



# Protection of Personal Information Act (POPI) Compliance Report

To : Council  
For : 2020/21 Financial Year  
Prepared by : Ms Masesi Koto  
Title : Company Secretary

---



## REPORT ON THE PROTECTION OF PERSONAL INFORMATION ACT NO. 4 OF 2013 – POPI ACT

### Introduction

The purpose of the Popi Act is to protect personal information, to strike a balance between the right to privacy and the need for the free flow of, and access to information, and to regulate how personal information is processed.

The Act was signed into law in November 2013, and in April 2014 certain sections of the Act came into force. The sections which came into force were:-

- the sections giving the definitions of certain terms that are used in the Act;
- the sections dealing with the appointment of the administrative body that will oversee the operation of the Act, namely the Information Regulator; and
- the sections empowering the Minister and the Information Regulator to make regulations as regards the implementation of the Act.

The implementation date of the POPI Act which is 01 July 2021. The office of the Information Regulator has since been filled and they will soon have the capacity to implement the POPI Act.

Once the Act comes into force, we will have 12 months to bring our business practices in line with the new laws.

## **Who does the POPI Act applies to?**

- The POPI Act sets the minimum standards for the protection of personal information.
- The Act applies to anyone who keeps any type of records relating to the personal information of anyone, unless those records are subject to other legislation which protects such information more stringently.
- It regulates the “processing” of personal information. “Processing” includes collecting, receiving, recording, organising, retrieving, or using such information; or disseminating, distributing or making such personal information available.
- The Act will also relate to records which we already have in our possession.

## **Important Definitions**

“processing” – any operation or activity concerning personal information.

“record” – any recorded information, regardless of when it came into existence.

“responsible party” – a public or private body or any other person which determines the purpose of and means for processing personal information.

## **Processing of personal information**

*Personal information can only be processed: – (section 11)*

- with the consent of the “data subject”; or
- if it is necessary for the conclusion or performance of a contract to which the “data subject” is a party; or
- it is required by law; or
- it protects a legitimate interest of the “data subject”; or
- it is necessary to pursue your legitimate interests or the interest of a third party to whom the information is supplied.

We all have the right to object to having our personal information processed. We can withdraw our consent, or we can object if we can show legitimate grounds for our objection.

A Responsible Party has to **collect personal information directly from the “data subject”**, unless:

- This information is contained in some public record or has been deliberately published by the data subject.
- collecting the information from another source does not prejudice the subject;
- it is necessary for some public purpose; or to protect your own interests;
- obtaining the information directly from the subject would prejudice a lawful purpose or is not reasonably possible.

**Compliance with the POPI ACT**

NO	REQUIREMENT	COMPLIANCE	RESPONSIBLE PERSON
1	We all have the right to be told if someone is collecting our personal information, or if our personal information has been accessed by an unauthorised person.	Communication should include that personal information is collected as part of the process.	Supply Chain, HR Department, Corporate Governance, Events Management, H&K and IT.  <b>Tender/RFP, Job Advertisement to be updated and the Declaration List by Security to be updated Notice regarding Names Database Freedom Park Website ICT information</b>

			<b>through email and social platforms</b>
2	We have the right to access our personal information.	Communication should include that individuals have a right to access personal information collected.	Supply Chain, HR Department, Corporate Governance, Events Management, H&K and IT.  <b>Tender/RFP, Job Advertisement to be updated and the Declaration List by Security to be updated Notice regarding Names Database Freedom Park Website ICT information through email and social platforms</b>
3	We also have the right to require our personal information to be corrected or destroyed, or to object to our personal information being processed.	Communication should include that individuals have the right to require our personal information to be corrected, or to object to their personal information being processed.  <b>Note Freedom Park cannot destroy collected information</b>	Supply Chain, HR Department, Corporate Governance, Events Management, H&K and IT.  <b>Tender/RFP, Job Advertisement to be updated and the Declaration List by</b>

			<b>Security to be updated</b> <b>Notice regarding Names Database</b> <b>Freedom Park Website</b> <b>ICT information through email and social platforms</b>
4	You can only collect personal information for a specific, explicitly defined and lawful purpose and the subject must be aware of the purpose for which the information is being collected. (section 13)	Communication should include the purpose for which the information is required	Supply Chain, HR Department, Corporate Governance, Events Management, H&K and IT.  <b>Tender/RFP, Job Advertisement to be updated and the Declaration List by Security to be updated</b> <b>Notice regarding Names Database</b> <b>Freedom Park Website</b> <b>ICT information through email and social platforms</b>
5	Once the personal information is no longer needed for the specific purpose, it must be disposed of (the subject must be “de-identified”), unless you need to keep it (or are allowed to keep it) by law, or you need to keep the	Communication should include the explanation that the information will be kept after the completion of the process that the information was required for,	Supply Chain, HR Department, Corporate Governance, Events

	record for your own lawful purpose or in accordance with the contract between yourself and the subject, or the subject has consented to you keeping the records. (section 14)	<b>Note – The Act also applies to information collected before the promulgation of the Act.</b>	Management, H&K and IT.  <b>Tender/RFP, Job Advertisement to be updated and the Declaration List by Security to be updated Notice regarding Names Database Freedom Park Website ICT information through email and social platforms</b>
6	You are entitled to keep records of personal information for historical, statistical or research purposes if you have established safeguards to prevent the records being used for any other purposes.	Communication should include the explanation that the information will be kept after the completion of the process that the information was required for	Supply Chain, HR Department, Corporate Governance, Events Management, H&K and IT.  <b>Tender/RFP, Job Advertisement to be updated and the Declaration List by Security to be updated Notice regarding Names Database Freedom Park Website ICT information</b>

			<b>through email and social platforms</b>
7	Records must be destroyed in a way that prevents them from being reconstructed.	Not Applicable – Records are archived by the Freedom Park in compliance with the Archives Act	<b>Notice to be updated that information by Freedom Park cannot be destroyed in compliance with the Archives Act.</b>
8	You can only use personal information that you have collected for the purpose which you collected it for. (section 15)	Communication should include the explanation that the collected information will be used for the purpose which it was collected it for. (section 15).  <b>Note – an exception should be added that the information can be made available during court processes.</b>	Supply Chain, HR Department, Corporate Governance, Events Management, H&K and IT.  <b>Tender/RFP, Job Advertisement to be updated and the Declaration List by Security to be updated Notice regarding Names Database Freedom Park Website ICT information through email and social platforms</b>



<p>9</p>	<p><i>When information is being collected, subjects must be made aware of: (section 18)</i></p> <ul style="list-style-type: none"> <li>• the information that is being collected and if the information is not being collected from the subject, the subject must be made aware of the source from which the information is being collected;</li> <li>• the name and address of the person/organisation collecting the information;</li> <li>• the purpose of the collection of information;</li> <li>• whether the supply of the information by the subject is voluntary or mandatory;</li> <li>• the consequences of failure to provide the information;</li> <li>• whether the information is being collected in accordance with any law;</li> <li>• If it is intended for the information to leave the country and what level of protection will be afforded to the information after it has left South Africa.</li> <li>• who will be receiving the information;</li> <li>• that the subject has access to the information and the right to rectify any details;</li> <li>• that the subject has the right to object to the information being processed (if such right exists);</li> <li>• that the subject has the right to lodge a complaint to the Information Regulator. The contact details of the Information Regulator must also be supplied.</li> </ul> <p><b>Note</b> - These requirements have to be met before the information is collected directly from the subject, or soon as reasonably practicable thereafter if the</p>	<p>Communication should specify which information will be collected from other persons.</p> <p>Details of the Information Regulator should be included in the communication.</p> <p><b>All emails send out should have a notice in compliance with section 18.</b></p>	<p>Supply Chain, HR Department, Corporate Governance, Events Management, H&amp;K and IT.</p> <p><b>Tender/RFP, Job Advertisement to be updated and the Declaration List by Security to be updated Notice regarding Names Database Freedom Park Website ICT information through email and social platforms</b></p>
----------	--	--	---

	information is not collected directly from the subject, unless the subject is already aware of these rights. If you collect additional information from a subject for a different purpose, you have to go through this process again. S18(3)		
10	Anybody who keeps personal information has to take steps to prevent the loss, damage, and unauthorised destruction of the personal information. They also have to prevent unlawful access to or unlawful processing of this personal information. (section 19)	Filing and record keeping to be strictly adhered to	Supply Chain, HR Department, Corporate Governance, Events Management, H&K and IT.  <b>Tender/RFP, Job Advertisement to be updated and the Declaration List by Security to be updated</b> <b>Notice regarding Names Database</b> <b>Freedom Park Website</b> <b>ICT information through email and social platforms</b>
11	We have to identify all risks and then establish and maintain safeguards against these identified risks. We have to regularly verify that the safeguards are being effectively implemented and update the safeguards in response to new risks or identified deficiencies in existing safeguards.	Filing and record keeping risk to be assessed	<b>Manco – next Risk Manco meeting.</b>

12	Anybody processing personal information on behalf of an employer must have the necessary authorisation from the employer to do so. They must also treat the personal information as confidential. (section 20)	<p>Authorisation letters to be prepared for employees processing personal information.</p> <p>Recommend that the letters should be signed by the CEO on behalf of the employer.</p>	Supply Chain, HR Department, Corporate Governance, Events Management, H&K and IT.
13	Such a person must have a written contract with their employer in which they are specifically obliged to maintain the integrity and confidentiality of the personal information and to implement the established safeguards against identified risks.	<p>Confidentiality Agreements to be prepared for employees processing personal information.</p> <p>Agreements should be signed by the CEO on behalf of the employer.</p> <p>Contracts of Employment to include a confidentiality clause.</p>	Supply Chain, HR Department, Corporate Governance, Events Management, H&K and IT.
14	This employee is also obliged to notify their employer if they believe that personal information has fallen into the wrong hands (section 21(2))	The Agreement should include a clause that the employee will notify their employer if they believe that personal information has fallen into the wrong hands (section 21(2))	Supply Chain, HR Department, Corporate Governance, Events Management, H&K and IT.

### **Process to be followed if breach occurs**

If there has been a breach and personal information has been accessed or acquired by any unauthorised people you need to notify the Information Regulator, and the subject (if you still know who the subject was). The notification to the subject needs to provide sufficient information to allow the subject to protect themselves against the possible consequences of the personal information falling into the wrong hands.

We all have the right to enquire as to whether somebody has our personal information, all we have to do is provide proof of identity and this information must be provided free of charge. We can also find out what this information consists of and if this information has been disseminated to any third parties. For these last bits of information however we might have to pay a fee. Access to this information is also subject to the Promotion of Access to Information Act.

We all have the right to have our personal information corrected or deleted if it is inaccurate, irrelevant, excessive, dated or misleading, or if it has been obtained unlawfully, or if the responsible party is no longer authorised to retain the information.

### **Special Personal Information**

This relates to religious or philosophical beliefs, **race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information**. Also included in this category is information relating to the alleged commission of any offence or any proceedings in respect of any offence allegedly committed and the outcome of such proceedings. (section 26)

You are not allowed to process this special personal information unless **it is done with consent**; or is necessary in law; or is done for historical, statistical or research purposes; or the information has been deliberately made public by the subject.

There are also limited exceptions to the prohibition against the processing of “special personal information”.

These relate to situations when this information is specifically relevant and constitutes the purpose for which the information is being collected, for example for the purposes of **BEE** or for insurance.

### **Recommendation**

It is recommended that the Council notes the POPI Act Compliance Report.

**Ms Masesi Koto**

**Company Secretary**

**Date: 07 July 2021**