



PROTECTION OF PERSONAL INFORMATION (POPIA) POLICY

1. Introduction

This document outlines the measures and policies implemented by Apricus Solutions ("the Company") to comply with the Protection of Personal Information Act (POPIA) for the operation of its platform. The platform is designed to cater to the needs of various sectors, such as financial, general services, and ICT companies, with a focus on bulk assessments of smaller financial brokers, intermediaries, and other service providers. Apricus Solutions uses Jotform, a third-party application, to gather information from users for the purpose of generating affidavits in compliance with legislative requirements. The Company also incorporates Microsoft applications, such as Power Automate and Power BI, to enhance its services.

2. Scope

This compliance document applies to all personal information collected, processed, and stored by the Company through the platform, including but not limited to email addresses, names, surnames, ID numbers, contact numbers, and business or company details.

3. POPIA Principles

The Company adheres to the following POPIA principles when processing personal information:

3.1. Accountability

The Company takes responsibility for ensuring compliance with POPIA and has appointed a designated Information Officer who oversees all activities related to the processing of personal information.

3.2. Processing Limitation

Personal information is processed only for the purpose of creating the agreed affidavits and for reporting on data submissions for the contracted entity. The information is processed lawfully, minimally, and not excessively.

3.3. Purpose Specification

Personal information is collected for the specific purpose of generating affidavits and for reporting on data submissions for the contracted entity. The Company does not process personal information for any other purposes.

3.4. Further Processing Limitation

Personal information is not processed beyond the initial purpose for which it was collected. The Company does not sell, share, or use personal information for any other purposes.

3.5. Information Quality

The Company takes reasonable steps to ensure that personal information is complete, accurate, not misleading, and updated when necessary.

3.6. Openness

The Company provides notice to users regarding the collection and processing of their personal information through a Privacy Policy displayed on the platform.

3.7. Security Safeguards

The Company implements appropriate technical and organizational measures to protect personal information against loss, damage, unauthorized access, or unlawful processing. This includes the use of encryption, secure server infrastructure, and regular security audits. By utilizing Jotform for data collection, the Company benefits from Jotform's robust security measures, including encryption technologies, compliance with data protection regulations, and security certifications.

3.8. Data Subject Participation

Users have the right to access, correct, or delete their personal information held by the Company. The Company provides mechanisms for users to exercise these rights, such as through an online account dashboard or by contacting the Information Officer.

4. Information Regulator Compliance

The Company complies with all requirements set forth by the Information Regulator, including registering the processing of personal information with the regulator and reporting any security breaches involving personal information.

5. Retention and Destruction of Personal Information

The Company retains personal information only for as long as necessary to fulfill the purpose for which it was collected and in accordance with legal, regulatory, and contractual requirements. When personal information is no longer needed, it is securely destroyed or permanently de-identified.

6. Third-Party Processors

The Company ensures that any third-party processors engaged for the processing of personal information on its behalf, including Jotform and Microsoft, adhere to the same level of data protection and security as outlined in this compliance document. The Company reviews Jotform's and Microsoft's data protection practices and policies to ensure they meet the standards set forth by POPIA.

Microsoft, as a third-party application provider, is committed to data protection and security. The company adheres to various data protection regulations, including the General Data Protection Regulation (GDPR) for the European Union, and has implemented strong security measures. Some key aspects of Microsoft's data protection and security measures include:

Encryption: Microsoft employs encryption technologies, both in transit and at rest, to protect the confidentiality and integrity of personal information.

Access Controls: Microsoft implements strict access controls to ensure that only authorized personnel have access to user data.

Security Certifications: Microsoft has obtained numerous security certifications, such as ISO 27001, to demonstrate its commitment to maintaining a high level of security for its cloud services.

Data Centers and Redundancy: Microsoft operates multiple data centers globally, ensuring redundancy, reliability, and strict security measures, including 24/7 surveillance, biometric access controls, and fire prevention systems.

7. Updates to the Compliance Document

The Company reserves the right to update this compliance document as necessary to reflect changes in legal requirements or the Company's processing practices. Users will be notified of any significant changes.

8. Contact Information

If you have any questions, concerns, or requests regarding the processing of your personal information, please contact our Information Officer at:

William Smith

william@apricusas.co.za

OUR COMMITMENT TO PRIVACY OF YOUR INFORMATION

- 1. Responsible Party:** Apricus, as the company collecting and processing users' personal information, is designated as the "responsible party" for the purposes of this policy.
- 2. What Personal Information is Collected:** Apricus may collect personal information such as name, date of birth, home language, address, account information, email address, contact details, financial information, and other related information. Apricus is required or authorized to collect personal information under certain laws, such as RICA and FICA.
- 3. Purpose/s for Collection and Processing of Personal Information:** Apricus collects and processes personal information for specific, explicitly defined, and lawful purposes related to its business functions and activities, including entering into contracts with users, complying with legal obligations, protecting legitimate interests of users, and direct marketing (with user consent).
- 4. Collection Directly from User:** Apricus will collect personal information directly from users, except under certain circumstances, such as when the information is available in a public record, written consent is given, or it is more practical or necessary to collect the information from another source.
- 5. Cookies:** Apricus may use cookies on its website to distinguish users, remember user preferences, estimate audience size, and speed up searches. Users can accept or decline cookies on their browser, but declining may limit access to certain website features.
- 6. General Conditions for Processing Personal Information:** Apricus will comply with all laws, contracts, and regulations when processing personal information and respect users' privacy rights. The company will ensure that personal information is relevant, adequate, and not excessive for the identified purpose/s of processing.

7. **Disclosure and Sharing of Personal Information:** Apricus may share personal information with third-party operators for purposes related to providing content or services or concluding transactions. Users will be notified of the information shared and the categories of operators it is shared with.
8. **User's Rights in Relation to the Processing of their Personal Information:** Users have the right to access and correct their personal information, object to the processing of their information, and lodge a complaint with the Information Regulator.
9. **Notification of Breach of Security:** In the event of a security breach, Apricus will immediately identify, and contact affected users, providing sufficient information for them to take protective measures against potential consequences.
10. **Retention of Information:** Users consent to Apricus retaining their personal information indefinitely unless they object. If they object, Apricus will keep the records only if lawfully entitled or obliged to do so.
11. **Returning, Destroying or Deleting Personal Information:** Apricus will either permanently destroy or delete personal information when no longer authorized to retain it or return the information to the user or transfer it to a third party, as per the user's written request.
12. **Consent:** Users consent to the processing of their personal information in accordance with this Privacy Policy, having read and understood its provisions. Users may withdraw their consent by notifying Apricus' information officer in writing.

WHAT DO WE NOT DO WITH YOUR INFORMATION

Apricus maintains strict confidentiality and privacy standards, ensuring the protection of your personal and company information. To provide clarity, we do not engage in the following activities:

1. Utilize personal information obtained for marketing purposes.
2. Utilize company information obtained for marketing purposes.
3. Sell or disclose personal information obtained to third parties.
4. Sell or disclose company information obtained to third parties.
5. Use personal or company information for any purpose other than generating the Affidavit and Affidavit Report.
6. Process personal or company information for purposes unrelated to achieving the intended results of our services.
7. Share personal or company information with any external entities, except as required by law or as necessary to fulfill our contractual obligations.

THE ROLE OF THE APRICUS SITE

As a service provider, Apricus recognizes the importance of ensuring the security and privacy of the personal information collected through our website. This may include information captured during order placement, email or newsletter subscriptions, payment processing, or online bookings. You, as our client, maintain control over this data, determining how it is collected and utilized. Apricus processes this information on your behalf by securely storing it on our servers, adhering to the highest standards of data protection and privacy.

YOUR RIGHT TO BE FORGOTTEN

The "Right to be Forgotten" or "Right to Erasure" refers to your entitlement to request the modification or deletion of your personal information when it is no longer necessary, such as upon the cancellation of your services with Apricus.

You may update your contact information through your website or per request. If you decide to discontinue your services with us and wish to delete your entire Apricus account, please reach out to our support team at info@apricusas.co.za

Please note that, due to legal requirements, we are unable to delete historical invoices containing your name and contact details.