Protection of Personal Information

A short guide for the Employer on POPI - from a Payroll / HRA perspective.

Below is a short guide to assist you. If you are using eTorQue, our cloud-based payroll and HRA database, you are already compliant from a Software Security and Data Storage perspective, with regard to the system.

Please ensure that your other internal processes are adjusted and in line with the recommendations below.

1. **What is POPI?**

The Protection of Personal Information Act (also referred to as the POPI Act) aims to protect an individual's right to privacy regarding their personal information which may have been collected by a third party during a normal commercial transaction or by
their HR department prior to, or during, the course of their employment. It also seeks to bring South African law regarding ensuring and managing personal data in line with international data protection laws.

2. **What is the objective of POPI?**

The purpose of POPI is to regulate and formalise how companies collect, store, protect, access and distribute consumer information and to protect the ongoing integrity and sensitivity of that private information.

The Act offers many safeguards regarding using an individuals' personal data, and primarily protects individuals from unsolicited emails & SMS's for services that they never applied for, as well as against any security breaches that could result in identity theft, when personal information is stolen or offered too freely by a third party.

3. **Who is covered?**

- Clients/Consumers - regarding their buying habits, historic transactions, activities, etc.
- Suppliers - their pricing, contracts, contacts, etc.
- Employees - HR info, Payroll records, CV's, applications for employment, CCTV records, T&A records, performance reviews, IR records, emails, etc.

4. **How does this affect the HR & Payroll Department?**

This Act will impact all companies who in their "normal course of business" collect, manage, manipulate, analyse, distribute, use, retrieve, store, retain, destroy, delete, or interrogate any form

of personal data, be that data from a potential Employee, an existing Employee or a discharged / previously employed Employee.

In most cases companies have implemented measures to manage their HR related information in a secure environment by either using internal or cloud based software systems. One cannot however assume that these measures are necessarily sufficient to satisfy POPI, so it is imperative that as a responsible business owner / Employer / HR or Payroll Manager Reviews of internal procedures and controls must regularly be conducted to ensure compliance with the Act. This should include, amongst others, reviewing recruitment process and obtaining consent from suppliers and Employees before collecting and storing personal information.

The requirements as specified in the Gazette that covers Record Keeping as well as the ICT and Tax Administration Acts are integral to a company's ability to adhere to this Act. Companies need to have an understanding of all these Acts and as such have an integrated approach when implementing POPI. The Act includes a section to do with managing Special Personal Information. This deals with, for example, information related to political, sexual, religious persuasion and information about children. Personal data which is maintained across borders is also dealt with by the Act, specifically relating to countries where inadequate information protection frameworks exist, or where companies store their data in the cloud and the actual cloud infrastructure is actually resident in another country.

5. 8 Key Conditions

The Act contains 8 key conditions that an entity which intends to process personal information lawfully, must comply with:

1. Processing Limitation

Personal information must be processed in accordance with the law. It must be managed in a proper and careful manner so as not to intrude on the privacy of the person / entity whose information is being processed.

2. Purpose Specific

The information must be collected for a specific purpose, which is properly defined and for legitimate reasons. It may not be kept for longer than is necessary (i.e. must suit the purpose).

3. Further Process Limitation

Must not be processed beyond the initial purpose i.e. which makes it incompatible with the original purpose.

4. Information Quality

The person collecting the data must take proper steps to ensure that the data is complete, accurate, current and not misleading in any way.

5. Openness

The information may only be collected by someone who has given notice to / disclosed the requirements, the purpose and the reason to the person / entity concerned and must obtain their consent.

6. Security Safeguards

This ensures that appropriate technical and organisational measures have been taken to ensure integrity of the data / information as well as safeguarding it from unauthorised access.

7. Individual Participation

Details of what data / information is collected must be made available to the person / entity that is the subject, free of charge. They must understand what data is being collected, why it's being collected and that they have the right to request that it gets discarded after using the data for the initial purpose (within reason).

8. Accountability

The responsible party will be held accountable for the management / implementation of the items mentioned above.

6. Executive Summary

It is of key importance that Directors of a company take a directing role in implementing measures to ensure their organisation is compliant. Penalties for noncompliance could include fines of up to R10 million and even jail sentences of up to 10 years - so this is a serious matter for everyone.

Annexure A – POPI Checklist

This checklist should assist companies to assess their compliance with POPI.

1. **Audit: Review the process / forms etc. which your organisation uses to collect, record, disseminate and destroy personal information. It is important to review the entire process before starting.**

Specifically Review the following:

- **Recruitment process:** How does the company receive, store and communicate information regarding candidates and for how long does the information get stored? Do you have the necessary consent from the candidate to retain the information if they are not successful in their request for employment
- **New employee take on process:** Does the company have clauses in Employee contracts explaining why specific personal information is required and does the Employee consent to this? In what manner is the information obtained, and how is this information then stored? Is the information stored in a secure environment?
- **Software security:** Is the software package used that manages Payroll / HR data from a reputable company? Is password complexity monitored? For what period of time are passwords valid?
- **Database storage**: Is your solution hosted in house or on the cloud? If in house, does your company have sufficient IT security protocols in place and are they monitored and evaluated on a periodic basis? If cloud based systems are used, have you reviewed your suppliers security certificate of compliance and gained and understanding of where is the data and system software is physically located? Are there regular backups taking place and are they tested frequently?
- **Information dissemination**: How does the HR/Payroll Department handle movement of personal information? Are the Employees aware and have they given consent that the company records and retains this information.

2. **Purpose: Define the purpose of information gathering and processing.**

Personal Information can only be gathered for specific and openly defined, lawful purposes related to a function or process within the company.

Ask the following questions:

a. Why am I collecting the information – i.e. is it to be compliant with SARS, the Dept. of Labour, etc.?
b. Has the employee consented?
c. In what manner will this information be used – i.e. to ensure that a correct Tax Certificate is submitted to SARS every six months?
d. Is this collection of specific data lawful?
e. Does this information relate directly to a function/process within the organisation?

3. Limit Considerations: Information collected must be lawful, adequate, and relevant to the purpose for which it is processed.

Ask the following questions:

a. Is this information relevant? i.e. Surname vs Religion?
b. Are there any other processes that require this information? i.e. Medical Aid Recons
c. Is it a legal requirement to keep this information? i.e. IRP5s
d. Have you validated that the information is correct?

4. Inform the Employee: The Employee must be informed that his/her information is being captured, retained and processed and exactly what the information will be used for.

Ensure you have the following in place:

- A clause in your employment contract specifically pertaining to the storage, processing and use of personal information.
- The Employees' consent to do so.

5. Procedures: Procedures for processing information must be in line with POPI

Ask the following questions:

a. How is information received from third parties – how do I know it is accurate?
b. How is information communicated to third parties – how do I ensure that I only provide that which is needed, and do I know what they are going to do with the data?
c. Has the Employee consented to the dissemination on his/her information between the company and these third parties?
d. Is the information secure while in "transit" – how do I know this?
e. Was the information initially collected for this purpose?

6. Employee Requests: Information must be available to Employees. Employees have the right to at any point in time request a list of information and third parties that may have access to their information.

7. Corporate Governance Officer: Appoint a Corporate Governance officer.

You need an internal champion – i.e. someone who responsible / accountable and constantly reviews what data you have, what data you need, how will you get the data without infringing on someone's privacy, and how will you manage the data.

That person also needs to establish a policy re:

a. At what point does the data / information become obsolete.
b. How does one delete / destroy redundant information.
c. How does one archive and then subsequently retrieve data / information.

Annexure B – Example Employee Take-on Form

Date	
Employee Number	
ID Number	
Join Date	
Position	

The contents of this form will remain confidential and will only be used by the Company to ensure compliance with the Employment Equity Act 55 of 1998 and the Income Tax Act 58 of 1962. The company takes all necessary precaution to ensure compliance with the Protection of Personal information Act 4 of 2013.

Personal Information	
Surname	
First Names	
Initials	
Preferred Name	
Age	
Position	
Employment Date	
Income Tax Number	
Gender	
Race	
Language	
Disabled	Yes / No
Number of Dependants	
Marital Status	
Driver's Licence	Yes / No
Drivers Licence Expiry	

Contact Details

Physical Address	
Unit Number	
Complex Name	

Street Number	
Street / Name of Farm	
Suburb / District	
City	
Province / State	
Country	
Code	

Postal Address	
In Care of Intermediary	
Unit Number	
Complex Name	
Street Number	
Street / Name of Farm	
Suburb / District	
Province / State	
City	
Country	
Code	

Contact Numbers	
Phone (Home)	
Phone (Mobile)	
Phone (Business)	
Email Address	

Identity & Passport Details	
Date of Birth	
Identity Number	
Passport Number	
Country of Issue	
Date Issued	
Validity Period	
Expiry Date	
Nationality	
Ethnic Persuasion	

Bank Details	
Account Holder Name	

Account Number	
Account Holder Relationship	Own / Joint / Third Party
Account Type	
Branch Code	

Education	
Qualification	
Institution	
Year Completed	
Subjects	

Qualification	
Institution	
Year Completed	
Subjects	

Qualification	
Institution	
Year Completed	
Subjects	

Annexure C – Example Employment Contract Clause

I hereby authorise the Company, the Company's Human Resource Department and authorized Management team to use, review and process any personal information provided to the company in the course of my application and employment as well as any information that I have provided in support of my application.

I understand my right to privacy and the right to have my personal information processed in accordance with the conditions for the lawful processing of personal information and hereby give my consent to the Company to collect process and distribute relevant personal information where the company is legally required to do so. I hereby consent that I understand that third party providers such as Funds, Insurance Suppliers, etc. have access to my personal information and I hereby consent to the company sharing my personal information strictly for the administration with these funds.