POPI Employee Guideline

Internal POPIA and PAIA Compliance Processes

Document Number: BMS/EI-MG-013
Revision Number: 2

APPROVAL PAGE

TITLE:	POPIA Employee Guideline
DOCUMENT NUMBER:	BMS/EI-MG-013
REVISION:	2
CLASIFICATION:	Confidential
DATE:	February 2024
MSWORD FILE:	BMS_EI-MG-013_2
AUTHOR (S):	Limpho Matolo, Jeanné Dunbar

APPROVAL:

Limpho Matolo
SHERQ Manager

2024-03-01
Date

Donald McKechnie
Business Unit Executive

2024-03-01
Date

AMENDMENT HISTORY

REVISION	CHANGE HISTORY	Author
1	New Document for Approval	Limpho Matolo
2	PAIA manuals for iST and EI developed and linked into this guideline. Reassignment of 2x previously designated DIOs. PI processing process is updated. Key definitions are added into the document. Incident notification categorisation expanded to include data breaches @ BU level reporting.	Limpho Matolo

TABLE OF CONTENTS

A. GLOSSARY OF TERMS AND DEFINITIONS

BU	Business Unit
Cerebro	An EOH business portal for company training, governance and related processes
EI	Energy Insight (Pty) Ltd
EOH	The holding company of IST and EI
HR	Human Resources
IST	Integrators of Systems Technology (Pty) Ltd
IT	Information Technology
OneDrive	A Microsoft cloud-based file storage platform
PAIA	Promotion of Access to Information Act
PI	Personal Information in terms of POPIA
POPIA	Protection of Personal Information Act, 2013 – South Africa
SAICA	South African Institute of Chartered Accountants
SharePoint	A Microsoft cloud-based service that helps organizations share and manage content, knowledge, and applications
Teams	A Microsoft collaboration platform for business teams
IO	Information Officer
DIO	Deputy Information Officer

TERM	DEFINITION
Data processing	Means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including— • 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; or • Merging, linking, as well as restriction, degradation, erasure or destruction of information.
Data subject	A person that the personal information belongs to or is about. A data subject can be a natural person (i.e. an individual) or a juristic person (i.e. legal entities such as companies), and therefore measures need to be put in place to protect the personal information of both individuals and legal entities.
Data processor	A party who processes personal information on behalf of the responsible party under a contract or mandate.
Information officer	Overall accountable for protection of personal information processed on behalf of the responsible party.
Responsible party	A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
Personal information	Personal information is information relating to an identifiable, living, natural person and, where applicable, an identifiable, existing juristic person. A juristic person includes a company, trust or close corporation.

1. COMPLIANCE FRAMEWORK

1.1. Gathering of Personal Information

1.1.1. Process to gather data and approvals – Employees

- New employees' process – Request employees to complete the required consent forms as part of the Group on boarding requirements (EOH HR – Group process).
- New employees' go through Group POPIA Training via Cerebro – refer to POPIA Employee Consent Form (EOH HR – Group process) and refresher training is conducted from time to time thereafter.
- IST and EI employees complete BMS/EI-F-148 (Consent to Process Personal Information form) before processor can request PI from employees for operational requirements.

1.1.2. Process to gather data and approvals – Clients (Procurement – Group process)

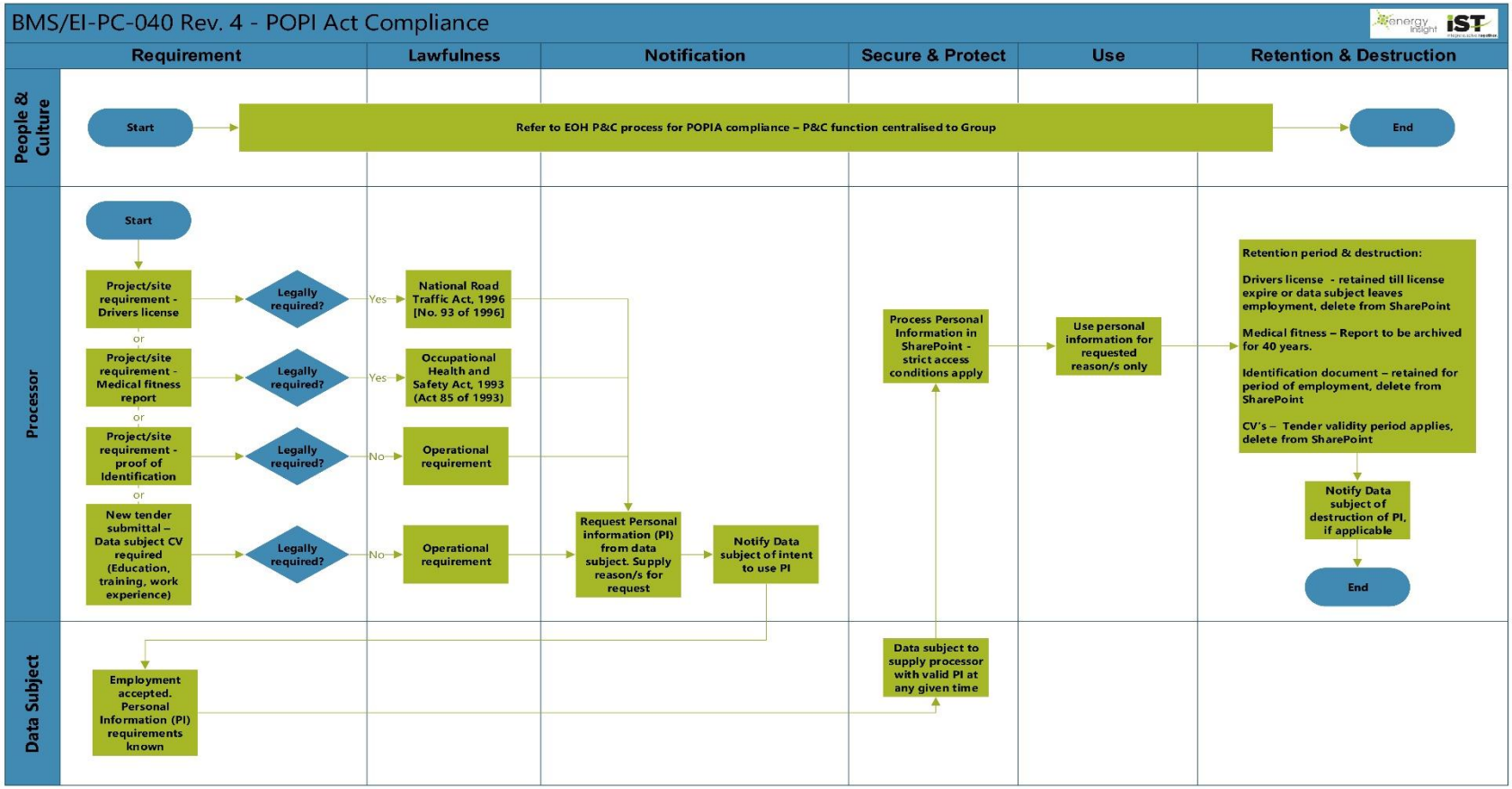
- Information owners will ensure that new clients follow the Procurement and Finance vetting and on boarding compliance processes and completion of the Data Privacy Amendment Contract.
- Close the gap on existing Clients – Information owners in collaboration with EOH Group Procurement to action through Data Privacy Amendment Contract.

1.1.3. Process to gather data and approvals – Creditors/Suppliers (Procurement – Group process)

- New Creditors/Suppliers complete a **Service Level agreement**.
- Close the gap on existing Creditors – EOH Group Procurement to action through Data Privacy Amendment Contract.
- Complete contractor vetting and compliance process.

1.2. Processing of Personal Information

Per system requirements and information flows.



1.3. Retention and Storage of Personal Information

1.3.1. Retention of Personal Information

a. A retention period of 15 years for all Employee Personal Information has been agreed in line with EOH Group HR.

b. In line with SAICA Retention Records Guide the following retention periods need to be upheld in line with relevant laws and/or EOH Shared Services Guidelines.

Relevant Act	Table of Relevant Acts/ EOH Guideline	Retention Period
Auditing Professional Act	Audit related documentation EOH IS Resource Solutions for Recruitment – CV's retention	5 years 3 years
Companies Act, 71 of 2008	Any accounts or records required for the Act, including AFS, minutes of meetings, director resolutions, etc.	7 years
Companies Act, 71 of 2008	Statutory company info	Indefinite
Electronics Communications & Transaction Act, 25 of 2000	Personal information and purpose for which it was collected.	For as long as the information being used or at least 1 year
COIDA: Compensation for Occupational Injuries & Disease Act	Record of earnings of all employees.	4 years after the date of last entry
Basic Conditions of employment Act, 75 of 1997	All Employee information (i.e. details, time, remuneration, etc.)	3 years from last entry and termination
Employment Equity Act	Records of employment equity plan and relevant records.	5 years after plan expiry
Labour Relations Act, 66 of 1995	Employee record of disciplinary transgressions.	Indefinite
Unemployment Insurance Act, 63 of 2001 (UIF)	Record of current employees.	Per income tax Act
Income Tax Act, 58 of 1962	Returns and supporting documents. Employee records and remuneration Payroll information.	5 years from date of submission 15 years
Value Added Tax, 89 of 1991 VAT	Vat vendor records.	5 years from date of submission

c. All Personal Information pertaining to employees and clients may only be stored in company-approved and secured databases:

i. EOH OneDrive, SharePoint and Teams electronic storage.

1.4. Management of Personal Information

1.4.1. Custodians of Personal Information

- BU Heads are the Information custodians for Customer/Client commercial agreements and/or contracts, within their business units.
- Project Managers are the Information custodians for Projects Intellectual property, including related Personal information collected within their areas of responsibility.
- Shared Services including Group Finance are the Information custodians for all financial related information.

1.4.2. Managing documents and Personal Information for electronic documents

This refers to documents and information stored in electronic form on resources such as EOH OneDrive, SharePoint and Teams.

Personal Information	Operator/Processor	Competency Head	SharePoint Folder
Employee Personal Information			
IST			
Tenders SHERQ Files Project/Site requirements Company Vehicles	Analitia Farquharson (BU – PIM) Anita McPherson (BU – PIM) Daniela Strydom (BU – EM) Sharron Klopper (BU – EM)	BU Heads supported by Limpho Matolo	EOH.Sharepoint.com/sites/ist-ei Intranet
EI			
Tenders SHERQ Files Project/Site requirements Company Vehicles	Daniela Strydom Sharron Klopper	BU Heads supported by Limpho Matolo	EOH.Sharepoint.com/sites/ist-ei Intranet

1.4.3. Process to secure Personal Information

- No storage of Personal Information collected and intended for IST & EI processing is permitted on personal laptops or unapproved electronic storage devices – A data merge is conducted to ensure that all information is placed in dedicated folders on SharePoint with restricted access and allocated Information Owners.
- Information owner is responsible for ensuring the integrity and accuracy of the information at all times.
- Information may only be accessed / disseminated for intended purposes with permission from the information owner.

1.4.4. Process to request, access and use Personal Information for internal requirements via Information Owner

- Information Owner must be clear on what consent enables / implies and be clear on how this information may be used and for what reasons.

- Upon request of information, the Information Owner must determine if the request is authorised and within consent parameters and may share / allocate access once verification is done.
- Sharing is only permitted via the secure SharePoint by enabling access to information via approved secure links – no sharing of information / documents, etc. via e-mail. Where the dissemination of information via email is required, an email trail and proof must be kept for track and trace purposes.

1.4.5. Process to retain and dispose of information that has reached retention period

- In reference to the IT data and Record Retention and Disposal Policy, Information will only be stored for the given retention period, as per the Documented Information procedure (BMS-PR-007).
- Continuous checks through internal audit program are executed through the SHERQ department at predetermined intervals to ensure that records that passed retention period are removed and destroyed in accordance with internal standards as set out in applicable procedures.
- Where records have passed expiry but are still required to be retained for whatever reason, the Data Subject will be notified and consent obtained for a retention extension.

1.5. Direct Marketing

- Where the Company is required to perform Direct Marketing, consent for processing Personal Information for the purpose of Direct Marketing will need to be received from the Data Subject.
- The Data Subject will have a reasonable opportunity to freely and informally object to the use of their Personal Information for Direct Marketing.
- The Data Subject will be required to complete BMS/EI-F-148 (Consent to Process Personal Information form), clearly indicating their consent for Direct Marketing purpose.

1.6. Cross-Border Transfers

- As covered per the current Consent to Process Personal Information form, Data Subject consent is in place where, if required for any employment reasons, Personal Information may be transferred cross-border to countries which do not necessarily have data-protection laws similar to South Africa, for verification purposes.
- Such information shall not be retained for periods longer that those allowed in the Republic of South Africa and in line with our internal documentation information policies and procedures.

2. PAIA MANUAL

In reference to EOH Privacy policy and EOH Social Media Policy, as an EOH company, IST and EI are mandated to create a PAIA Manual and make it easily accessible to the Public via the IST and EI websites, to employees via the IST/EI Intranet, as well as have a printed version on hand at designated office facilities.

IST PAIA Manual: BMS-MG-013_1 .pdf
EI PAIA Manual: BMS-MG-013_2.pdf

2.1. Enabling the Rights of Data Subjects

2.1.1. Process to request access to information held by the company, by the data subject

- A Data Subject has the right at any time to ask the Company to provide them with the following:
  - The details of any of their Personal Information which the Company holds on their behalf, and
  - The details as to what the Company has done with the Personal Information

2.1.2. Process to lodge a complaint by the data subject

- A Data Subject has the right to address any complaints to the Information Officer or Deputy Information Officer as a first point of call
- If the Data Subject is not satisfied with the outcomes of this process, they have the right to lodge a complaint with the Information Regulator of South Africa

2.1.3. Process to request the management / updating of personal information by the data subject

- POPIA requires that all Personal Information of Data Subjects and related details supplied, are complete, accurate and up to date.
- Whilst the Company will always use its best endeavours to ensure that Personal Information pertaining to Data Subjects are reliable, it will be the Data Subjects responsibility to advise the Company of any changes to Personal Information, as and when these may occur.

2.1.4. Process to request the deletion of personal information by the data subject

- Personal Information will be safely and securely archived as per the stipulated retention period, in line with the requirements of the SAICA guide on Retention of records, or longer, should any other law applicable in South Africa require this. Thereafter, all Data Subject's Personal Information will be permanently destroyed.
- Where the Data Subject requests the destruction of Personal Information prior to the retention period, the Data Subject must be notified that the Company will still have the right, in terms of POPIA, to retain their information without their consent under any of the following circumstances:
  - Where such retention and use of Personal Information is necessary in order to give effect to a contractual relationship between the Data Subject and the Company
  - Where such retention is required in terms of a law, such as without limiting the generality thereof, the Basic Conditions of Employment Act 75 of 1997 (BCEA), the Skills Development Act, 97 of 1998 (SDA), Skills Development Levies Act, 9 of 1999 (SDLA) the Employment Equity Act, 55 of 1998 (EEA) Unemployment Insurance Contributions Act, 4 of 2002 (UICA), Unemployment Insurance Act, 6 of 2001 (UIF), Financial Advisory and Intermediary Services Act, 37 of 2002 (FAIS), the Financial Intelligence Centre Act 38 of 2001 (FICA), the National Credit Act, 34 of 2005 (NCA) and / or the Compensation for Occupational Injuries and Disease Act, 130 of 1993, or
  - Where such retention is necessary to protect the legitimate interest of the Company or a third party

2.1.5. Process to object to the processing of personal information

- In terms of Section 11 (3) of the POPIA, a Data Subject has the right to object in the prescribed manner to the Company processing their Personal Information.
- The Data Subject is required to submit a request via email to the Deputy IO.
- On receipt of the objection form the Data Subject, the Company will place a hold on any further processing until the cause of the objection has been resolved.

2.1.6. Process to request withdrawal of consent by data subject

- Should a Data Subject refuse to provide the Company with the required Consent and / or information, or withdraw consent, the Company will be unable to assist the Data Subject with employment and / or recruitment requirements or provide the Company's goods or services.
- The Data Subject is required to submit a request via email to the Information Officer (IO) and Deputy IO.
- The consequences of such withdrawal must be communicated to the Data Subject
- Furthermore, the Data Subject must be notified that the Company will still have the right, in terms of POPIA, to process his/her information without their consent under any of the following circumstances:
    - Where such processing and use of Personal Information is necessary to give effect to a contractual relationship between the Data Subject and the Company
    - Where such processing is required in terms of a law; or
    - Where such processing is necessary to protect the legitimate interests of the Company or a third party

2.2. Data Subject Notification of Outcomes

- The Data Subject must be notified by the Company for the following reasons including, but not limited to:
    - Any changes to Personal Information usage, processing and the like;
    - A request for consent to use Personal Information gathered from alternative sources;
    - Request for consent to use Personal Information for purposes other than as stipulated in the prior consent; or
    - General notification on requests/queries raised by a Data Subject.

3. INCIDENT MANAGEMENT PROCESS

IST and Energy Insight are mandated to secure all information in line with the EOH Group IT standards and policies, and to support the facilitation of relevant processes and practices implemented by EOH Group IT to rapidly identify when an Information Security Incident has occurred, to respond thereto and to mitigate the risks associated therewith.

- In the instance of a security or information breach, the Security Incident Management Standard Operating Procedure (EOH 000 ITG SOP 03) will be followed in line with the policies as stipulated above for the following key components:
    - Incident Reporting
    - Incident Assessment
    - Incident Investigation and Response
    - Incident Containment and Recovery
    - Incident Escalation and Notification
    - Review and Control
    - Continuous Improvement
- Report all personal information data breach incidents including near misses on the 'Incident Notification Platform' immediately or latest within 8 hours (same working shift) of occurrence.

  Click here to report:
  Document Management System - Incident Notification Form - All Items (sharepoint.com)

- In terms of escalation and the responsibility of the Information Officer therein, where a potential Breach has occurred, the normal Incident Management and Breach process will be implemented as follows:
    - Group IT Manager informs stakeholders of the reported / identified breach, of which the IST/EI Information officer is included.
    - Group IT Manager will conduct the relevant investigations into the breach.
    - Once determined that Personal Information had in fact been breached, the Information Officer will then step in to ask certain questions relating to the breach, identifying who the Data Subjects are that are impacted and then craft communication to be sent to the impacted Data Subjects as well as the Information Regulator.
- Where a third-party system or supplier has Personal Information and a breach occurs, they will be responsible for informing the IST/EI Information officer accordingly.

4. INFORMATION OFFICERS

Employee Name	Designation	Accountability	BUs/Legal Entities
Donald McKechnie	**Information Officer**	**Overall accountable for POPIA compliance**	**IST & EI**
Limpho Matolo	**Deputy Information Officer**	**Responsible to facilitate the establishment of internal POPIA compliance processes, ensure alignment with Group requirements, and guide implementation across all BUs**	**IST & EI**