# The Moonstone Group of Companies

# DATA PRIVACY POLICY

At the Moonstone Group of Companies, we value the trust our clients, employees and service providers place in us when they share their personal information with us. Without this personal information, we would not be able to function effectively, so it is crucial that we protect it in accordance with the guidelines set out in the Protection of Personal Information Act (POPIA) and other privacy regulations. This policy sets out how we achieve that.

| | |
|---|---|
| Version | 2021.06 (v.2) |
| Publishing Date | 2021.06 |
| Last Review Date | 2021.04 |
| Frequency of Review | Bi-Annually |
| Next Review Date | November 2021 |
| Policy Owner | The Moonstone Group of Companies |
| Responsible Business Unit | Moonstone Compliance (Pty) Ltd, Moonstone Information Refinery (Pty) Ltd, Moonstone Business School of Excellence (Pty) Ltd., Moonstone Software Solutions (Pty) Ltd., Moonstone Business Solutions (Pty) Ltd |

# Table of Contents

## CONTROL MEASURES

- Establish a Compliance Management Framework for the organisation.
- Implement control measures (actions, activities, processes and/or procedures) that will provide reasonable assurance that the organisation's compliance obligations are met and that non-compliances are prevented, detected and corrected.
- Control measures must be periodically evaluated and tested to ensure their continuing effectiveness.

| Action / Activity / Process / Procedure | Control Owner |
|---|---|
| Bi-Annual Review | Hjalmar Francois Otto Bekker |
| Information Officer | Hjalmar Francois Otto Bekker |
| Deputy Information Officer | Jean-Marié Tosen |
| POPI Audit | Jean-Marié Tosen |
| POPI Awareness Training | Jean-Marié Tosen |

**POLICY STATEMENT**

- This policy forms part of the policy owner's internal business processes and procedures.
- Any reference to the "organisation" or "we/us" is a direct reference to "The Moonstone Group of Companies", which in turn refers to Moonstone Information Refinery (Pty) Ltd, Moonstone Compliance (Pty) Ltd, Moonstone Business School of Excellence (Pty) Ltd, Moonstone Software Solutions (Pty) Ltd, Moonstone Business Solutions (Pty) Ltd and any subsequent subsidiary or holding company of the Moonstone Group which may be incorporated or registered after the date on which this Policy was adopted.
- Any reference to the "organisation" also refers to the "policy owner".
- The organisation's governing body, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of the organisation are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.
- Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

**POLICY ADOPTION**

By signing this document, I authorise the policy owner's approval and adoption of the processes and procedures outlined herein.

| | |
|---|---|
| Name & Surname | Hjalmar Francois Otto Bekker |
| Capacity | Chief Executive Officer / Information Officer |
| Signature |  |
| Date | 29-06-2021 |

## 1. WHY WE HAVE THIS POLICY

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

## 2. 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; and
- All employees, service providers, contractors, and other individuals who have access to personal information.

## 3. WHY IT IS 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

The 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 Act; and
- Conduct data protection impact assessments.

### 4.1 We follow the principles 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 a legal basis for processing activities** | We ensure that: |

| | |
|---|---|
| | • All processing activities have a legal basis; and<br>• We document the specific legal basis for processing personal information for each activity. |
| **Keep processing to a minimum** | We ensure that:<br>• We process personal information that is adequate, relevant and not excessive, considering the purpose of the activity; and<br>• 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. |
| **Obtain personal information from lawful sources** | We obtain personal information from lawful sources only.<br>Lawful sources of personal information include:<br>• The data subject;<br>• Information that the data subject made public deliberately;<br>• Public records; and<br>• A source that the data subject has consented to.<br>Other sources may be lawful in special circumstances. If you are unsure, speak to the Deputy Information Officer. |
| **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** | We only share personal information if it is legal to do so and ethically justifiable. We:<br>• Identify all instances when personal information is shared with external organisations or individuals (third parties);<br>• Ensure that sharing personal information complies with data protection legislation and the Information Sharing Procedure;<br>• Enter into appropriate contracts and take additional steps that may be necessary to reduce the risk created by sharing personal information; |

| | |
|---|---|
| | • Conduct an information sharing assessment through the completion of the Information Sharing Checklist on the PrivIQ platform 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 risk created by sharing;<br>• 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. |
| **Keep personal information secure** | 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. |
| **Manage personal information incidents** | All employees must report incidents in accordance with our Information Security Management Policy and Incident Management Procedure.<br>An incident includes:<br>• Non-compliance with this policy and any procedures that relate to it;<br>• Contraventions of any data protection legislated such as the POPI Act; and<br>• Security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availability of personal information.<br>Employees must immediately report:<br>• Any known or suspected incidents; or<br>• Any circumstances that increase the risk of incident occurring.<br>Reports must be sent to Jmtosen@moonstonecompliance.co.za |
| **Manage retention periods** | We ensure that all records are managed appropriately and in accordance with any operational or legal rules that may apply. |
| **Respect data subjects' rights** | We respect the rights of data subjects to:<br>• Access their records;<br>• Know who their information was shared with; |

| | |
|---|---|
| | • Correct or delete inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or illegally obtained information;<br>• Withdraw consent; and<br>• 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.<br>All data subject requests must go through the Data Subject Request Procedure. |

### 4.2 We conduct personal information impact assessments

Senior Management must ensure that a personal information impact assessment is done before starting 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:

- 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**:

1. Identify activities in which personal information is processed.
2. Complete the data protection impact assessment questionnaire to document the activity, classify information, and perform a risk-rating for the activity.
3. 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 RESPONSIBILITIES

These are the responsibilities in respect of this policy:

| | |
|---|---|
| **The Information Officer (CEO – Hjalmar Bekker)** | The Chief Executive Officer of the Moonstone Group of Companies is our Information Officer. The Information Officer has a co-ordinating function that focuses on the policy-based protection of our information and is the policy owner of this policy.<br>The Information Officer must ensure that this policy receives support from senior management throughout the |

| | |
|---|---|
| | Organisation and that senior management discharges their responsibilities. |
| **Deputy Information Officer (Jean-Marié Tosen)** | The Deputy Information Officer of the Moonstone Group of Companies is Jean-Marie Tosen.<br><br>The Deputy Information Officer must support the Information Officer, and is responsible for strategic guidance to the Organisation on data privacy risk management.<br><br>The Deputy Information Officer must:<br>• Oversee the implementation of this policy;<br>• Develop procedures and standards to support data privacy;<br>• Provide advice on the identification and management of data privacy risk;<br>• Monitor whether personal information impact assessments are performed when required;<br>• Develop training on data privacy;<br>• Respond to data subject requests and objections;<br>• Respond to requests from the information regulators and working with regulators when there is an investigation;<br>• Monitor whether this policy is implemented throughout the Organisation. |
| **IT Manager (Marius Rall)** | The IT Manager supports the Information Officer and the Deputy Information Officer by:<br>• Developing Information Technology policies, procedures, standards and guidelines;<br>• Providing technical advice on data privacy;<br>• Supporting the implementation of this policy through appropriate technology investments;<br>• Ensuring that the Organisation only invests in information technology that complies with this policy. |
| **Legal and Compliance Advisor (Jean-Marié Tosen)** | The Legal and Compliance Advisor:<br>• Oversees the management of data privacy – related legal obligations; |

| | |
|---|---|
| | • Ensures that appropriate contracts with third parties are concluded;<br>• Ensures that employees are aware of contractual obligations and their responsibilities;<br>• Provide legal advice on the interpretation of legislation; and<br>• Manages legal risks and provides legal advice when an incident occurs. |
| **Senior Management** | 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.<br>Senior Management must ensure that:<br>• Business areas comply with this policy;<br>• A register of information assets used in important information processing activities in their business area is created and maintained;<br>• Information used in important information processing activities is classified;<br>• Personal information impact assessments are conducted before confidential and personal information is processed;<br>• Data privacy-related risks in their business area are managed; and<br>• 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:<br>• Adhere to all policies, procedures and guidelines that relate to the use of information; and<br>• Report any actual or suspected incidents. |
| **Internal and external audits** | Internal and external audit provides independent assurance that the Organisation's risk management, governance and internal control processes are operating effectively, including in compliance with this policy. |

## 6 OUR POLICY GLOSSARY

| | |
|---|---|
| **Data subjects** | The person or organisation to whom personal information relates. This includes:<br>• Prospective customers<br>• Customers;<br>• Staff members and job applicants;<br>• Service providers, contractors and suppliers;<br>• Shareholders and directors; and<br>• Members of the public and visitors. |
| **Incident** | An incident includes:<br>• Non-compliance with this policy and any procedures relating to it;<br>• Contraventions of any data protection legislation such as the POPI Act; and<br>• Security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availibility 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.<br>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.<br>Examples include:<br>• 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;<br>• 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;<br>• information relating to physical or mental health, wellbeing, or disability;<br>• 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;<br>• biometric information: this refers to techniques of identification that are based on physical, physiological, or behavioural characterisation, such as blood-typing, fingerprinting, DNA analysis, retinal scanning, facial recognition, and voice recognition;<br>• someone's opinions, views, and preferences;<br>• private or confidential correspondence and any further correspondence that would reveal the contents of the original correspondence;<br>• views or opinions about a person, such as interview notes and trade references; and<br>• the criminal behaviour 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. |
| **POPIA** | The Protection of Personal Information Act 4 of 2013 and its regulations. |
| **POPIA Programme** | The POPIA Programme is our ongoing efforts to comply with the provisions of the POPIA and includes:<br>• stakeholder consultation;<br>• defining roles and responsibilities;<br>• policy development;<br>• policy implementation;<br>• monitoring and audit; and<br>• continual improvement. |
| **Processing** | Any operation or activity or any set of operations concerning personal information, including:<br>• collecting, receiving, recording, organising, collating, storing, updating or modifying, retrieving, altering, consulting, or using;<br>• disseminating by means of transmission, distributing, or making available in any other form; or<br>• merging, linking, restricting, degrading, erasing, or destroying personal information. |

## 7 SUPPORTING DOCUMENTS

You must read this policy with:

- Data Subject Request Procedure;
- Information Sharing Procedure; and
- Personal Information Impact Assessment Procedure.

## 8 DOCUMENT METADATA

| | |
|---|---|
| Document version: | 2021.06 (v.2) |
| Document approval authority: | Hjalmar Francois Otto Bekker |
| Document approval date: | 2021.06 |
| Document owner: | Hjalmar Francois Otto Bekker |
| Document author(s): | Jean-Marié Tosen |
| Last updated: | 2021.06 |
| Next review date: | 2021.11 |
| Visibility: | The POPIA Compliance Folder, Policy Shepard |