



INFINOX CAPITAL LIMITED SA (PTY) LTD  
2018/616118/07

**DATA PRIVACY POLICY**

*An authorised Financial Services Provider FSP No: 50506*

**JULY 2022**

## **Table of Contents**

1. Why we have this policy	3
2. The Scope of this policy	3
3. Why is it important to comply with this policy	3
3.1 If the organisation does not comply	3
3.2 If you do not comply	3
4. Our Policy	3
4.1 We follow the principle of data privacy	3
4.2 We conduct personal information impact assessment	6
5. Roles and Responsibility	7
6. Our policy glossary	8
7. Supporting Documents	10
8. Document Metadata	11

## 1. Why we have this policy

We have this policy to help guide our actions so that we keep our customers, employees and suppliers/service providers data safe, protect our reputation, and comply with all relevant data protection regulations, including the Protection of Personal Information Act (POPIA).

## 2. The Scope of this policy

This policy applies to:

- Any activity where we produce or use personal information (processing activities);
- Anybody involved in processing activities where we produce or use personal information;
- All employees, service providers, contractors, and other individuals who have access to personal information.

## 3. Why is it important to comply with this policy

### 3.1 If the organisation does not comply

Our reputation is our biggest asset. Without our reputation, our relationships with key stakeholders and investors would suffer. In addition, we could face substantial fines.

### 3.2 If you do not comply

This organisation only works when we all do our part, and all of us want to see the organisation succeed. If you do not comply with this policy, or if you discover that we are not complying with the policy and you do not tell us about it, you could face disciplinary action.

## 4. Our Policy

While all personal information should be protected, we take a risk-based approach to compliance. We prioritise the protection of personal information that is used in our important business activities, and in activities that could have a substantial impact on a data subject's right to privacy.

It is our policy to:

- follow the principles of privacy protection that are set out in the POPIA; and
- conduct data protection impact assessments.

### 4.1 We follow the principle of data privacy

THE PRINCIPLE	WHAT WE DO
Classify personal information	We identify and classify the personal information that we use and produce.

Document processing activities	We document all processing activities to ensure that we can respond to requests from the Information Regulator and requests for information by data subjects or third parties.
Specify the purpose for processing	We specify and document the purposes for which we process personal information.
Provide legal basis for processing activities	<p>We ensure that:</p> <ul style="list-style-type: none"> <li>• All processing activities have a legal basis; and</li> <li>• We document the specific legal basis for processing personal information for each activity.</li> </ul>
Keep processing to a minimum	<p>We ensure that:</p> <ul style="list-style-type: none"> <li>• we process personal information that is adequate, relevant, and not excessive, considering the purpose of the activity; and</li> <li>• we de-identify personal information before we start the activity where possible. Where de-identification is not possible, we must consider masking the personal information.</li> </ul>
Obtain personal information from lawful sources	<p>We obtain personal information from lawful sources only.</p> <p>Lawful sources of personal information include:</p> <ul style="list-style-type: none"> <li>• The data subject;</li> <li>• information that the data subject made public deliberately;</li> <li>• public records; and</li> <li>• a source that the data subject consented to.</li> </ul> <p>Other sources may be lawful in special circumstances. If you are unsure, speak to the Deputy Information Officer.</p>
Process transparently	We disclose all processing activities to data subjects in our privacy notices.
Ensure personal information quality	We take reasonable steps to ensure that personal information is complete, accurate, not misleading, and updated when necessary.
Limit sharing	<p>We only share personal information if it is legal to do so and ethically justifiable. We:</p> <ul style="list-style-type: none"> <li>• identify all instances when personal</li> </ul>

	<p>information is shared with external organisations or individuals (third parties);</p> <ul style="list-style-type: none"> <li>● ensure that sharing personal information complies with data protection legislation and the Information Sharing Procedure;</li> <li>● enter into appropriate contracts and take additional steps that may be necessary to reduce the risk created by sharing personal information;</li> <li>● conduct an information sharing assessment to determine who is responsible to ensure that contracts are concluded, who must review the contracts, and whether we must take additional steps to reduce the risks created by sharing;</li> <li>● keep record of personal information sharing activities, including the outcome of assessments, a record of additional steps taken, what personal information was shared and when, and the method we used to share the personal information.</li> </ul>
<p>Keep personal information secure</p>	<p>We protect all personal information that we use and produce against breaches of confidentiality, failures of integrity, or interruptions to the availability of that information.</p> <p>All personal information processing must comply with our Information Security Management Policy.</p>
<p>Manage personal information incidents</p>	<p>All employees must report incidents in accordance with our Information Security Management Policy and Incident Management Procedure.</p> <p>An incident includes:</p> <ul style="list-style-type: none"> <li>● non-compliance with this policy and any procedures that relate to it;</li> <li>● contraventions of any data protection legislation such as the POPIA; and</li> <li>● security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availability of personal information.</li> </ul> <p>Employees must immediately report:</p> <ul style="list-style-type: none"> <li>● any known or suspected incidents; or</li> <li>● any circumstances that increase the risk of an incident occurring.</li> </ul> <p>Reports must be sent to <a href="mailto:dany.mawas@infinox.com">dany.mawas@infinox.com</a></p>
<p>Manage retention periods</p>	<p>We ensure that all records:</p> <ul style="list-style-type: none"> <li>● are managed appropriately and in accordance with any operational or</li> </ul>

	<p>legal rules that may apply; and</p> <ul style="list-style-type: none"> <li>● comply with our Records Management Policy.</li> </ul>
Respect data subjects' rights	<p>We respect the rights of data subjects to:</p> <ul style="list-style-type: none"> <li>● access their records;</li> <li>● know who their information was shared with;</li> <li>● correct or delete inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or illegally obtained information;</li> <li>● withdraw consent; and</li> <li>● object to the processing of their information when it is not necessary for the conclusion or performance of a contract or to comply with an obligation imposed by law.</li> </ul> <p>All data subject requests must go through the Data Subject Request Procedure.</p>

## 4.2 We conduct personal information impact assessment

Senior Management must ensure that a personal information impact assessment is done before we start a new processing activity. The data protection impact assessment must include a risk analysis of the activity.

We must conduct a personal information impact assessment before we:

- continue to process personal information as part of an activity that has not undergone a data protection impact assessment before;
- change an existing processing activity;
- launch a new product or service;
- expand into other countries;
- use new systems or software for processing personal information; or
- share personal information with third parties.

A personal information impact assessment has three phases:

- Identify activities in which personal information is processed.
- Complete the data protection impact assessment questionnaire to document the activity, classify information, and perform a risk-rating for the activity.
- Complete a further investigation and assessment with assistance from the Deputy Information Officer if the activity had a risk rating of high or critical after the data protection impact assessment questionnaire was completed.

All activities that are rated as critical or high risk during the data protection impact assessment must undergo an assessment every three years.

## 5. Roles and Responsibility

These are the responsibilities in respect of this policy:

<p>The Information Officer (<i>Dany Mawas</i>)</p>	<p>Our Regional Director for Africa is our Information Officer. The Information Officer has a coordinating function that focuses on the policy-based protection of our information and is the policy owner of this policy.</p> <p>The Information Officer must ensure that this policy receives support from senior management throughout the organisation and that senior management discharges their responsibilities.</p>
<p>Deputy Information Officers (<i>Catia Merola</i>)</p>	<p>Deputy Information Officers must support the Information Officer and are responsible for strategic guidance to the organisation on data privacy risk management.</p> <p>The Deputy Information Officers must:</p> <ul style="list-style-type: none"> <li>● oversee the implementation of this policy,</li> <li>● develop procedures and standards to support data privacy,</li> <li>● provide advice on the identification and management of data privacy risk,</li> <li>● monitor whether personal information impact assessments are performed when required,</li> <li>● develop training on data privacy,</li> <li>● respond to data subject requests and objections,</li> <li>● respond to requests from the information regulators and working with regulators when there is an investigation,</li> <li>● monitor whether this policy is implemented throughout the organisation.</li> </ul>
<p>Director of IT</p>	<p>The Director of IT supports the Information Officer and the Deputy Information Officers by:</p> <ul style="list-style-type: none"> <li>● developing Information Technology policies, procedures, standards and guidelines;</li> <li>● providing technical advice on data privacy;</li> <li>● supporting the implementation of this policy through appropriate technology investments;</li> <li>● ensuring that the organisation only invests in information technology that complies with this policy.</li> </ul>
<p>Senior Management</p>	<p>Senior Management must implement this policy, create or align other policies and processes in their business areas with this policy, and monitor and advocate for compliance within their business areas.</p> <p>Senior Management must ensure that:</p>

- business areas comply with this policy;
- a register of information assets used in important information processing activities in their business area is created and maintained;
- information used in important information processing activities is classified;
- personal information impact assessments are conducted before confidential and personal information is processed;
- data privacy-related risks in their business area are managed; and
- their business area participates in investigations into incidents.

Users of information

All users who have access to the organisation’s information or information systems must:

- adhere to all policies, procedures and guidelines that relate to the use of information; and
- report any actual or suspected incidents.

Internal and external audit

Internal and external audit provides independent assurance that the organisation’s risk management, governance and internal control processes are operating effectively, including compliance with this policy.

## 6. Our policy glossary

Data subjects

The person or organisation to whom personal information relates. This includes:

- prospective customers
- customers;
- staff members and job applicants;
- service providers, contractors, and suppliers;
- shareholders and directors; and
- members of the public and visitors.

Incident

An incident includes:

- non-compliance with this policy and any procedures relating to it;
- contraventions of any data protection legislation such as the POPIA; and
- security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availability of personal information.



## Processing activities

Processing activities are a collection of interrelated work tasks that achieve a specific result during which personal information is created, collected, used, shared, transformed, stored, or destroyed.

A processing activity is important if we could experience critical or high levels of risk if the process or activity is disrupted or could no longer continue.

---

## Personal information

Personal information means any information relating to an identifiable individual (living or deceased) or an existing organisation (a company, public body, etc.). This includes the personal information of all customers, staff members, job applicants, shareholders, board members, service providers, contractors, suppliers, members of the public, and visitors.

Examples include:

- identifiers, such as a name, identity number, staff number, account number, customer number, company registration number, tax number, photos, videos, or any other unique information that can be used to identify a person;
  - demographic information, such as race, gender, sex, pregnancy, marital status, national or ethnic or social origin, colour, sexual orientation, age, religion, conscience, belief, culture, language, and birth;
  - information relating to physical or mental health, wellbeing, or disability;
  - background information, such as education, financial, employment, medical, criminal or credit history;
  - contact details, such as physical and postal address, email address, telephone number, online identifier (e.g. a person's twitter handle) or location information;
  - biometric information: this refers to techniques of identification that are based on physical, physiological, or behavioral characterisation, such as blood-typing, fingerprinting, DNA analysis, retinal scanning, facial recognition, and voice recognition;
  - someone's opinions, views, and preferences;
  - private or confidential correspondence and any further correspondence that would reveal the contents of the original correspondence;
  - views or opinions about a person, such as interview notes and trade references; and
-

---

	<ul style="list-style-type: none"> <li>● the criminal behavior of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject.</li> </ul>
<hr/>	
POPIA	The Protection of Personal Information Act 4 of 2013 and its regulations
<hr/>	
POPIA Programme	<p>The POPIA Programme is our ongoing efforts to comply with the provisions of the POPIA and includes:</p> <ul style="list-style-type: none"> <li>● stakeholder consultation;</li> <li>● defining roles and responsibilities;</li> <li>● policy development;</li> <li>● policy implementation;</li> <li>● monitoring and audit; and</li> <li>● continual improvement.</li> </ul>
<hr/>	
Processing	<p>Any operation or activity or any set of operations concerning personal information, including:</p> <ul style="list-style-type: none"> <li>● collecting, receiving, recording, organising, collating, storing, updating or modifying, retrieving, altering, consulting, or using;</li> <li>● disseminating by means of transmission, distributing, or making available in any other form; or</li> <li>● merging, linking, restricting, degrading, erasing, or destroying personal information.</li> </ul>
<hr/>	

## 7. Supporting Documents

You must read this policy with:

- Data Subject Request Procedure
- Personal Information Impact Assessment Procedure and assessment

## 8. Document Metadata

Document number:	<b>#1</b>
Document version:	<b>V1.2</b>
Document approval authority:	<b>Jay Mawji</b>
Document approval date:	<b>July 2022</b>
Document owner:	<b>Catia Merola</b>
Document author(s):	<b>Catia Merola</b>
Last updated:	<b>June 2021</b>
Next review date:	<b>July 2023</b>
Visibility (where will it be displayed):	<b>Website</b>