Energy Management SA Personal Information Impact Assessment Report

November 2021

TABLE OF CONTENTS

1. COMPANY OVERVIEW

Energy Management SA specialises in utility cost analysis, helping their clients reduce the cost of electricity, sewerage, refuse, property rates and water bills.

By leveraging their 34 years of industry experience, they have reduced their clients' monthly utility expenditure by 10% or more. They have saved their clients in excess of R 300 million.

Their clients rely on them to analyse the impact of utility and demand side management, to implement changes and increase their bottom line.

They offer a contingency based service, which means that their clients don't pay unless they save them money.

2. SCOPE OF THE PIIA

2.1. Scope

The Personal Information Impact Assessment comprises the following activities and outcomes:

- A high level risk assessment.
- An assessment (but not including a detailed cybersecurity risk assessment) of Energy Management SA's systems, technology and information flows.
    - The information management systems that were considered included the storage, use, access, retention, collection, and destruction of data processes.
- A review of any third-party relationships and agreements that may include processing of or access to personal information.

Remediation actions associated with the identified risks have not yet been implemented as of date of this PIIA report and will be planned during the next months.

2.2. Process

Energy Management SA was assisted in compiling this Personal Information Impact Assessment by BizArmour. BizArmour, being experts in the field, advised Energy Management SA and led the process.

BizArmour is a specialist risk management company which focuses on various areas of legal and regulatory compliance, with a specific focus on POPIA, examining legal and compliance risk, reviewing and framing policy on behalf of clients and providing focused awareness and

use-case-specific training along with hands-on guidance to assist organisations in getting their house in order.

In gathering information for the preparation of this report, the primary stakeholders of the Energy Management SA business were consulted through a comprehensive self-assessment questionnaire.

At this stage, we did not complete a detailed review of Energy Management SA's agreements, policies, notices, technology and security systems and processes related to the gathering, storage, retention, destruction, and processing of personal information.

The risk assessment in this report has been based on the input received from Energy Management SA and BizArmour does not accept responsibility for any errors or omissions.

3. PERSONAL INFORMATION

Energy Management SA deals with a combination of standard personal information as well as special personal information of natural persons. Energy Management SA also deals with the personal information of juristic persons for both clients and suppliers of Energy Management SA. The information collected, stored, and processed relates to employees, minors, clients and suppliers.

Personal information of natural persons includes:

- Name and Surname
- Address
- Identification documents
- Banking details
- Photographs
- Videos

Personal information of juristic persons include:

- Public information including company name, email, registration etc.
- Registration documents
- Banking details

Special personal information includes:

- Confidential / privileged information

All information is collected through electronic (activated PDF). The data is stored on paper based and physical files as well as cloud-based storages based outside South Africa.

4. PRIVACY ASSESSMENT

The principles in POPIA provide the legal framework that the organisation must consider. This section provides a clear view of whether the organisation has complied with each principle of POPIA.

Each row in the following table summarises the key requirements of each of the POPIA principles and outlines some key questions or considerations that should be addressed.

The table below also indicates the risk level for each of the principles.

#	Privacy Principle	Personal Information Involved– Use and Process to Manage	Assessment of Compliance	Risk level
1	Principle 1 –Purpose Specification a) Clear lawful purpose. b) Purpose communicated to data subjects. c) Retention period not longer than the existence of the required purpose.	The purpose of collecting the personal information is to conduct utility cost analysis. Employees' data is collected for an effective employee/employer relationship.	a) A lawful purpose exists. b) The purpose is communicated to data subjects. c) Retention period 5 years.	***4.0 Low***

#	Privacy Principle	Personal Information Involved– Use and Process to Manage	Assessment of Compliance	Risk level
2	Principle 2 – Openness a) Notify data subject that data is being collected. b) Notify data subject why information is collected. c) Notify data subject that data is going to be retained. d) Notify the data subject regarding the retention period.	Data subjects are notified about information being collected when engaging the services of the organisation. The organisation has policies in place clearly that define the purpose for collecting the information	*a)* Compliant *b)* Compliant *c)* No declaration of retention. *d)* information is retained for a period of 5 years.	***3.0 Low***
3	Principle 3 – Information Quality a) Information is complete. b) Information is correct. c) Information is up to date. d) Information is not misleading.	Process followed to check quality of data is through collecting it directly from the data subject. Information supplied is updated upon new information conveyed by the data subject. The organisation does not automate any decision making and only human judgment is applied.	a) Minimal information is maintained. b) Information is correct upon collection. c) Information is updated at the request of the data subject. d) Information is clear.	***4.8 Low***

#	Privacy Principle	Personal Information Involved– Use and Process to Manage	Assessment of Compliance	Risk level
4	Principle 4 – Processing limitations a) Only the required information necessary to obtain the purpose is collected. b) Justifiable reasons for collection are recorded. c) Information collected directly from data subjects. d) Informed consent is obtained.	Information is collected directly from the data subjects through electronic (activated PDF) from the data subject when they engage the organisation.	a) Minimal information is obtained. b) The services sought by the data subjects specifies the reasons for collection. c) Compliant. d) Compliant.	***5.9 Medium***

#	Privacy Principle	Personal Information Involved– Use and Process to Manage	Assessment of Compliance	Risk level
5	Principle 5 – Further processing limitations a) Collection of additional information is linked to a specific purpose. b) Further processing is compatible with purpose. c) Identifiable personal information only retained for the period related to specified purpose.	The data subject expects their data to only be used for purposes aligned with the services of Energy Management SA. The employee data subject only expects their data to be used for the purposes of the employment relationship. No data is processed further by third parties.	a) Further processing is linked to purpose. b) The purpose is defined. c) Information is retained during transacting and retained for a further period of 5 years.	***5.0 Medium***

#	Privacy Principle	Personal Information Involved– Use and Process to Manage	Assessment of Compliance	Risk level
6	Principle 6 – Data Subject Participation a) Notify data subjects of process to gain access to information. b) Notify data subjects of process to correct information. c) Notify data subjects of process to destroy information.	The organisation deals with requests for access on a case-by-case basis. There are no documented processes and corrections, and updates are done at the request of data subjects.	a) The process should be documented. b) The process should be documented. c) No process in place.	***5.2 Medium***

#	Privacy Principle	Personal Information Involved– Use and Process to Manage	Assessment of Compliance	Risk level
7	Principle 7 – Security Safeguards a) Ensure integrity and confidentially of collected information. b) Internal risks assessed. c) External risks assessed. d) Breach process.	The organisation safeguards the personal information held, through physical and technical controls that protect the information. Safeguards include: Third party servers, and SSL certificate. Vulnerabilities include no security measures audits, no disaster recovery plan and no preach processes and protocols in place.	a) Some security safeguards are in place b) Non-compliant c) Non-compliant d) No breach process in place.	***7.5 High***
8	Principle 8 – Accountability a) Information officer appointed. b) Information officer registered. c) PIIA completed.	The organisation communicates to the data subjects to whom they disclose the data subjects' information. Data subjects are informed that certain information may be shared with third parties.	a) An information officer has been identified. b) An information officer must be registered with the Information Regulator. c) Compliant.	***4.9 Low to medium***

#	Privacy Principle	Personal Information Involved– Use and Process to Manage	Assessment of Compliance	Risk level
9	Other legislation a) Basic Conditions of Employment Act. b) Labour Relations Act; and c) Promotion of Access to Information Act.	The organisation has to comply with other legislation related to POPIA. The assessment is only with regards to POPIA and where this legislation overlaps with each other.	a) *Not assessed* b) Not assessed c) Not assessed. d) Compliant	2.5 Low

5. KEY RECOMMENDATIONS TO MINIMISE IMPACT ON PRIVACY

The key recommendations to minimise the impact on privacy based on the risk assessment are summarised below:

PLEASE NOTE THAT ITEMS INDICATED IN RED ARE NOT INCLUDED IN THE CURRENT OPTION CHOSEN WITH BIZARMOUR. PLEASE ENQUIRE FOR PRICING DETAILS.

Ref	Recommendation	Agreed Y/N	Completed
R-001	Training is required for employees dealing with data subjects' personal information.		
R-002	POPI specific policies must be drafted and implemented.		
R-003	A breach policy and process should be implemented.		
R-004	An incident register must be maintained.		
R-005	Document retention and destruction processes for personal information should be documented.		
R-006	More controls regarding only collecting information needed for purpose.		
R-007	A PAIA manual to be published		

6. KEY ACTIONS

This section of the report describes what actions are being taken (whether short or long term) and how they will be monitored. Some action link to specific process within the organisation.

Once the PIIA is completed, any on-going privacy monitoring will be incorporated into normal business operations.

The table below sets out the action that will be taken with specific accountable persons and deadlines to ensure such actions are executed successfully.

PLEASE NOTE THAT ITEMS INDICATED IN RED ARE NOT INCLUDED IN THE CURRENT OPTION CHOSEN WITH BIZARMOUR. PLEASE ENQUIRE FOR PRICING DETAILS.

Ref	Agreed action	Who is responsible	Completion Date
A-001	All staff to complete the awareness training.	Energy Management SA	30 November 2021
A-002 A-003	Client to approve that BizArmour provides a third party POPIA compliance declaration and indemnity to Energy Management SA. ENERGY MANAGEMENT SA to submit the declaration for completion to all suppliers.	Energy Management SA Energy Management SA	30 November 2021 TBC
A-004 A-005	BizArmour to draft the following POPI specific policies: ▪ Internal POPI policy ▪ IT Policy ▪ PAIA Manual ENERGY MANAGEMENT SA to implement these policies across the organisation.	BizArmour Energy Management SA	30 November 2021
A-006 A-007	Client to approve BizArmour to provide a breach process and incident register template, which will be maintained by ENERGY MANAGEMENT SA going forward.	Energy Management SA Energy Management SA	30 November 2021
A-008	Client to approve BizArmour to provide a documented retention policy.	Energy Management SA	TBC

A009	Client to implement retention policy	Energy Management SA	
A-010	Publish process for accessing personal information.	Energy Management SA	30 November 2021