Rocketseed and POPIA

Protection of Personal Information Act 2013

Date: August 2021

This document, as reviewed by SA legal professionals, serves as a statement of Rocketseed Assurances Under the Protection Of Personal Information Act 2013 (POPIA).

Rocketseed and its subsidiaries do not sign individual Operational Agreements as this vetted statement, and accompanying Privacy Policy summary below, both of which supplement our full ***Privacy Policy*** and InfoSec documents (upon request only), suffice as assurance of our security measures and legal obligations within the framework of our business.

1. Rocketseed is a multinational corporation and has been applying internationally recognised data protection and privacy laws, chiefly amongst them the General Data Protection Regulations in the European Union, for several years.
2. This letter serves to give you, our valued stakeholder, specific assurances that Rocketseed are compliant in all respects with the Protection of Personal Information Act (POPIA) and the GDPR and continually strive foremost to protect those whom we serve.
3. Herewith a summary of our key compliance items, which are enumerated in our policies and procedures, both publicly accessible and internally enforced:

NO.	HEADLINE	DESCRIPTION
1	***Chief Compliance Officer***	Dr Eszter Nagy – eszter.nagy@rocketseed.com
2	***Personal Information***	All information we receive, store, and handle is presumed by our staff and contractors to be personal information of the most sensitive category.
3	***Background checks***	We carry out background checks on all our personnel and obtain assurances from all our service providers in this regard.
4	***Access control***	We apply strict access restrictions to data which is designed to ensure that access to information is allowed strictly on a need-to-know basis.
5	***System back-up***	All data is backed up frequently in accordance with our business continuity impact assessment.
6	***Complaints and reporting***	All complaints should be directed to our Compliance Officer and will be immediately investigated and reported upon. We implement stringent internal reporting, incident classification, investigation, and remedial structures.

7	***Cyber risks***	As part of our ongoing data privacy obligations applied globally for several years we have designed and implement a comprehensive risk assessment, which covers cyber risks, we monitor and consult with industry experts on the dynamic field of cyber security, prevention, and mitigation. We have developed and we implement a cyber risk management framework to identify and manage cyber threats and vulnerabilities and implement mitigating controls.
8	***Training***	All our staff and significant contractors undergo training on trends and changes in the data privacy industry, from industry experts and compliance specialists.
9	***Systems and networks***	Our systems and networks are configured in a consistent, accurate manner and application of approved good-practice security settings. We continuously monitor designated systems and networks and record security events including the identification of and response to information security/privacy incidents as well as recovery and post implementation reviews for current and predicted levels of traffic and alternative facilities support. We implement security protocols and measures to protect systems like e-mail, instant messaging, and VoIP and configuring security settings, performing capacity planning, and hardening supporting infrastructure. We implement network dematerialised zones, wireless and critical systems, and the segregation of areas/computer systems for access control purposes.
10	***Assurances***	We have in place assurances from all our services providers in line with adherence to our policies, procedures, and rules.
11	***Cryptography***	We apply cryptographic techniques to data transmitted and stored.
12	***Disaster recovery***	We implement a DRP that is supported by alternative processing facilities and tested regularly using simulations of the live environment.
13	***ISO 27001***	We implement rules for the disposal of electronic and physical data when it is no longer needed in accordance with the ISO 27001 standard.
14	***Malware and handling capabilities***	We implement appropriate solutions including anti-virus software and behavioural analysis.

For more information Privacy, please turn to our ***Group Privacy Policy page*** at where there are details of our procedures concerning your data, in addition to the option for individuals to submit requests for the ***Right to Access and Erasure***.

Protection Of Personal Information Act Summary

About this document

The following sections are set out with Rocketseed and its subsidiaries entering into contract with Clients mainly in the capacity of an **Operator**.

Definitions

Personal data: 'Personal information' is defined broadly in POPIA to include information relating to both an identifiable, living, natural person, and where applicable, an identifiable juristic person or legal entity, and includes:

- information about a person's race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language, and birth;
- information relating to the education, medical, financial, criminal, or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views, or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
- Sensitive data: POPIA provides for a separate category of information called 'special personal information' which 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).

Data controller: A 'Responsible Party' is 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: An 'Operator' is 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' means 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 applicable for Rocketseed.

Health data: Not applicable for 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 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.

1. Introduction

Rocketseed treats confidential information with the utmost discretion. This is in line with the South African Protection of Personal Information Act (POPIA), 4 of 2013, which operationalises the constitutional right to privacy and the protection of personal information. POPIA promotes the fair and transparent use of personal information and requires us to safeguard it appropriately.

2. Information Rocketseed collects

2.1. 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

2.2. 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 connection.

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

3. Processing

3.1. 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.

3.2. Processing information of children

Rocketseed does NOT collect or process any data on children.

3.3. How do we collect personal information?

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 etc.
- Directly from other sources, such as public databases, data aggregators and third parties etc; e.g. LinkedIn.

Please refer to the ***Privacy Policy*** for details.

4. To whom will we disclose your information?

To maintain and improve our services, your 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 your personal information in response to requests from a court, police services or other regulatory bodies. Where feasible, we will consult with you prior to making such disclosure and, in order to protect your privacy, we will ensure that we will disclose only the minimum amount of your information necessary for the required purpose.

Data storage and where processing takes place, unless specifically requested by a client to be on a dedicated server within their own premises, are hosted by sub-processors (data centres), which have been assessed having rigorous safety environment, ISO certifications and stringent breach management and prevention procedures. These sub-processors can be found ***here***, along with their locations and Data Protection Policies.

5. How do we protect your information?

We are committed to ensuring that your information is secure. To prevent unauthorised access or disclosure, we have put suitable physical, electronic and managerial procedures in place to safeguard and secure the information we collect. Please see statement above.

6. How long will we keep your information?

We will keep your 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).

7. Your data protection rights

You have the right to ask us to confirm whether we hold any information about you. You may also request a record from us about the personal information we hold about you, as well as information about all third parties with whom we have shared your personal information. Once we have given the information to you, you may ask that we:

- 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 your 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 this ***link***. (Note: even if the Right to Access and/or Erasure form is operated through our UK-platform, all geographical requests will be actioned globally.

8. Supervisory Authorities

Information Regulator
JD House, 27 Stiemens Street
Braamfontein, 2001
Johannesburg
complaints.IR@justice.gov.za
www.justice.gov.za/

For more information, please contact us through an online form, email, or telephone on our contact page at https://www.rocketseed.com/contact/.