSA complies to this Act.

The policy provides guidelines as to how the Policy is to be implemented.

2. Scope

The Act is applicable to all EMSA Board Members and various community members of the Emmaus ministries.

3. Definitions

(a) **POPI Act**: Protection of Personal Information Act, 2013 (Act No 4 of 2013) - the law that provides protection of personal information.

(b) **PAIA**: Promotion of Access to Information Act, 2000 (Act No. 2 of 200) – the law that gives the right to access personal information.

(c) **Information Regulator** (IR): Juristic body established in terms of POPIA to see that there is compliance with both the Act and Promotion of Access to Information Act (PAIA).

(d) **EMSA**: Emmaus Ministries South Africa.

(e) **Data subject**: The person to whom the information relates. For e.g., pilgrims, butterflies and community members.

(f) **Special data subjects**: Children under 18 years of age.

(g) **Personal information**: any information in any form – electronic and paper – based files – including information but not limited to identity number, name, surname, sex, pregnancy, marital status, nationality, colour, sexual orientation, age, physical or mental health, well-being, disability, conscience, belief, culture, language, criminal and employment history.

(h) **Special personal information**: Information specific to information categories such as religion, race, ethnical origin, membership of a trade union, political affiliation, sexual life, medical information, biometrical information (blood type, fingerprints).

(i) **Processing**: Any activity (automated or manual) such as collection, receipt, recording, organizing, storage, collation, retrieval, alteration, updating, distribution, dissemination by transmitting, erasure or destructing.

(j) **Responsible party**: The person who determines why and how to process.

(k) **Operator**: The person who processes personal information on behalf of the responsible party.

(l) **Data bridge**: Unlawful, unauthorized disclosure of personal data – either accidental or deliberate.

(m) **Information officer**: Person registered with the regulator responsible to ensure that the POPI Act is implemented.

(n) **Deputy Information officer**: The person supporting the information officer whom the Information officer delegates to.

4. Obligations and consequences

All organisations, companies and institutions in South Africa must comply to POPIA. Various obligations are placed on the responsible party, which is the body ultimately responsible for the lawful processing of personal information:

To regulate the collection and processing of personal information in a manner that will safeguard such information:

- To regulate the collection and processing of personal information in a manner that will safeguard such information against unauthorized access and usage.
- To establish the requirements and conditions for the collection, distribution, and retention of personal information in line with the Act.
- To determine the purposes for which personal information will be used.
- To ensure only operators that can meet the requirements of lawful personal information processing prescribed by POPIA are used.
- Personal information should only be processed if it is adequate, relevant, and not excessive i.e., only collect information which is needed.

The EMSA exco supported by the information officer and deputy information officer of EMSA are responsible for administering and over seeing the implementation of this policy and any applicable supporting guidelines and procedures.

Violations of this policy and of the POPI Act will be dealt with by the Information Regulator. Data subjects may refer their complaints to the Information Regulator.

There are two legal consequences for the responsible party in case of data breach:

- A fine or imprisonment of between R1 million and R10 million or one to ten years in jail.
- Financial compensation to data subjects for the damage they have suffered.

Other consequences:

- Reputational damage.
- Losing customers.
- Losing employees.
- Failing to attract new stakeholders, sponsors, donors, volunteers and so forth.
- Security compromise could occur with back door access to the financial institutions' information in that cybercrime could occur.

5. FORMS OF STORED INFORMATION

Data is stored in the following ways:

- Electronic database.
- Manual filing system.
- Address books, calendars, diaries.
- Payroll system.
- Sent and received via email stored via cloud.
- Contracts.
- Sign in registers at reception.
- Telephone records.
- Invoices, orders, quotes.
- Application forms.
- Attendance registers.
- Meeting recordings – zoom, Skype, Microsoft Teams.

6. GENERAL POLICY GUIDELINES

- It is each organization, company, institution's obligation to do what is reasonably expected to ensure that data is protected, and information is kept safe.
- Data should rather be restored in a cloud and not on computers or external hard drives.
- Computers should not be left unattended, and screens should be locked.
- Responsible parties must ensure that information quality is complete, accurate, not misleading and updated. Assurance should also be in consent forms and terms and conditions.
- PAIA promotes access to information in terms of section 32 (1)(a) of the constitution. Therefore, both PAIA and POPIA must be implemented. A manual must be developed, monitored, maintained, and made available.

7. CONDITIONS FOR LAWFUL PROCESSING

- Accountability – responsibility to ensure compliance.
- Processing limitations – only process information, which is adequate, relevant and not excessive.
- Purpose specific – explicitly defined.
- Further processing limitations – only process data if it forms part of the originally obtained purpose.
- Information quality – ensure that information is complete, accurate, not misleading and updated.
- Openness – notify data subjects about the circumstances in which such compliance would be mandatory e.g. where the law authorizes the processing.
- Security safeguards – this is the list of measures that should be taken to prevent loss, damage, unauthorized and unlawful access.
- Data subject participation – they have the right to request the records kept on them and how their information was shared.

8. STEPS TO COMPLY

- Data subjects be informed of the purpose or reason for the collection of their data, so that they may give consent or refuse it.
- Any further use of the collected personal information - must be compatible with the initial purpose of collection. All information that is collected by EMSA may only be used for the initial purpose for which it was collected.
- EMSA may not process a data subjects' information without consent unless imposed by law, in public interest, or to complete a project which the data subject is party to.
- Consent is given by a data subject by signing an agreement or application or a tick box on a form.
- Data subjects – must be advised of the consequence of not giving consent e.g., not participating in an activity.
- If EMSA seeks to use the information for another purpose, the data subject – must be contracted to obtain content for further processing.
- The data subject may revoke his/her consent at any time. The withdrawal of consent must be communicated to the Information Officer in writing within a reasonable time. The withdrawal will only be effective if EMSA agrees in writing. The data subject will be informed of the consequences of the withdrawal as it will result in EMSA being unable to provide services or benefits.
- EMSA will not keep personal information of data subject for a specific purpose for longer than is necessary to fulfil the purpose of its collection unless further retention is required by law or the data subject's consent is obtained to make provision for further retention.
- Once the purpose of retention of the information is fulfilled the information will be destroyed in accordance with the POPI Act.
- EMSA will take all reasonable steps to ensure secure data transmission over the internet or via its online services.
- Data is only collected with consent from the data subject. EMSA relies on data subjects for correctness of information. The Data subjects are required to confirm the correctness of information.

- An Information Officer of EMSA must be registered with the Information Regulator.
- Existing policies must be reviewed to comply with the POPIA and be reviewed every two years.
- Members must be made aware of POPI and EMSA’s policy.
- Data breaches must be reported to the Information Regulator and data subjects.
- A data breach response plan must be developed.