PROTECTION OF PERSONAL INFORMATION ACT (POPIA)

COMPLIANCE FRAMEWORK

December 2022

POPIA COMPLIANCE FRAMEWORK FOR OVERBERG DISTRICT MUNICIPALITY

In terms of the POPIA Regulations (2018) an Information Officer must prepare, implement, monitor and maintain a compliance framework. In the absence of a prescribed format and based on the requirements stipulated in the POPIA, such a compliance framework should include the following:

1. **Name of Information Officer and Deputy Information Officers** – ensure that the Information Officer and Deputy Information Officers are registered with the Information Regulator.

2. **Data mapping** – prepare a document that describes all personal information (data) processes that takes place within the organisation, consisting of the following:

    - The name and contact details of the person administering the specific process.
    - A description and the purpose of the process.
    - The categories of data subjects and categories of personal information.
    - A description of the notification to data subjects when personal information is collected.
    - The categories of recipients to whom personal information would be disclosed.
    - Where applicable, transfers of personal data to a third party in a foreign country or an international organisation, including the identification of that third party and country or international organisation.
    - Where possible, the envisaged time limits for erasure of the different categories of personal information.
    - A description of the applicable security measures to prevent loss of, damage to or unauthorised destruction of personal information, or unauthorised access to the processing of personal information.

3. Describe the **practical measures** to ensure that personal information is complete, accurate, not misleading and updated where necessary.

4. Ensure that **personal** information (data) policies are in place and updated when necessary.

    - Provide clear information about your personal information processes and the applicable legal justification thereof.
    - Inform people that you collect their personal information and why, how is it processed, who has accessed to it and how is the personal information safeguarded.

5. Conduct a **personal information impact assessment** to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information. The higher the risk of interference in the rights of persons, the more important is the personal information impact assessment.

A personal information impact assessment should include the following:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the responsible party.
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
- An assessment of the risks to the rights and freedoms of data subjects.
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal information and to demonstrate compliance with POPIA.

6. Develop, monitor and maintain a **PAIA manual** (manual of functions of and index of records held by an organisation).

7. Ensure that **internal measures are developed** together with adequate systems to process requests for information or access thereto. This would for example include the use of forms or templates to obtain specific personal information.

8. Ensure that **internal awareness sessions** are held in the organisation regarding the provisions of POPIA and its regulations, any codes of conduct and other information produced by the Information Regulator.

9. Develop a **data breach response plan** that includes:- who has responsibility to deal with such cases, an indication of the response time, notification to the Information Regulator and the data subjects, any other reporting requirements.

10. Ensure that there are **data processing agreements** in place between you (responsible party) and any operator who processes personal information for you. This includes for example cloud services, e-mail services and analytics software.

11. Adopt the **personal information protection** by design approach in all activities of your organisation when dealing with personal information.

12. Ensure that a **privacy notice**, i.e. a notice stating how your organisation processes personal information in compliance with POPIA is available to the public and placed on your organisation's website. This notice should be concise, intelligible, easily accessible, in clear and plain language, in particular for any information provided to children.

_____ _____

MUNICIPAL MANAGER **DATE**