POPIA

Protection of Personal Information Act 4 of 2013

life, done better

Privacy and data protection is a cornerstone of our democracy.

The Protection of Personal Information Act (POPIA) has been passed to protect these rights, effective from 1 July 2020, with a 12-month grace period which ended on 1 July 2021.

WHY DO WE NEED POPIA?

South Africa has a high incidence of data breaches and identity theft is now the white collar crime of choice in our country with many people suffering raids on their bank accounts etc. POPIA aims to reduce the incidence of cybercrimes and provides for massive penalties should those who hold others' personal information not protect it adequately.

WHAT IS POPIA ABOUT?

POPIA is designed to protect the personal information we hold in respect of all clients, staff and third parties such as outsourced contractors. Personal information (PI) relates to an identifiable, living, natural person, and where applicable, an identifiable, existing, juristic person. There are more than 40 types of personal information which can be categorised into six sections being:

- Contact details
- Biometrics
- Opinions
- Demographics
- Personal history
- Private and special confidential correspondence

Some examples of PI include: race, gender, sex, marital status, nationality, sexual orientation, age, physical or mental health, disability, religion, language, education, medical, financial, employment, ID, email, address, telephone number, location information, blood type, biometric information, personal opinions, preferences, private or confidential correspondence, and views or opinions of another person.

We need to implement reasonable technical, legal and organisational procedures to protect this PI while we process it.

WHAT IS FMI DOING ABOUT POPIA?

We strive to comply with the eight processing conditions namely:

1. **Accountability**: We must ensure that the conditions for lawful processing of PI are complied with.
2. **Processing limitation**: Must be lawful and in a reasonable manner that does not infringe on privacy. PI may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive. Information must be collected directly from and with the consent of the data subject. Processing of PI must be with consent unless it is necessary:
   - to conclude or perform a contract
   - to fulfil a legal obligation
   - to pursue the legitimate interests of FMI
   - to protect the legitimate interest of a data subject
3. **Purpose specification**: Must be for a specific, explicitly defined and legal purpose. The data subject must be made aware of the purpose, what is being collected, who is collecting it, whether collection is voluntary or mandatory and the consequences of failure to provide PI.
4. **Further processing limitation**: Further processing of PI must be compatible with the purpose for which it was collected.
5. **Information quality**: PI collected from a data subject must be complete, accurate, not misleading and updated as and when necessary.
6. **Openness**: When PI is collected, the data subject must be told of the PI being collected, the source of any PI not directly collected, the purpose for which the PI is being collected, whether or not it is mandatory to give their PI and the data subject must also be aware of their right to object to the processing of their PI.
7. **Security safeguards**: Security measures to ensure the integrity and confidentiality of PI must be in place. Security measures for PI processed by third party operators must be stipulated and evaluated. Notification of security compromises must be made to the Information Regulator and all data subjects affected as soon as possible.
8. **Data subject participation**: The process must be transparent and the data subject must be able to:
   - request details of all their PI held;
   - have ease of access to maintain their PI;
   - be aware of our process; and
   - be able to complain if they suspect their PI has been misused.

HOW DO WE PROCESS YOUR PI?

We take the processing of your PI seriously. For full details on how we process your PI, please read our Privacy Notice here.

For non-compliance:

- we can receive fines of up to R10 million;
- time in prison for up to 10 years;
- civil damage claims, including class action suits;
- company reputational damage;
- loss of customers; and
- business disruption.

WHAT IS PAIA?

POPIA should not be confused with the Promotion of Access to Information Act (PAIA) which has been in force for many years. PAIA is the Act that allows us to access any of our information held by public or private bodies. We need to comply with PAIA as well and our PAIA Manual is currently displayed on our website.

WHAT CAN I DO TO PROTECT MY PI?

- Always use secure networks when accessing documents that contain PI.
- Make sure that you are sending information to the correct recipient.
- Use strong passwords and change your passwords as required.
- Do not access links, emails or websites from sources that are not trusted.