Personal Information Impact Assessment

September 2024

LINKTANK

CONTENTS

1. COMPANY OVERVIEW

Linktank supports technology providers, independent financial advice practices, networks and corporate financial services institutions, enabling the journey to provide financial well-being to their clients.

Linktank assists Financial Services Providers in selection, implementation, support, integration, testing, training, support and maintenance of technology solutions that meet their needs.

Services provided by Linktank include:

- Support, testing, training, business consulting and data management services for FSP's

2. SCOPE OF THE PIIA

2.1 SCOPE

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

- A high-level risk assessment through a guided self-assessment tool.
- The self-assessment considered changes in information management from the previous PIIA conducted in 2023

Remediation actions associated with the identified risks were implemented previously. The initial risk ratings and the amended ratings are indicated in this document below.

2.2 PROCESS

To ensure compliance with POPIA requirements, Linktank engaged BizArmour, who advised Linktank and assisted Linktank in compiling this report.

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

A detailed review of Linktank's agreements, policies, notices, technology and security systems and processes related to the gathering, storage, retention, destruction, and processing of personal information was not conducted.

The risk assessments in this report indicate both the initial risk rating as assessed throughout reviews, as well as the current status. All risks have been assigned clear treatment or remediation actions which have, for the most part, been implemented.

3. PERSONAL INFORMATION

Linktank processes personal information for the following categories of data subjects as part of its business operations:

- Employees (natural persons)
- Customers (mainly juristic persons)
- Suppliers (mainly juristic persons)
- Investors (mainly natural persons) – this information is processed on behalf of Linktank's customers as part of a set of data management, transformation and migration services
- System Users (mainly natural persons) – this information is processed as part of system administration services that Linktank performs on behalf of its customers.

Linktank deals with standard personal information of natural persons as well as the personal information of juristic persons for its clients and suppliers. The information collected, stored and processed relates to employees, clients and suppliers.

Linktank previously also dealt with special personal information, but this has not been declared in the 2024 self-assessment and, as such, has been excluded from their risk profile.

Linktank does not provide products or services directly to natural persons and processing of the information of natural persons is either

(a) to fulfil a contracted service where Linktank acts on behalf of a Responsible Party; or (b) where it collects the personal information of officers or directors of any juristic person they engage with.

Personal information of natural persons includes:

- Name and Surname;
- Address;
- Identification documents;
- Photos/videos

Personal information of juristic persons includes:

- Registration documents
- Banking details;

In previous assessments, additional categories of personal information included the following, but it appears that these have now been abandoned:

- Public information (company name/emails/company registration number);
- Payment facilities;
- Credit information

- Banking details;
- Payment facilities;
- Confidential/privileged information;
- Trademark data;
- Race or ethnic origin

Where juristic persons engage with Linktank, all information is collected directly from the data subjects, electronically only.

Linktank previously followed a 'cloud-first' strategy, and all its systems and services were contracted with leading Software as a Service (SaaS) or Platform as a Service (PaaS) providers. Currently, all data is stored only on cloud-based servers outside of South Africa. It was declared that this is subject to the following security measures:

- Restricted permissions and/or access control;
- Authentication controls/passwords;
- Multi-factor authentications;
- Encryptions;
- Data loss prevention (DLP) software;
- Emails are automatically scanned for malware etc.;
- Endpoint protection for PCs, laptops and mobile devices;
- Strict information security policies; and
- Security-certified cloud services

Linktank also provides specialist consulting services which include migration, transformation and transportation of data and system administration for the XPLAN system where personal information is processed on behalf of Linktank clients.

All information is transferred securely according to Linktank's policies and procedures.

Minimal juristic personal information is shared with Linktank's UK partner, Evotra. In such circumstances, equal security measures and privacy principles are adhered to in compliance with POPIA. No personal information of EU or UK subjects is processed.

4. PRIVACY RISK 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.

4.1 OVERALL RISK SUMMARY

The graph below illustrates the summary risk levels assessed for each of the POPIA conditions and certain additional considerations. It indicates the scoring at the start of the POPIA readiness project (July 2021) compared to the re-assessment in November 2021 and the current status (July 2023).

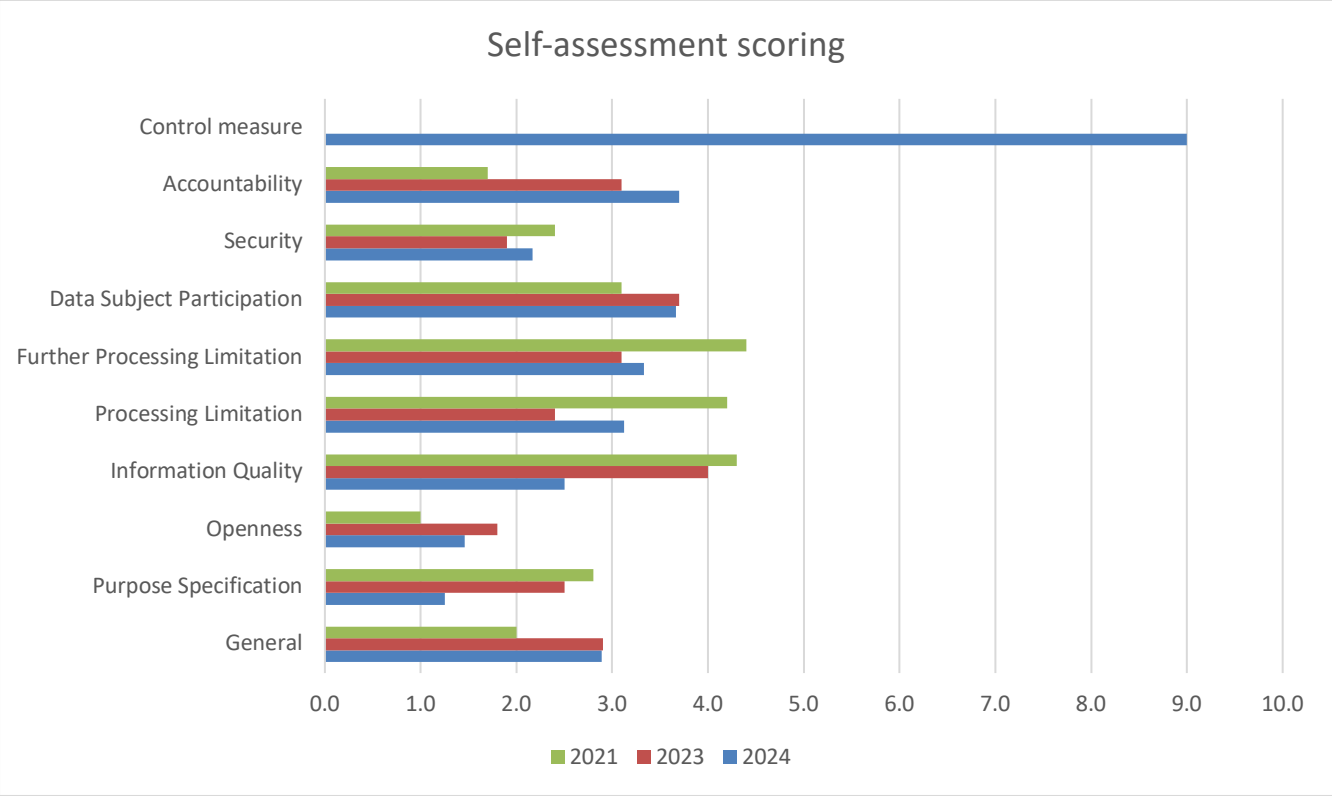

Figure 1 – Assessed Risk Summary by Condition / Area

The 'General' item above considers the size of the company, the number of data subjects' information processed and other factors. The risk in this area is low which is in line with the inherent risk rating.

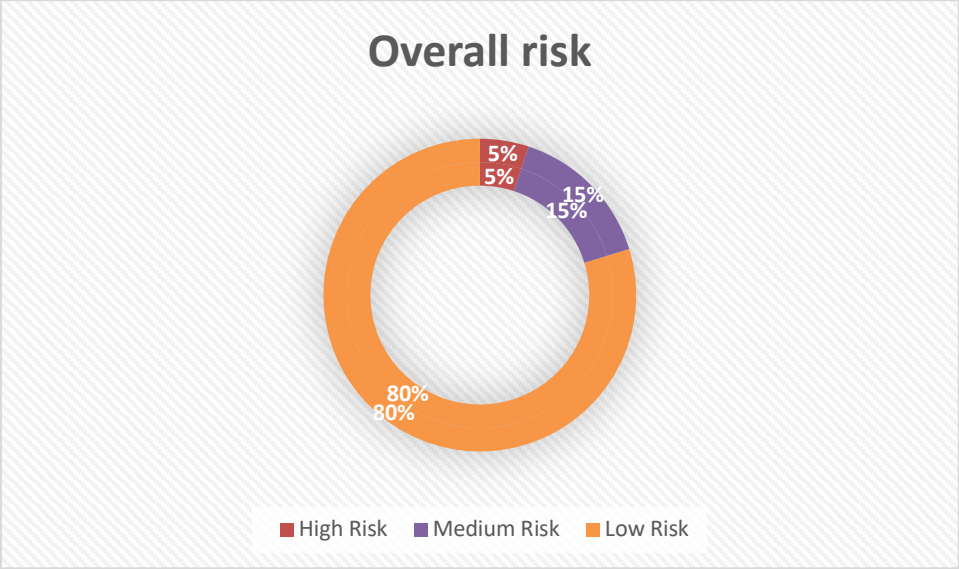

Figure 2 – Assessed Risk Summary by Risk Level as at September 2024

The table below summarises the findings of the assessment conducted, in relation to each of the POPIA conditions. It sets out the key requirements identified at the start of the project and indicates what has been completed. The comparative scoring over the three assessments is indicated:

Table 1 – Assessed Risk by Condition with Status and Treatment / Mitigation

Privacy Condition / Principle	Assessed State Including Mitigation or Treatment	Risk Score		
		Sep 24	Jul 23	Nov 21
Condition 1 – Accountability				
1.1. Information officer appointed, trained, and fulfilling their tasks.	1.1. Information Officer appointed and registered	3.7 LOW – MEDIUM	3.1 LOW	1.7 LOW
1.2. PAIA manual and training	1.2. Compliant			
1.3. PIIA completed.	1.3. Compliant			
1.4. Incident Response Policy	1.4. Compliant			
1.4. POPIA Policy	1.4. Compliant			
1.6. POPIA Awareness and Training	1.5. Compliant.			
Condition 2 – Processing Limitation				
2.1. Only required information necessary to achieve the purpose is collected.	2.1. Control and definition implemented. Notice of processing and consent to data subjects.	3.1 LOW	2.4 LOW	4.2 LOW - MEDIUM
2.2. Justifiable reasons for collection are recorded.	2.2. Forms for collection of information specify reasons. Information processed on behalf of third parties is provided based on agreements. No sensitive personal information is collected. Reasons are clearly defined.			
2.3. Information collected directly from data subjects.	2.3. Compliant.			
2.4. Informed consent is obtained.	2.4. All agreements and contracts include specific contractual clauses or data processing agreements.			
2.5. Access is restricted	2.5. Access is strictly managed.			
2.6. Retention of Personal Information is defined.	2.6. Data Classification and Data Retention policies are in place.			

Privacy Condition / Principle	Assessed State Including Mitigation or Treatment	Risk Score		
		Sep 24	Jul 23	Nov 21
Condition 3 – Purpose Specification				
3.1. Personal information is collected for a clear lawful purpose.	3.1. All processing performed based on agreements or contracts.	1.3 LOW	2.5 LOW	2.8 LOW
3.2. The purpose for processing is clearly recorded.	3.2. All forms and agreements contain notice and consent for processing.			
3.3. This purpose is communicated to data subjects.	3.3. All forms and agreements contain notice and consent for processing.			
3.4. Contracts and Policies reviewed for POPIA	3.4. Full reviews performed in 2021. Consider additional reviews for any updated documents.			
Condition 4 – Further processing limitation				
4.1. Further processing to be compatible with purpose of collection	4.1. Compliant – processing is done based on agreements which specify Linktank's role as Operator or Joint-Responsible party.	3,3 LOW	3.1 LOW	4.4 MEDIUM
4.2. Third parties process personal information of Linktank clients	4.2. It appears that this is no longer the case. Previously contractual clauses and Operator Agreements mitigated this risk.			
4.3. Third-parties processing Linktank client data are bound by contract to restrict further processing.	4.3. It appears that this is no longer the case. Previously contractual obligations were in place to restrict further processing.			
4.4. Direct Marketing	4.4. Direct marketing is only performed via social media and subject to both opt-in and opt-out options.			
4.5. Storage is controlled to ensure no misuse	4.5. Very little paper use. ZOHO CRM implemented consistently. Information storage cloud-based with restricted access.			
Condition 5 – Information Quality				
5.1. Collection mechanisms / methods	5.1. Information received exclusively via electronic means. Ensure to review cyber security risks regularly.	2.5 LOW	4.0 MEDIUM-LOW	4.3 MEDIUM-LOW
5.2. Regular Update of information	5.2. Ad-hoc (upon request). Guided by processing purposes. Consider additional communication to data subjects to ensure information quality remains up to date.			
5.3. Destruction of old or unused information	5.3. Retention policy defined and implemented.			

Privacy Condition / Principle	Assessed State Including Mitigation or Treatment	Risk Score		
		Sep 24	Jul 23	Nov 21
Condition 6 – Openness				
6.1. Data subject notified when collecting information	6.1. Forms and consent notices have been implemented.	1.5 LOW	1.8 LOW	1.0 LOW
6.2. Monitoring of staff emails and devices	6.2. No monitoring is performed.			
6.3. Publishing of client / employee information	6.3. Yes and consent mechanisms have been created with consent management software managing the consent.			
6.4. Privacy Notices	6.4. Privacy notice available on website and email notice is in place.			
Condition 7 – Security Safeguards				
7.1. Third-party contracts commit operator to same standards as responsible party	7.1. Contracts include Data Processing / Operator agreement or appropriate POPIA clauses.	2.2 LOW	1.9 LOW	2.4 LOW
7.2. Security mechanisms – data protection	7.2. Secure online storage and processing. Laptops are secured. Strict access control applied. Backup and encryption of laptops have been increased including the implementation of DLP.			
7.3. Security audits, risks assessed.	7.3. Security policy updates (Acceptable Usage). Security audit and cybersecurity assessment to be conducted annually.			
7.4. Security Policies and Procedures	7.4. Security policies and procedures are defined – to be reviewed and enhanced as necessary.			
7.5. BCP and Disaster Recovery	7.5. Policy and procedure defined. Since Linktank is fully remote, cloud only, testing requirements are minimal and performed annually.			
7.6. Incident and breach response and notification	7.6. Incident Management and breach policy and procedures implemented.			

Privacy Condition / Principle	Assessed State Including Mitigation or Treatment	Risk Score		
		Sep 24	Jul 23	Nov 21
Condition 8 – Data Subject Participation				
8.1. Data subjects are informed about the information recorded and processed as well as purpose of processing.	8.1. All engagement mechanisms, including forms, application and contracts ensure notice and consent. Consent management software has been implemented to assist with this requirement.	3.7 LOW	3.7 LOW-MEDIUM	3.1 LOW - MEDIUM
8.2. Data subjects provide clear and explicit consent (opt-in) for all personal information gathered.	8.2. All engagement mechanisms, including forms and contracts ensure notice and consent.			
8.3. Clear plans and mechanisms to respond to requests by data subjects to access their data.	8.3. Internal processes and systems in place. All personal information is recorded securely and electronically with secure transfer mechanisms to and from third parties.			
8.4. Data Subjects are notified of process to gain access to information.	8.4. Privacy notices and PAIA Manual in place. Consider regular communication with data subjects to ensure continued transparency.			
8.5. Data Subjects are notified of process to correct their personal information.	8.5. The nature of the business does not require significant data subject participation. Regular communication with existing data subjects should be considered.			
8.6. Notify data subjects of process to destroy data.	8.6. Data Retention & Disposal policy in place.			
General				
9.1. Promotion of Access to Information Act.	9.1 Compliant.	2.9 LOW	2.9 LOW	2.0 LOW

5. KEY ACTIONS TAKEN FOR COMPLIANCE

BizArmour's assessment of risk in accordance with the information provided by Linktank provided several key recommendations. These are summarised below along with the recommended activity to be undertaken.

5.1 PRIMARY RECOMMENDATIONS

Ref	Continued actions to ensure POPIA compliance is maintained
R-001	Training is required for any new employees dealing with data subjects' personal information.
R-002	Registration of the information officer must be done annually via the Information Officer's portal.
R-003	Annual PAIA reports have to be submitted on the Information Regulator's portal.
R-004	Perform an annual POPIA risk assessment to ensure any changes or updates within the organisation remains POPIA compliant.
R-005	Any updates or changes of access rights to personal information should be documented and processes put in place regarding authorised access.
R-006	Continuously ensure that third parties declare their POPI compliance to Linktank.
R-007	Consider additional communication to data subjects to ensure information quality remains up to date. Regular communication with data subjects will also ensure continued transparency.
R-008	Regular reviews of cyber security measures should be in place.
R-009	Where any new documentation or procedures are implemented, these should be reviewed for POPIA compliance.

6. CONCLUSION

Linktank takes its responsibilities regarding the protection of personal information seriously and has undertaken a thorough process to ensure compliance with POPIA as well as being able to demonstrate good governance.

At the time of the creation of this PIIA, all known risks have been assessed and remediated as fully as possible. Additional recommendations may be implemented over the coming months. Ongoing application of policy and procedures will ensure continued compliance and governance.

ANNEXURE A – FLOW OF PERSONAL INFORMATION

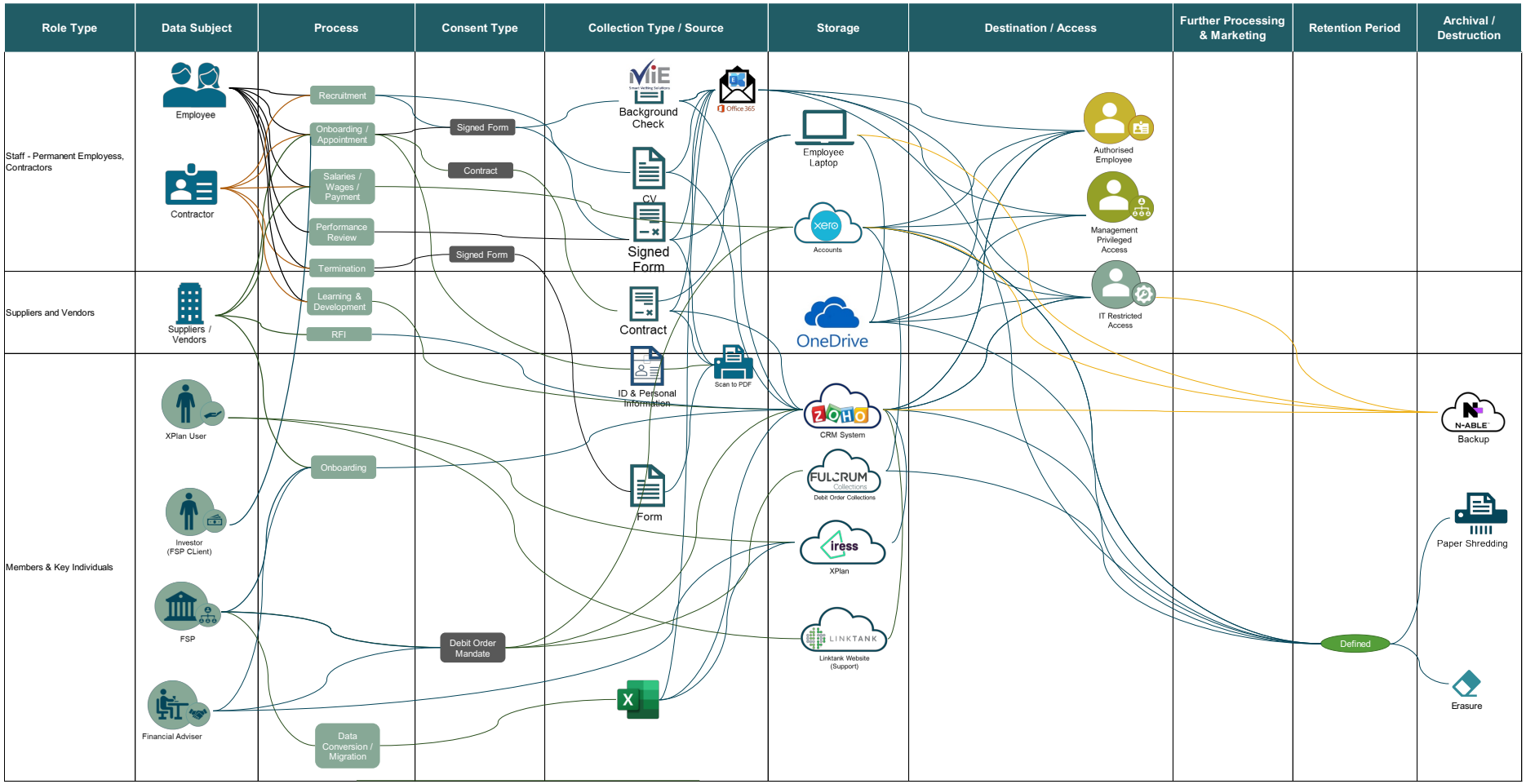

Figure 3 – High level illustration of Linktank's information flows