Data Protection Compliance & Security Policy

Protection of Personal Information Act (POPI Act)

Version 2

January 2023

Contents

Overview and Definitions

Contact Rocketseed

Data Collection and Processing

Service and Support

Security and Safeguarding Data

Companies Concerned

The South African entities of the Rocketseed Group, which are relevant to the Company POPIA statement and PAPIA manual are:

- **RocketFin (Pty) Limited** (2018/227819/07) – Holding company of the below South African subsidiaries and Rocketseed Group finance function
- **RocketDev (Pty) Limited** (2016/094522/07) –Research and Development
- **Rocketseed (South Africa) (Pty) Limited** (2000/021758/07) – Sales and Distribution
- **RocktePad (Pty) Limited** (2020/241196/07) – Sales and Distribution
- **RocketMailer (Pty) Limited** (2020/240933/07) – Newsletter Tool
  - o   RocketMailer (Pty) Limited has a separate POPIA statement applicable to its operations.

Overview and Definitions

1. Introduction

This POPI Compliance and Security Policy describes how Rocketseed (and applicable subsidiaries, together 'Rocketseed') operate in South Africa. The below sections clarify how Rocketseed collects, processes and safeguards personal information and data from individuals/clients using the Rocketseed software and services. This Policy was last revised on January, 2023.

Rocketseed has two main responsibilities regarding Personal Data:

- Collecting information for the purpose to fulfil the requirements of a contractual and/or service relationship.
- Collecting the necessary information needed to provide service of conveying pertinent content through everyday email branding and signatures.

Rocketseed is a Responsible Party / Controller regarding the client's Personal Information: company details, staff/user details, such as email, addresses, phone numbers, billing details, and other information used to do business.

Rocketseed is the Operator/Processor regarding the Personal Information that the client uploads in the form of a database, distribution list, or the like, as we process Personal Information.

2. Compliance

Rocketseed is compliant with the following South African legislations:

- Protection of Personal Information (POPI) Act
- Promotion of Access to Information Act (PAIA)
- Electronic Communications Act of 2002 (ECT)
- The Consumer Protection Act, 68 of 2008 (CPA)
- Section 14 of the Constitution of the Republic of South Africa
- Cybercrime and Cybersecurity Act

Rocketseed globally is also compliant to a number of international legislations, where applicable, on data safety and security such as:

- EU-General Data Protection Regulation 2016/679 (EU-GDPR) and the UK-General Data Protection Regulation (UK-GDPR);
- United States Privacy Act, the Safe Harbor Act and the Health Insurance Portability and Accountability Act
- Open Web Application Security Project (OWASP) development principals – applicable to RocketDev only.

Additionally, Rocketseed is also in the process of ISO27k certification with a Letter of Commitment available upon request.

3. Definitions

Personal data/Personal information: defined to include information relating to both an identifiable, living, natural person, and where applicable, an identifiable juristic person or legal entity, and includes

Sensitive data/Special Personal Information: includes all information relating to a person's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, or criminal behaviour. POPIA also specifically regulates personal information (of a child). _Not collected by Rocketseed_.

Data controller/Responsible Party: A public or private body that determines the purpose and means for processing personal information of a data subject. In our case it is our clients who contract us to process information through our Software.

Data processor/Operator: A party that processes personal information on behalf of a responsible party, without coming under the direct authority of the responsible party. In our case, it is a Rocketseed subsidiary with whom the contract is signed.

Data subject: Any party to whom personal information relates.

Biometric data/Biometrics: A technique of personal identification that is based on physical, physiological, or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition. *Not collected by Rocketseed*.

Health data: *Not collected by Rocketseed*.

Pseudonymisation: POPIA does not provide a definition for pseudonymisation. However, 'de-identify', in relation to personal information of a data subject, means to delete any information that:

- identifies the data subject;
- can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- can be linked by a reasonably foreseeable method to other information that identifies the data subject; and
- 'de-identified' has a corresponding meaning.

Right To Request/Access information/erasure: POPIA allows a data subject the right to request that a responsible party correct or delete personal information that is inaccurate, irrelevant, and excessive, or which the responsible party is no longer authorised to retain.

or which the responsible party is no longer authorised to retain.

4. Privacy Principles

Being fully compliant with the POPI Act, Rocketseed has adopted its well-accepted attributes and principles which must be addressed for a successful POPIA implementation.

Accountability

Rocketseed has an appointed Information Officer who is responsible for ensuring that the information protection principles within POPIA and the controls are in place and complied with.

Processing Limitation

Rocketseed only collects the minimum of necessary information needed with consent, justification and objection to be able to provide service and meet contractual obligation.

Additionally, processing can only be done for which it was intended and agreed, and further processing must be compatible for what was previously specified.

Purpose Specification

The personal information collected is or a specific purpose and the data subjects must be made aware of the purpose for which the personal information was collected.

Security Safeguards

Rocketseed has rigorous procedures in place, so that the integrity of the personal information in its control is secured through technical and organisational measures.

Information Quality and Data Subject Participation

Rocketseed takes reasonable steps to ensure that the personal information that has been collected is complete, accurate, not misleading and up to date.

Data subjects have the right to request that a Responsible Party confirm (free of charge) whether it holds personal information about the data subject, and he or she may also request a description of such information.

Rocketseed provides a Right to Request form on through its compliance platform, where data subjects have the right to request that a Responsible Party confirm (free of charge) whether it holds personal information about the data subject, and he or she may also request a description of such information.

Data subject also has the right to request data to be deleted

Contact Rocketseed

5. How to Contact Us

Data subjects have the right to access, correct, amend, or delete any Personal Information Rocketseed may hold, register a complaint, or simply want to know more. A request can be submitted at any time to Rocketseed via the Group *Privacy Page*. **Note:** although the Right to Access and/or Erasure form is operated through our EU/UK-platform, all geographical requests will be actioned globally.

Contact our compliance team *privacy@rocketseed.com*, or by post for the appropriate address given on the Privacy Page.

Additionally, by submitting the Data Subject Request Form, also displayed on the Privacy Page.

5.1. Changes to this Policy

If we make any material changes, we will notify you by email or by providing the revised policy on our website. Your continued use of our services following the update means that you accept Rocketseed's updated Data Protection Compliance & Security Policy.

Data Collection and Processing

6. Information Rocketseed Collects

6.1. Collection of personal information from clients

We collect personal information in the following ways:

- Directly from Client during the inception of the contractual service.
- Indirectly from Client when interacting with us electronically; e.g. browsing our website (including through mobile), filling out online forms, submitting requests for ticketing etc.
- Directly from other sources, such as public databases, data aggregators and third parties etc;
- e.g. LinkedIn.

6.2. Directly from Users of Service

As a user of our services, personal information is required to fulfil the requirements of a contractual or service relationship, which may exist between Client and our organization. We collect:

- Financial Details
- Identification Number
- Location Information
- Banking Details

- Confidential Correspondence
- Email, Social Networks
- Name
- Telephone contact details

6.3. Indirectly Through Branding Interaction in B2B Emails

Our technology allows Clients of the Rocketseed software product, to convey pertinent content through everyday email branding and signatures. Clients and their Recipients of emails are businesses who engage with each other and may already have an established relationship and communication.

If **full engagement measurement** is required, apart from normal information needed to send emails (such as an email address), the following data is stored for analytical purposes only;

- IP address
- Time of click
- URL served – i.e. where the branding redirects the recipient as defined by the Client.

In the case of providing Data Analytics as an Operator, Rocketseed can only do so if *requested by Client as part of the contractual agreement of service and processing instructions*. Hence, Clients should present in their Privacy Note on their website if they are collecting data for Analytical purposes.

If **Pseudonymisation** of data is requested, in which case we only have limited analytics capabilities, the information stored is limited to:

- Domain name (e.g. @gmail.com)
- Time of click
- URL served – i.e. where the branding redirects the recipient as defined by the Client

7. Processing

7.1. The lawful bases Rocketseed relies on for processing

- We have your consent to do so;
- We have an obligation to carry out the performance of a contract with you;
- We are required by law to process your personal information;
- The processing protects your legitimate interest; and
- We have a legitimate interest to pursue.

7.2. Processing information of children

Rocketseed does NOT collect or process any data on children.

7.3. Processing and Sub-Processing

Rocketseed engages with third party data centres for data storage and large scale processing. These are referred to as sub-processors. Sub-processors are vetted based on their ability to provide rigorous safety environment, ISO certifications and stringent breach management and prevention procedures, as well as robust business continuity infrastructure. are hosted by sub-processors (data centres), which have been assessed having. Personal information is held at local data centres who operate within South Africa, ensuring that such data is not transferred outside of South Africa in line with POPI Act compliance requirements.

Information on our Sub-Processors can be found *here*, along with their locations and Data Protection Policies.

For added reassurance, Clients may opt to have a dedicated server within their own premises, and behind their own firewalls.

7.4. Disclosing information

To maintain and improve our services, personal information may need to be shared with or disclosed to service providers, other Controllers or, in some cases, public authorities. We may be mandated to disclose personal information in response to requests from a court, police services or other regulatory bodies. Where feasible, Rocketseed will consult with Client prior to making such disclosure and, in order to protect privacy, we will ensure that we will disclose only the minimum amount of information necessary for the required purpose.

7.5. Retaining information

We will keep information only for as long as we need it, given the purpose for which it was collected, or as required by law (including tax legislation) and any other statutory obligations (including anti-money-laundering and counter-terrorism requirements).

Personal Information for processing purposes (e.g. emails, IP addresses or domain names) are purged from the system bi-annually to remove inactive/retired users. If data subject requests removal sooner, Rocketseed will oblige within the time limit set out in Data Protection Laws.

7.6. Data protection rights

PAIA gives legislative effect to the right of access to information

Clients and individuals who have conducted business with Rocketseed or believe we may hold their personal data, has the right to request a record from us about the type of personal information we hold, as well as information about all third parties with whom we have shared that personal information. Once Rocketseed responded to the request, we can be asked to:

- correct or delete the personal information in our possession or under our control if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or has been obtained unlawfully;
- destroy or delete a record of any personal information that we are no longer authorised to keep in terms of the Act or other regulatory requirements; or
- stop or start sending you marketing messages by informing us in writing by post or email through our office network, or website.

A request can be submitted at any time to Rocketseed via our *[Privacy Page](#)*.

Rocketseed can also be reached through the individual offices featured on our Privacy Page, or by emailing us at *privacy@rocketseed.com*.

Service and Support

8. Implementation

8.1. Project Management

To ensure smooth implementation, Rocketseed uses a clearly defined project management methodology, which incorporates parallel processes for the technical and marketing aspects of the rollout and customized the needs of Clients.

8.2. Structured Rollout and Support

The key to implementation is a controlled rollout process, with defined focus areas encompassing:

- step-by-step technical and security setup procedures conducted alongside intense monitoring until sign-off
- continued normal 24/7 monitoring with feedback for continued functionality of hardware, email flow and potential risk of disruptions
- resolution via technology and support process enables the immediate correction of any issues that may arise, including email format issues

Procedures include:

- Mark-up testing
- Functional Testing
- Load testing
- Security reviews

9. Hosting Options

9.1. Shared servers – Logical Separation

Rocketseed hosts shared servers in data centres in USA, UK, and South Africa. Each server handles outbound email traffic for a number of customers. Customers are segregated into individual accounts and cannot see or affect other users' mail traffic and branding.

All such servers are maintained with failover pairs in distinct locations. If an issue should affect a primary server, there is a spare server at the ready to take over branding duties until the problem is resolved. Cutover is made by Rocketseed staff and does not require any action by the customer.

9.2. Dedicated Servers and Azure – Physical Separation

Customers can be provisioned on a dedicated server hosted in one of our data centres. Rocketseed remains responsible for the hardware, networking, monitoring and backups. Each dedicated server delivers mail from a unique IP address, ensuring there is no reputation risk from other clients' traffic creating blacklist entries.

These servers are normally set up in tandem pairs in distinct locations to ensure full failover redundancy if desired.

The Rocketseed software is fully compatible with modern virtualization environments. In particular, hosting a Rocketseed email media appliance in the Azure cloud makes sense for many customers hosted on Microsoft Office 365.

9.3. Release strategy - Installation, Testing, and Rollback

The process of installing a new server undergoes extensive testing and training by Rocketseed system administrators. Each new installation, as well as software upgrade, requires a sequence of steps to ensure that functionality is complete, and a checklist is employed to test all aspects of the system before customers access it.

Rocketseed installations consist of a pair of servers acting in tandem with offsite database backups to ensure the ability to roll back any upgrades if needed.

9.4. SLA

SLA are provided with more detailed outline of the support and incident management procedures.

Security and Safeguarding Data

10. Security

10.1. Product Security

Patch management of servers and desktops are properly maintained with the latest updates in order to reduce system vulnerability to enhance and repair application functionality.

Third Party Security Scans are performed on software updates and tested for security vulnerabilities and to validate data integrity, using up to date scanning software.

The software is fully tested for various hacking processes, as well as breaches. Other tests, practices and monitoring are put into place to ensure system stability.

10.2. Cyber Security

All US, UK and EU Rocketseed hosting providers are ISO 27001 and 9001 certified with tier-one security premises and have stringent controls in place.

Server Hardening procedures fully lock down Rocketseed servers and have been developed to pass 3rd party security review processes, such as those from legal, technical or financial enterprise customers, with high security requirements. Servers can be further secured with additional measures, where requested.

Both hardware and software based firewalls, and regular penetrations tests are performed to provide additional security.

10.3. Reports & Incidents

Rocketseed information security incident response, business continuity, and disaster recovery plans to follow should an incident occur. In general it follows the below steps:

- Identification and classification of incident or threat
- Containment, recovery and response
- Notification of breach
- Evaluation
- Risk assessment
- Future controls for mitigation

11. Business Continuity

11.1. Escrow Deposits

Each major release of the Rocketseed software is delivered to a third-party escrow management company and is regularly updated. This ensures that in the event of a complete dissolution of the Rocketseed development team, or a complete loss of the development archives, the entire software system can be recreated.

11.2. Real Time Monitoring And Response

Each server is monitored from a centralized Rocketseed control system; tracking email flow, disk and memory usage, server load and other parameters that measure email delivery and branding operations.

Notification occurs via email and SMS alerts, and is configured to reach a number of different support personnel to ensure prompt response.

11.3. Server Redundancy

Each Rocketseed server is configured with internal redundancy to ensure the highest possible hardware uptime.

Every hosted Rocketseed server is configured with a matching spare server in stand-by at a separate data centre.

Further elements of redundancy management includes:

- Live database redundancy
- Mail server redundancy
- Complete system redundancy

11.4. Data Backups

No data from backups are shared with any third party unless Rocketseed would be legally obligated to. The scheduled data backups are stored in an separate offline database and are encrypted.

Daily Backups

Daily snapshot backups are performed on every account including contact data, messages, and reports. These daily backups are kept onsite for 14 days (two weeks).

Two types of backups are performed:

- Physical backups entailing the entire server and data on site and remotely – for UK/US only
- Logical backups regards the database exclusively, both locally and remotely.

Offsite Backups

Complete daily backups are stored offsite for 3 days and then updated.

Encryption

Although the data is not encrypted at rest(the upgraded tech stack(not cloud) is being testing with encryption of data at rest), it is encrypted in transit via TLS, HTTPS, SSH.

Resting data is stored in the files of the database management system, Postgresql, and cannot be accessed from the database unless the necessary login details are correct. The database servers exist behind a secure firewall and root access via SSH to the servers is not possible.

- Secure ISP : Our internet service provider uses the highest security protocol.
- SFTP/SCP: We transfer files using a secure data stream.
- HTTPS: This secure layer encrypts and decrypts user page requests and pages returned by the server.
- Secure MTA: Our MTA uses strict security measures to make sure all messages are secure during transfer.

12. Access Control

12.1. Physical Access to the Office

The following physical safety measures are applicable to Rocketseed offices:

- Gated security
- Keycard entry
- Security alarms
- Receptionist to identify and ensure visitors sign-in register
- CCTV

12.2. Staff

All staff, including employees and contractors, are vetted through agencies with thorough background checks (criminal records, eligibility to work at a specified location etc), references and with necessary documentations requested.

All staff are moderated by their contracts.

All staff attest to terms and conditions that specifically outline privacy, information security, and confidentiality and must verify in signing that they have read and understood all the procedures and policies of the company.

This also includes necessary training and coaching before being allowed to access any confidential or personal files.

Our Data Safety as well as HR Handbooks form part of the employment/working relationship between Rocketseed and its staff, and must be signed prior to work commencing. These include, but not limited to:

- **Acceptable Usage Policy** relating to the use of any office technology and software (e.g. telephone, mobile phone, fax, email, internet, intranet, and remote access, etc.) are outlined in our internal handbooks.
- **Clean Desk Policy and Awareness** ensures that visitors or unauthorised persons are unable to view personal or sensitive information, whether held on paper documents or displayed on monitors, etc.
- **Other policies** include; e.g. email usage, remote access, password/passphrase creations, laptops and other company devices, cyber security, ethics, harassment, and overall business conduct.

12.3. Third Party Platforms and Server Access

Access to various platforms concerning day-to-day activities, (Google Drive, PeopleHR, Salesforce, ticketing systems, etc) are managed by top directors with admin access. Staff access to data on these platforms are given in a tiered fashion.

Email is controlled by top management technical staff ('super admins') who either add upon employment start, or immediately remove staff upon decision to retire or leave the company.

Access to servers is managed through rigorous controls by Rocketseed, as well as host centre, or sever provider. The controls are company confidential and restricted to the specific IP addresses of certain, authorised Rocketseed, listed as 'high-level' Rocketseed technical staff.

Staff who access servers for installation, maintenance or support purposes also need identity verification from the data centre for additional security and control, meaning, both ends need to identify the requestor for successful access.

Retired or resigned staff are removed immediately from access control lists.