Guidelines and Training Manual

Pilot Software Holdings

The Protection of Personal Information (POPI) Act

as published in the Government Gazette Notice 37067 on 26 November 2013

This is a guide!

Its purpose is to assist you and your company to be compliant and to align with the intent and purpose of the Act. The provisions of POPI are a reflection of the ideals as enshrined in common law and more importantly Section 14 of the Constitution.

Unfortunately POPI is not an event, in essence it requires a change in corporate culture and a concerted and directed effort. POPI Compliance requires at least the following:

- Will from management
- Training of staff
- Regular inspection and process flow management
- Reporting and measurement
- Re-training

Steps to POPI:

- Appointment of a COMPLIANCE OFFICER.
- Your POPI Training Guide and Compliance Manual is only your, "Introduction to POPI", The Start.
- No two business are the same, you will need to build your own corporate culture regarding POPI.
- The Golden Rule for POPI is; Personal Information has now become, ***"Treasured Goods".***
- The guide serves to outline the fundamentals of the Act including the following;
    - Who are the role players?
    - What is meant by "Personal Information"?
    - What is "Processing"?
    - The job of the Compliance Officer .
    - Checklists and guides.

Section 51 Manual

in terms of

The Promotion of Access to Information Act, (Act 2 of 2000)

Incorporating additional requirements of

The Protection of Personal Information Act, (No 4 of 2013)

for

Pilot Software Holdings

SECTION 51 MANUAL FOR Pilot Software Holdings (1997/020387/07)

INFORMATION REQUIRED UNDER SECTION 51(1)(a) OF THE ACT

Postal Address of head of Pilot Software Holdings:

PO BOX 448 Wendywood 2144

Physical Address of head of Pilot Software Holdings:

15 Polo Crescent Woodmead Office Park Woodmead 2125

Tel. No of head of Pilot Software Holdings:

0116028300

Fax. No of head of Pilot Software Holdings:

none

Email address of head of Pilot Software Holdings:

priya.jacob@pilot.co.za

DESCRIPTION OF GUIDE REFERRED TO IN SECTION 10: SECTION 51(1)(b)

A guide has been compiled in terms of Section 10 of PAIA by Pilot Software Holdings. It contains information required by a person wishing to exercise any right, contemplated by PAIA.

This Guide is available for inspection, inter alia, at the office of the offices of Pilot Software Holdings at the physical address above and at the SAHRC.

THE LATEST NOTICE IN TERMS OF SECTION 52(2) (IF ANY):

At this stage no notice(s) has/have been published on the categories of records that are automatically available without a person having to request access in terms of PAIA.

ACTS AND OTHER LEGISLATION HELD AT PHYSICAL ADDRESS BY Pilot Software Holdings

Basic Conditions of Employment 75 of 1997

SUBJECTS AND CATEGORIES OF RECORDS HELD AT PHYSICAL ADDRESS BY Pilot Software Holdings

- Attendance registers
- Correspondence
- Licences (categories)
- Minutes of Management Meetings
- Minutes of Staff Meetings
- Statutory Returns
- Employee Records
- Employment Contracts
- Employment Equity Records
- General Correspondence
- Industrial and Labour Relations Records
- Information relating to Health and Safety Regulations
- Performance Appraisals
- Personnel Guidelines, Policies and Procedures
- Remuneration Records and Policies
- Skills Requirements
- Staff Recruitment Policies
- Statutory Records
- Training Records
- Contracts
- Marketing Records
- Annual Financial Statements
- Asset Register
- Budgets
- Financial Transactions
- Insurance Information
- Management Accounts
- Purchase and Order Information
- Stock Records
- Tax Records (company and employee)
- IT Policies and Procedures

SUBJECTS AND CATEGORIES OF PERSONAL RECORDS HELD AT PHYSICAL ADDRESS BY Pilot Software Holdings

- Identity Numbers
- Dates of birth
- Telephone numbers
- eMails
- Addresses
- Banking details
- Bank account numbers
- Licence numbers
- BEE Certificates
- Invoices

CUSTOMER PERSONEL INFORMATION SHARED BY Pilot Software Holdings

- Group companies
- 3rd Party service providers to uphold contract service obligations of client

EMPLOYEE INFORMATION RECEIVED BY Pilot Software Holdings

Medical aid funds

IT PRACTISES BY Pilot Software Holdings

- Physical security, (PC's locked to fixture/locked computer room)
- Network security controls
- Password controls
- Virus & Malware protection
- Software updates
- Disaster recovery & back-up policy

COUNTRIES OF OPERATION

-

DETAIL ON HOW TO MAKE A REQUEST FOR ACCESS - SECTION 51(e)

- The requester must complete Form B and submit this form together with a request fee, to the head of the private body

- The form must be submitted to the head of the private body at his/her address, fax number or email address
- The form must:
    - provide sufficient particulars to enable the head of the private body to identify the record/s requested and to identify the requester
    - indicate which form of access is required
    - specify a postal address or fax number of the request in the Republic
    - identify the right that the requester is seeking to exercise or protect
    - provide an explanation of why the requested record is required for the exercise or protection of that right
    - in addition to a written reply, the requester wishes to be informed of the decision on the request in any other manner, to state that the manner and the necessary particulars to be informed in the other manner, if the request is made on behalf of another person, to submit proof of capacity in which the requester is making the request, to the reasonable satisfaction of the head of the private body.

FORM B

REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

(Section 53(1) of the Promotion of Access to Information Act, 2000

(Act No. 2 of 2000)

[Regulation 10]

A. Particulars of private body

The Head:

B. Particulars of person requesting access to the record

(a)	The particulars of the person who requests access to the record must be given below.
(b)	The address and/or fax number in the Republic to which the information is to be sent must be given.
(c)	Proof of the capacity in which the request is made, if applicable, must be attached.

Full names and surname:

Identity number:

Postal address:

Fax number:

Telephone number: E-mail address:

Capacity in which request is made, when made on behalf of another person:

C. Particulars of person on whose behalf request is made

This section must be completed *ONLY if* a request *for information is* made on behalf of *another* person.

Full names and surname:

Identity number:

D. Particulars of record

(a) Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.
(b) If the provided space is inadequate, please continue on a separate folio and attach it to this form.
The requester must sign all the additional folios.

1 Description of record or relevant part of the record:

2 Reference number, if available:

3 Any further particulars of record:

E. Fees

(a) A request for access to a record, other *than* a record containing personal information about yourself, will be processed only after a request fee has been paid.
(b) You will be *notified of* the amount required to be paid as the request fee.
(c) The fee payable for access to a record depends *on* the form *in which* access is required and the reasonable time *required* to search for and prepare a record.
(d) If you qualify for exemption *of* the payment *of* any fee, please state the reason for exemption.

Reason for exemption from payment of fees:

F. Form of access to record

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in 1 to 4 hereunder, state your disability and indicate in which form the record is required.

Disability:	Form in which record is required
Mark the appropriate box with an X. NOTES: (a) Compliance with your request in the specified form may depend on the form in which the record is available. (b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form. (c) The fee payable for access for the record, if any, will be determined partly by the form in which access is requested.	

1. If the record is in written or printed form:			
	copy of record*		inspection of record
2. If record consists of visual images this includes photographs, slides, video recordings, computer-generated images, sketches, etc)			

POPI COMPLIANCE OFFICER
Pilot Software Holdings

CERTIFICATE OF APPOINTMENT

~~**Glenn Miller** as Head of **Pilot Software Holdings** confirm I will act as the POPI COMPLIANCE OFFICER.~~
or
Glenn Miller as Head of **Pilot Software Holdings**, I confirm I have appointed **Priya Jacob** to act as the POPI COMPLIANCE OFFICER.

The purpose of this appointment is to give effect to; the right to privacy in terms of our common law, section 14 of the Constitution and the purpose and application of the Protection of Personal Information Act, No 4 of 2013.

Specifically to implement and maintain the provisions of the POPI Act including but not limited to the following:

- To give effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible party.
- To regulate the manner in which 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.
- To provide persons with rights and remedies to protect their personal information from processing that is not in accordance with the Act.

The Act regulates how anyone who processes personal information must handle, keep and secure that information. If an individual or a company processes personal information relating to a person, that individual or company must comply with the Act. Failure to comply with the Act may lead to the imposition of certain penalties under the Act.

Punishable offences in terms of the Act The following offences are, if committed, punishable with either a fine (not exceeding R10 million), or imprisonment (for a period not exceeding 10 years), or both:

- Obstruction of a Regulator.
- Failure to comply with enforcement or information notices.
- Offences by witnesses - Giving false evidence before the Regulator.
- Unlawful acts by a responsible party in connection with information/usage.
- Unlawful acts by third parties in connection with information/usage.
- Any person who sells/offers to sell information obtained illegally.
- Failure to notify the Regulator that processing is subject to prior authorization.
- Breach of confidentiality.
- Obstruction of the execution of a warrant.

SIGNATURE
Glenn Miller
as Head of **Pilot Software Holdings**,

SIGNATURE
Priya Jacob

2018-10-15

POPI COMPLIANCE OFFICER - TRAINING OVERVIEW

Who are the role players?

- Data Subject: the person to whom the information relates.
- Responsible Party: Your company, a private or public body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;
- Operator: a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of the responsible party.
- Regulator: The Information Protection Regulator established by POPI.

What is meant by "Personal Information"?

''Personal Information'', means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, and may include the following:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.
- Information relating to the education or the medical, financial, criminal or employment history of the person.
- Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person.
- The biometric information of the person. **(Biometric information includes a technique of personal identification that is based on physical, physiological or behavioural characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.*
- The personal opinions, views or preferences of the person.
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.
- The views or opinions of another individual about the person.
- The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

Both INDIVIDUALS and COMPANIES are included in the ambit of "personal information".

What is "Processing"?

- Processing is *ANY* activity concerning personal information, e.g.
  - the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
  - dissemination by means of transmission, distribution or making available in any other form;
  - merging, linking, blocking, degradation, erasure or destruction of information.

Not covered:

- Purely household activity.
- Information that has been de-identified, *(cannot identify a person).*

It is not "personal information" if the information is already in the public domain or is not used, or intended to be used, in trade or commerce.

Your job as the POPI COMPLIANCE OFFICER in your organisation is to form a view and take steps in order to:

- Clearly understand the data processing activities that an organisation engages in;
- Training of relevant staff should be conducted on a continuous basis to ensure that staff are trained to understand the impact of POPI on their particular area of focus within the organisation;
- Consider whether appropriate written contracts are in place with *third parties* for whom personal data is processed, or to whom the processing of personal data is outsourced;
- Evaluate the security measures in place to keep personal data secure at all times;
- The terms under which intra-group transfers of personal data are made;
- Consider, in detail, the cross-border transfer of personal data; and review internal procedures ensuring continued compliance with POPI and the effective and efficient handling of enquiries and complaints by individuals.

POPI compliance 101, you need ensure:

- The legitimate grounds for collecting and using personal data collected in order to ensure that data is not used in ways that have unjustified adverse effects on the individuals concerned;
- The lawful purpose for which data are being collected to ensure that the data shall not be further processed in any manner that is contrary to that purpose or the purposes for which the data were collected;
- The extent of information that is required for the purpose as intended and to ensure that they collect adequate and relevant information and prevent any excessive information collection;
- The information retention periods and requirements applicable together with destruction processes and procedures;
- The rights of individuals, i.e. data subjects, in terms of POPI.

POPI compliance, other issues you need to deal with:

- Security measures required to prevent the unauthorised or unlawful processing of personal data/ access to personal data, including accidental loss or destruction or damage to personal data;
- If you transfer data outside the country, to understand the roles, duties and responsibilities of all parties involved; and
- What processes and procedures should be in place to ensure that data is kept up to date and current and accurate at all times.

SECURITY IMPLEMENTATION CHECKLIST			
Premesis	**Date**	**Comment**	**Recommended Intervention**
Inspection of physical security & access	04/04	Secure	
Access conrol, cards, tags & biometrics	04/04	Pin access - change	To be changed every 2 months
Burglar Bars		Not required	
Alarm & deactivation codes		Yes	
Armed response		Yes	
No-go areas, demarcated		N/A	
Risk analysis of security issues		Yes	
Filing and Physical Record keeping			
Locked offices & cabinets		Yes	
No-go areas		N/A	
Proper disposal of records/files/hard copy - shredding policy		Yes	
Work/document flow - data remains secure		Yes - Passwords	
File integrety & lockup		Yes	
Staff			
Keys to authorised employees only		Yes	
Alarm codes		Yes	
Area specif access		Yes	
Staff are aware of their POPI obligations		Yes	
Third Party Processing			
External Operators all have written contracts		Yes	
External Operators are aware of data usage security and limitations		Yes	
External Operators Confidentiality requirements		Yes	
Inspection of 3rd parties premesis, systems & compliance (Monthly)		N/A - International	
IT and Data			
Computers physically secured		Yes	
Password policy		Yes - change every 45 days	
Encription of data		Yes	
Back-ups policy & schedule		Yes	
Person appointed to manage backups		Yes - Grant	
Off-site storage		Cloud	
Proper disposal of damanged devices/data drives		Yes	
Network, Internet & www Security		Yes	
Mobile devices			
No flash drives / removable media in restricted areas		Yes	
Private devices not permitted to sync on networks		Yes	
Laptop - data encripted		Yes	
Laptop - password secured		Yes	
Theft prevention strategy			
Security breaches			
Any loss of data / security breach the regulator		Yes	
Any loss of data / security breach the data subjects		Yes	

POPI COMPLIANCE

The 10 Protection Principles for Responsible Parties

1. Accountability

The **Responsible Party** must ensure compliance. The Responsible Party is required to **audit the processes used to collect, record, store, disseminate and destroy personal information:** in particular, ensure the integrity and safekeeping of personal information in your possession or under your control.

The Responsible Party must take steps to prevent the information being lost or damaged, or unlawfully accessed.

2. Purpose Specification

The Responsible Party must **define the purpose of the information gathering and processing:** personal information must be collected for a specific, explicitly defined and lawful purpose that is related to a function or activity of the company concerned.

3. Processing Limitation

The Responsible Party must ensure **processing is lawful** and:

- Is done in a reasonable manner that does not infringe the privacy of the data subject.
- Must be adequate, relevant and not excessive given the purpose.
- Must have obtained consent or necessity, if consent, it must be *Voluntary, Specific, Informed.*

Data subject consent is required - ***BUT NOT*** if;

- Would prejudice lawful purpose, or
- Information is contained in public record.

What is "**Special Personal Information**"?

- religious or political beliefs
- race or ethnic origin
- trade union membership
- political opinions
- health, sexual life
- criminal behaviour.

4. Take steps to notify the 'data subject'

The individual whose information is being processed has the right to know this is being done and why.

The data subject must be told;

- the name and address of the company processing their information,
- he or she must be informed as to whether the provision of the information is voluntary or mandatory.

5. Further Processing limitation - (limit the processing parameters)

To assess whether further processing is permitted - Ask the following:

- Is there a valid relationship between the purposes?
- What is the nature of information?
- What are the consequences for data subject?
- The manner in which information was collected?
- Are there any contractual rights between the parties?

To check the rationale for any further processing - Ask the following:

- If information is received via a third party for further processing, this further processing must be compatible with the purpose for which the data was *initially* collected.

6. Information quality

The Responsible Party must take reasonably practicable steps to ensure that the information is:

- Complete
- Accurate
- Not misleading; and
- Updated where necessary

Notify the information *Protection Regulator*:

Once POPI is FULLY enacted and a Regulator established, organisations processing personal information will have to notify the Regulator about their actions.

AND

The Responsible Party must take reasonable steps to notify the data subject of:

- Information being collected
- Purpose for which information is collected
- Whether the supply of information is voluntary or mandatory
- The consequences of failure to provide information
- Any particular law that applies

You will only need to notify once, not each instance of processing, but if processing is different than initially notified, you are required to notify within 1 year.

7. Accommodating data subject requests

POPI allows data subjects to make certain requests, *free of charge*, to organisations holding their personal information.

For instance, the data subject has the right to know the identity of all third parties that have had access to their information. A data subject can also ask for a record of the information concerned.

8. Security

The Responsible Party is required to *secure the integrity of personal information* by taking appropriate, reasonable technical and organisational measures to prevent;

- Loss, damage or unauthorised access
- Unlawful access to or processing of personal information

The Responsible Party must take all reasonable measures to;

- Identify all reasonably foreseeable internal and external risks
- Establish and maintain appropriate safeguards against the risks
- Regularly verify that the safeguards are adequately implemented
- Ensure the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards

The Responsible Party must oversee an Operator who processes data on his/her behalf.

Responsible Party must be aware;

- The Operator must treat information confidentially
- The Responsible Party must ensure that the operator establishes and maintains appropriate security safeguards
- *ALL* processing by an operator must be governed by a written contract
- In the event of security breaches, the Responsible Party must notify the Regulator and the data subject

9. Retain records for required periods

- Personal information must be destroyed, deleted or 'de-identified' as soon as the purpose for collecting the information has been achieved.
- However, a record of the information must be retained if an organisation has used it to make a decision about the data subject. The record must be kept for a period long enough for the data subject to request access to it.

10. Cross Border Data Transfer

There are restrictions on the sending of personal information out of South Africa as well as on the transfer of personal information back into South Africa.

The applicable restrictions will depend on the laws of the country to whom the data is transferred or from where the data is returned, as the case may be.

The Responsible Party must institute a written protocol to cover these aspects.

Roles and Responsibilities of an OPERATOR

1. Who is Who

- **Data Subject**: the person to whom the information relates
- **Responsible Party**: The entity which determines the purpose of and means for processing personal information;
- **Operator**: The company or a person who processes personal information for a responsible party *in terms of a contract or mandate*, without coming under the direct authority of the responsible party;
- **Regulator**: The Information Protection Regulator, established by POPI.

2. Duties of an Operator

All Information processed by an operator must be treated in the following manner:

- The Responsible party must be aware of the Operators processing.
- The Operator must treat information confidentially.
- The Responsible party must ensure that the Operator establishes and maintains appropriate security safeguards.
- In the event of security breaches, the Operator via the Responsible party must notify the Regulator and the data subject.
- The processing by an operator must be governed by a written contract between the Responsible party and the Operator.

3. Contents of the Contract

The Contract between Operator and Responsible Party must detail at least the following:

- the legitimate grounds for collecting and using personal data collected,
    - the **lawful purpose** for which data are being collected,
    - the **limit of processing** and prohibiting of further processing,
    - the extent of **information that is required** to prevent any excessive information collection,
    - the information **retention periods** and requirements applicable together with destruction processes and procedures,
    - The **right of individuals to request** such information and query the use thereof,
    - The **security measures** required to prevent the unauthorised or unlawful processing of personal data or access to personal data, including accidental loss or destruction or damage to personal data.

DEALING WITH SPECIAL PERSONAL INFORMATION

1. Religious or Philosophical Beliefs

Processing may take place by:

- Spiritual or religious organisations & institutions, provided that the information concerns data subjects belonging to such organisations; if it is necessary to achieve their aims and principles; or
- To protect the spiritual welfare of the data subjects.

Unless they have objected to the processing.

This information may not be supplied to 3rd parties without the data subject's consent.

2. Race

Processing may be carried out to:

- Identify data subjects when this is essential
- Comply with laws or measures designed to protect or advance persons disadvantaged by unfair discrimination

3. Trade Union Membership

Processing may take place by a trade union to which the data subject belongs, or the trade union federation to which the trade union belongs, if the processing is necessary to achieve the aims of the trade union/trade union federation.

This information may not be supplied to 3rd parties without the data subject's consent.

4. Political Persuasion

Processing may take place by an institution founded on political principles if such processing is necessary to achieve the aims or principles of the institution.

This information may not be supplied to 3rd parties without the data subject's consent.

5. Health or Sexual Life

Processing may take place by:

- Medical practitioners, healthcare institutions
- Insurance companies, medical aid scheme providers
- Schools
- Institutions of probation, child protection or guardianship
- Pension funds and employers if processing is necessary for:
    - Implementation of laws/pension regulations