Privacy Policy

This Privacy Policy outlines how Fund The People collects, processes, stores, and protects personal information obtained through our website. We are committed to safeguarding your privacy and ensuring compliance with all applicable laws, including the Protection of Personal Information Act, 2013 (POPIA), and other relevant legislation governing information management and electronic transactions.

1. Introduction and Purpose

Our purpose in processing personal information is to give effect to the constitutional right to privacy, balancing it against other rights such as access to information, and protecting important interests like the free flow of information. We aim to regulate the manner in which personal information is processed by establishing minimum threshold requirements for lawful processing, in harmony with international standards. We also strive to promote compliance with this Act and other applicable legislation.

2. Information We Collect

We collect personal information that is necessary for specific, explicit, and lawful purposes related to our functions and activities. This may include, but is not limited to:

• **Identity Data:** Such as your name, contact details (e.g., email address, phone number, physical address).

• **Financial Data:** Information related to payments, financial transactions, or other financial services, handled with appropriate control processes for integrity, security, and confidentiality. For financial services, this also includes information about financial situations, product experience, and objectives to help us provide suitable advice.

• **Technical Data:** Information about your device and browsing activity on our website, including IP address and system information.

• **Marketing and Communications Data:** Your preferences in receiving marketing from us and your communication preferences.

• **Other Information:** Any other information you voluntarily provide to us through forms, inquiries, or interactions on our website.

For certain services, such as those provided by a credit bureau or accountable institution, specific customer due diligence records, including identity verification, are required.

3. How We Collect Information

We collect information through various means, including:

• **Direct Interactions:** When you provide it to us directly, such as when filling out forms, subscribing to services, or contacting us via email.

• **Automated Technologies:** As you interact with our website, certain technical data may be automatically collected.

4. Purpose for Collecting and Processing Information

We process your personal information for a specific, explicitly defined, and lawful purpose related to a function or activity of our organization. These purposes include, but are not limited to:

• **Providing Services:** To deliver the products or services you have requested, including the determination of qualification criteria for licenses, concessions, or other authorizations in respect of economic activity.

• **Operational Management:** To ensure efficient operations and effective management of our affairs, including financial and risk management systems.

• **Compliance with Legal Obligations:** To comply with all applicable statutory and common law requirements. This includes fulfilling reporting obligations to regulatory bodies. For example, public entities must report on compliance with broad-based black economic empowerment in their audited financial statements and annual reports.

• **Enhancing User Experience:** To improve our website and tailor content to your preferences.

• **Marketing and Communications:** To send you relevant information about our products or services, subject to your preferences.

• **Security and Fraud Prevention:** To identify and mitigate risks, including financial crime, and to prevent unauthorized access to or processing of personal information. This involves establishing and maintaining appropriate safeguards and regularly verifying their effectiveness.

• **Record Keeping:** To maintain full and proper accounting records, as well as records concerning your workforce and employment equity plans. For critical databases, this also includes recording details of the administrator and database location.

5. Legal Basis for Processing

We will only process your personal information if at least one of the following conditions applies:

• **Consent:** You, or an authorized person on your behalf, have given your consent to the processing. You have the right to withdraw your consent at any time, without affecting the lawfulness of processing before such withdrawal.

• **Contractual Necessity:** The processing is necessary for the conclusion or performance of a contract to which you are a party.

• **Legal Obligation:** The processing is necessary for compliance with a legal obligation to which our organization is subject.

• **Protection of Legitimate Interests:** The processing is necessary for the legitimate interests pursued by our organization or by a third party to whom the information is supplied, unless those interests are overridden by your fundamental rights and freedoms.

• **Public Interest:** The processing is necessary for the proper performance of a public law duty by a public body, or for the pursuit of the legitimate interests of the public.

6. Information Quality

We take reasonably practicable steps to ensure that the personal information we process is complete, accurate, not misleading, and updated where necessary. This includes steps taken by credit bureaus to verify the accuracy of consumer credit information.

7. Information Security

We are committed to securing the integrity and confidentiality of your personal information. We implement appropriate technical and organizational measures to prevent loss, damage, or unauthorized access to, or processing of, personal information. These measures include:

• **Risk Identification:** Identifying all reasonably foreseeable internal and external risks to personal information in our possession or under our control. Our governing body oversees the integration of technology and information risks into organization-wide risk management.

• **Safeguard Implementation:** Establishing and maintaining appropriate safeguards against identified risks. This also applies to operators who process personal information on our behalf, through written contracts.

• **Regular Verification:** Regularly verifying that safeguards are effectively implemented.

• **Continuous Updates:** Ensuring safeguards are continually updated in response to new risks or deficiencies.

• **Industry Standards:** Having due regard to generally accepted information security practices and procedures, as well as specific industry or professional rules and regulations. For financial institutions, this aligns with robust risk management frameworks.

8. Sharing and Disclosure of Information

We may disclose your personal information to third parties in certain circumstances, strictly in accordance with applicable laws and this Privacy Policy:

• **Internal Disclosure:** Personal information may be processed by employees or persons acting under our authority, who are required to treat such information as confidential and not disclose it unless required by law or in the proper performance of their duties.

• **Service Providers:** We may engage third-party service providers (operators) to perform functions on our behalf. Any processing by an operator is done only with our knowledge or authorization and under a written contract ensuring they establish and maintain appropriate security measures. Our governing body ensures service providers are held accountable for complying with their mandates.

• **Regulatory Authorities:** We may disclose information to regulatory or supervisory authorities, such as the Information Regulator, Financial Sector Conduct Authority, Prudential Authority, National Credit Regulator, or the Financial Intelligence Centre, when legally required or necessary for compliance with relevant acts or directives. For example, critical database information can be disclosed for criminal investigations or to government agencies for safety and security. Financial sector regulators must have written processes for information sharing consistent with POPIA, granting authority only to senior officials.

• **Legal Proceedings:** Disclosure may occur for the purposes of criminal or civil proceedings, or to assist statutory bodies in investigations.

• **Public Disclosure:** Certain information, like annual reports, financial statements, and regulatory strategies, may be published on our website or official registers as required by law. Complaints related to broad-based black economic empowerment may also be made public in prescribed forms.

9. Cross-Border Transfers of Information

We will not transfer your personal information to a third party in a foreign country unless:

• The foreign country provides an adequate level of protection for personal information.

• You consent to the transfer.

• The transfer is necessary for the performance of a contract between you and us, or for the implementation of pre-contractual measures taken in response to your request.

• The transfer is necessary for the conclusion or performance of a contract concluded in your interest between our organization and a third party.

• The transfer is for your benefit and it is not reasonably practicable to obtain your consent, and if it were practicable, you would likely give consent.

• The transfer is necessary for prosecuting or enforcing a legal claim.

• The transfer is for purposes of international public interest or for law enforcement cooperation.

• The Information Regulator has authorized the transfer.

10. Your Rights as a Data Subject

As a data subject, you have the right to have your personal information processed in accordance with the conditions for lawful processing as referred to in POPIA. These rights include:

• **Right to Access:** To request access to your personal information held by us.

• **Right to Correction/Deletion:** To request the correction, destruction, or deletion of your personal information.

• **Right to Object:** To object, on reasonable grounds, to the processing of your personal information.

• **Right to Withdraw Consent:** To withdraw your consent to processing at any time.

• **Right to Complain:** To submit a complaint to the Information Regulator regarding any alleged interference with the protection of your personal information.

• **Right to Institute Civil Proceedings:** To institute civil proceedings regarding any alleged interference with the protection of your personal information.

11. Direct Marketing and Automated Decision-Making

• **Direct Marketing:** We will only send you direct marketing communications by electronic means if you have given your consent, or if you are an existing customer and the communication relates to our similar products or services, and you have been given an opportunity to object. We will also ensure clear opportunities to opt-out of future communications.

• **Automated Decision-Making:** You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you, unless it is in connection with a contract, governed by law/code of conduct, or appropriate measures are taken to protect your legitimate interests. Where automated decisions are made, we will provide an opportunity for you to make representations and sufficient information about the underlying logic of the processing. Our codes of conduct may specify measures for automated decision making.

12. Data Retention

We will retain your personal information for no longer than is necessary to achieve the purpose for which it was collected or subsequently processed, unless a longer retention period is required or authorized by law.

13. Cookies and Other Tracking Technologies

Our website may use cookies and similar tracking technologies to enhance your browsing experience, analyze site usage, and support our services. Details on the use of these technologies will be provided in a separate Cookie Policy on our website.

14. Changes to this Privacy Policy

This Privacy Policy may be updated periodically to reflect changes in our data processing practices or legal requirements. Any material changes will be published on our website. Our governing body ensures ongoing monitoring of the regulatory environment and appropriate responses to changes and developments.

15. Contact Us / Complaints

If you have any questions about this Privacy Policy, our data practices, or wish to exercise any of your rights, please contact our Information Officer:

Information Officer:

Praneshan Naidoo

Support@fundthepeople.co.za

16 Fricker Road, Illovo, Sandton, Johannesburg, Gauteng, 2196.

Our Information Officer is responsible for encouraging compliance with POPIA, dealing with requests, and ensuring overall compliance. All Information Officers must be registered with the Information Regulator.

You have the right to submit a complaint to the Information Regulator if you believe your rights have been infringed. Complaints must be made in writing and should be lodged within 180 days of the decision you are aggrieved by.

The Information Regulator (South Africa):

Physical Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

Postal Address: P.O Box 31533, Braamfontein, Johannesburg, 2017

Email: enquiries@inforegulator.co.za

Website:https://inforegulator.org.za/