

PRIVACY POLICY



TABLE OF CONTENTS

Introduction	3
1. Important information and who we are	3
1.1. Purpose of this Privacy Policy.....	3
1.2. Responsible Party.....	4
1.3. Contact details.....	4
1.4. Changes to the Privacy Policy and your duty to inform us of changes.....	5
1.5. Third-party links	5
2. The Personal Information we collect about you	5
2.1. Categories of Personal Information.....	6
2.2. Other categories of Personal Information	7
2.3. If you fail to provide Personal Information.....	7
3. How is your Personal Information collected?	8
3.1. Methods of collection	8
4. Usage of Personal Information	10
4.1. How we use your Personal Information	10
4.2. Purposes for which we will use your Personal Information	10
4.3. Marketing.....	13
4.4. Promotional offers from us	13
4.5. Third-party marketing	14
4.6. Opting out.....	14
4.7. Cookies.....	14
4.8. Change of purpose	14
5. Disclosures of your Personal Information.....	15
6. Cross-border transfers of Personal Information	15
7. Security	16
8. Our retention of your Personal Information.....	16
8.1. Duration of retention	16
9. Your legal rights.....	16
9.1. Rights.....	16
9.2. Time limit to respond.....	19
10. Glossary	19



Introduction

Welcome to the Southern African Fraud Prevention Service's (**SAFPS**) Privacy Policy.

SAFPS respects your privacy and is committed to protecting your Personal Information. This Privacy Policy will inform you as to how we look after your Personal Information and tells you about your privacy rights and how the law protects you.

Please also use the Glossary (section 10 below) to understand the meaning of the capitalised words which are used in this Privacy Policy.

1. Important information and who we are

1.1. Purpose of this Privacy Policy

The SAFPS is a non-profit company committed to improving vigilance with regards to fraud, financial crime and identity theft by educating businesses and consumers about fraud and assisting them to protect themselves. The SAFPS achieves this by delivering a centralised fraud-prevention function. This Privacy Policy is applicable to the extent that SAFPS Processes Personal information to fulfil these objectives, This Privacy Policy aims to give you information on how SAFPS collects and otherwise Processes your Personal Information when you:

- visit our website (regardless of where you visit it from);
- use any of our Services as a Member, consumer, service provider or in any other manner;
- receive our assistance to protect you from fraudulent activities including identity theft and impersonation;



- receive our protective registration assistance to protect you from incurring losses related to fraudulent activities; or
- are subject to listings on our databases as a suspected fraudster.

This website and our Services are not intended for children, and we do not knowingly collect Personal Information relating to children.

It is important that you read this Privacy Policy together with any other privacy policy or fair processing policy we may provide on specific occasions when we are collecting or otherwise Processing Personal Information about you so that you are fully aware of how and why we are using your Personal Information. This Privacy Policy supplements other notices and privacy policies and is not intended to override them.

1.2. **Responsible Party**

In respect of this website and our Services, SAFPS is the Responsible Party and is responsible for your Personal Information.

We have appointed an information officer (**IO**) who is responsible for overseeing questions in relation to this Privacy Policy. If you have any questions about this Privacy Policy, including any requests to exercise your legal rights, please contact the IO using the details set out below.

1.3. **Contact details**

If you have any questions about this Privacy Policy or our privacy practices, please contact our IO in the following ways:

Email address: safps@safps.org.za

Postal address: P.O. Box, 2629, Alberton, 1450

Telephone number: +27(0)11 867 2234



You have the right to make a complaint at any time to the Information Regulator, the South African supervisory authority for personal information protection issues (<http://www.justice.gov.za/infoereg/>) (**Information Regulator**). We would, however, appreciate the opportunity to deal with your concerns before you approach the Information Regulator so please contact us in the first instance.

1.4. Changes to the Privacy Policy and your duty to inform us of changes

We keep our Privacy Policy under regular review.

It is important that the Personal Information we hold about you is accurate and current. Please keep us informed if your Personal Information changes during your relationship with us.

1.5. Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share information about you. We do not control these third-party websites and are not responsible for their privacy statements. We make no representations or warranties about the privacy practices of any third-party website and do not accept any responsibility for the privacy practices of, or content displayed on, these third party websites. Third party website providers are responsible for informing you about their own privacy practices. We encourage you to read the privacy policy of every website you visit.

2. The Personal Information we collect about you

Personal Information means any information about a natural or juristic person from which that person can be identified. It does not include information where the identity has been removed (anonymous information).



2.1. Categories of Personal Information

We may collect, use, store and transfer different kinds of Personal Information about you which we have grouped together as follows:

- **Identity Information** includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.
- **Contact Information** includes billing address, delivery address, email address and telephone numbers.
- **Financial Information** includes bank account and payment card details.
- **Transaction Information** includes details about payments to and from you and other details of Services you have purchased from us.
- **Technical Information** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access this website.
- **Profile Information** includes your username and password, subscription to our Services, your interests, preferences, feedback and survey responses.
- **Usage Information** includes information about how you use our website and our Services.
- **Marketing and Communications Information** includes your preferences in receiving marketing from us and our third parties and your communication preferences.
- **Criminal convictions and offences information** includes information about convictions to assist with fraud prevention and the verification of authentic consumers.



2.2. Other categories of Personal Information

- We also collect, use and share **Aggregated Information** such as statistical or demographic data for any purpose. Aggregated Information could be derived from your personal information but is not considered Personal Information in law as this information will **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Information to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Information with your Personal Information so that it can directly or indirectly identify you, we treat the combined data as Personal Information which will be used in accordance with this Privacy Policy.
- In respect of some of our Services, we collect **Special Personal Information** about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and biometric information, and alleged criminal behaviour). We will only collect Special Personal Information if we are lawfully entitled to do so.
- If you are a user of the Secure Citizen Application from Secure Citizen (Pty) Ltd ("**Secure Citizen App**"), we collect and otherwise Process certain categories of your Personal Information via the Secure Citizen App including Identity, Contact, Financial, Transaction and Special Personal Information ("**Secure Citizen App Information**") to the extent that the Secure Citizen App uses any of our Services or infrastructure which supports such Services.

2.3. If you fail to provide Personal Information

Where we need to collect Personal Information by law, or under the terms of a contract we have with you, and you fail to provide that information when requested, we may not be able to perform the contract we have or are trying to



enter into with you (for example, to provide you with our Services). In this case, we may have to cancel a Service you have with us but we will notify you if this is the case at the time.

3. How is your Personal Information collected?

3.1. Methods of collection

- We use different methods to collect information from and about you including through:
- **Direct interactions.** You may give us your Identity, Contact and Financial Information by filling in forms or by corresponding with us by post, phone, e-mail or otherwise. This includes Personal Information you provide when you:
 - apply or register for our Services;
 - create an account on our website;
 - subscribe to our newsletters or publications;
 - request marketing to be sent to you;
 - enter a competition, promotion or survey; or
 - give us feedback or contact us.
- **Automated technologies or interactions.** As you interact with our website, we will automatically collect Technical Information about your equipment, browsing actions and patterns. We collect this Personal Information by using cookies, server logs and other similar technologies. We may also receive Technical Information about you if you visit other websites employing our cookies.



- **Third parties or publicly available sources.** We will receive Personal Information about you from various third parties and public sources as set out below, where relevant to our Services:

- Secure Citizen App Information from Secure Citizen (Pty) Ltd, its affiliates or sub-contractors.

- Technical Information from the following third parties:
 - (a) analytics providers;
 - (b) advertising networks; and
 - (c) search information providers.

- Contact, Financial and Transaction Information from providers of technical, payment and delivery services.

- Identity Information and Special Categories of Personal Information from state or law enforcement agencies including the Department of Home Affairs.

- Identity and Contact Information from data brokers or aggregators.

- Identity and Contact Information from publicly available sources.

- The SAFPS members, providing confirmed fraud information and Victim information.



4. Usage of Personal Information

4.1. How we use your Personal Information

We will only use your Personal Information when the law allows us to. Most commonly, we will use your Personal Information in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you or deliver our Services.
- Where it is necessary for our legitimate interests (or those of a third party).
- Where we need to comply with a legal obligation.
- Where we have obtained your consent to Process your Personal Information for the specific purposes described to you. Where you have provided such consent, you have the right to withdraw it at any time by contacting us, however you may not be able to access certain Services if you withdraw consent.

4.2. Purposes for which we will use your Personal Information

We have set out below, in a table format, a description of all the ways we plan to use your Personal Information, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may Process your Personal Information for more than one lawful basis depending on the specific purpose for which we are using your information. Please contact us if you need details about the specific legal basis we are relying on to Process your Personal Information where more than one basis has been set out in the table below.



Purpose/Activity	Type of Personal Information	Lawful basis for Processing including basis of legitimate interest
A. Using our Services		
To register and manage your subscription as a Member to the SAFPS database and employment application fraud and employee fraud database (see definition of Services in the Glossary)	(a) Identity Information (b) Contact Information	Performance of a contract with you
To verify your authenticity as an applicant consumer for credit / Services and products through the Secure Citizen App or SAFPS databases	(a) Identity Information (b) Contact Information (c) Secure Citizen App Information	Your consent
To enable us to perform our obligations to you in terms of a written contract, and/or to enable us to receive services you may be providing to us in terms of a written contract	(a) Identity Information (b) Contact Information (c) Financial Information	Performance of a contract with you
B. Assistance to consumers and victims		
To enable you to receive our assistance to protect you from fraudulent activities including identity theft and impersonation	(a) Identity Information (b) Contact Information (c) Financial Information	(a) Your consent (b) Protects your legitimate interest
To enable you receive our protective registration assistance to protect you from incurring losses related to fraudulent activities	(a) Identity Information (b) Contact Information (c) Financial Information	(a) Your consent (b) Protects your legitimate interest
C. Fraud prevention		
To combat fraud and assist our Members with detecting	(a) Identity Information	(a) Pursuit of our legitimate interests



and preventing fraudulent activity, and protecting consumers against identity theft and impersonation	(b) Contact Information (c) Financial Information	(b) Pursuit of legitimate interests of a third party (for example, our Members) to whom the information is supplied
D. Website		
To administer and protect our business, this website and our Services (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity Information (b) Contact Information (c) Technical Information	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity Information (b) Contact Information (c) Profile Information (d) Usage Information (e) Marketing and Communications Information (f) Technical Information	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, Services, marketing, customer relationships and experiences	(a) Technical Information (b) Usage Information	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
E. General		
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or Privacy Policy	(a) Identity Information (b) Contact Information (c) Profile Information	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation



<p>(b) Asking you to leave a review, take a survey or provide feedback</p> <p>(c) communication required for the purposes of fulfilling our services or to indicate changes to services</p>	<p>(d) Marketing and Communications Information</p>	<p>(c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)</p>
<p>To enable you to complete a survey</p>	<p>(a) Identity Information</p> <p>(b) Contact Information</p> <p>(c) Profile Information</p> <p>(d) Usage Information</p> <p>(e) Marketing and Communications</p>	<p>(a) Performance of a contract with you</p> <p>(b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)</p>
<p>To make suggestions and recommendations to you about services that may be of interest to you</p>	<p>(a) Identity Information</p> <p>(b) Contact Information</p> <p>(c) Technical Information</p> <p>(d) Usage Information</p> <p>(e) Profile</p> <p>(f) Marketing and Communications</p>	<p>Necessary for our legitimate interests (to develop our products/services and grow our business)</p>

4.3. Marketing

We provide you with choices regarding certain Personal Information uses, particularly around marketing and advertising.

4.4. Promotional offers from us

We may use your Identity, Contact, Technical, Usage and Profile Information to form a view on what we think you may want or need, or what may be of interest to



you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You may receive marketing communications from us if you have requested information from us, subscribed to our Services, and/or you have not opted out of receiving that marketing.

4.5. Third-party marketing

We will get your express opt-in consent before we share your Personal Information with any third party for marketing purposes.

4.6. Opting out

You can ask us or third parties to stop sending you marketing messages at any time by contacting us at any time.

Where you opt out of receiving these marketing messages, this will not apply to Personal Information provided to us as a result of a subscription to a Service.

4.7. Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly.

4.8. Change of purpose

We will only use your Personal Information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

If we need to use your Personal Information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.



Please note that we may Process your Personal Information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5. Disclosures of your Personal Information

We may share your Personal Information with the parties set out below for the purposes set out in the table above (see section 4.2 of this Privacy Policy):

- Third parties whom we subcontract to provide our Services like software developers and other IT vendors.
- Third parties, to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your Personal Information in the same way as set out in this Privacy Policy.

We require all third parties to respect the security of your Personal Information and to treat it in accordance with the law. We usually do not allow our third-party service providers to use your Personal Information for their own purposes and usually only permit them to process your Personal Information for specified purposes and in accordance with our instructions.

6. Cross-border transfers of Personal Information

we may transfer your Personal Information out of South Africa to countries which may not have data protection laws similar to those of South Africa for storage purposes and other lawful business reasons.



7. Security

We have put in place appropriate security measures to prevent your Personal Information from being lost, damaged, destroyed in an unauthorised way or accessed in an unauthorised way. In addition, we limit access to your Personal Information to those employees, agents, contractors and other third parties on a need to know basis. We will use reasonable efforts to ensure that they will only Process your Personal Information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected Personal Information breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

8. Our retention of your Personal Information

8.1. Duration of retention

We may retain your Personal Information indefinitely, unless you object, in which case we will only retain it if we are legally permitted or obliged to do so.

In some circumstances you can ask us to delete your information. For more information about this, see section 9 below to view your legal rights.

9. Your legal rights

9.1. Rights

Under certain circumstances, you have the following rights under personal information protection laws in relation to your Personal Information:



- **Notification that your Personal Information is being collected.** When your Personal Information is collected, you have the right to be informed that your information is collected and where the information is not collected from you, you have the right to be informed of the source from whom/which it is collected.
- **Notification of security compromises.** Where reasonable grounds exist for us to believe that your Personal Information has been accessed or acquired by an unauthorised person, you have the right to be notified.
- **Request access to your Personal Information.** You have the right to confirm, free of charge, whether or not we hold any of your Personal Information, and to the extent that we do hold your information, to request a copy or description of that record for a prescribed fee **OR** free of charge. Please contact us to view our PAIA Manual which sets out how you can request access to your Personal Information. You will be required to provide adequate proof of your identity so that we can confirm your identity and ensure your right to access your Personal Information. We may need to request other specific information from you to help us process your request. This is a security measure to ensure that Personal Information is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.
- **Request correction of your Personal Information.** You have the right to request us to correct or delete your Personal Information which we have in our possession, where it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.
- **Request destruction or deletion of your personal information.** You have the right to ask us to delete or remove your Personal Information



where there is no good reason for us continuing to Process it. You also have the right to ask us to delete or remove your Personal Information where you have successfully exercised your right to object to Processing (see below), where we may have Processed your Personal Information unlawfully or where we are required to erase your Personal Information to comply with the law. Note, however, that we may not always be able to comply with your request of destruction or deletion for specific legal or practical reasons which will be notified to you, if applicable, at the time of your request.

- **Object to Processing of your Personal Information.** You have the right to object to our Processing of your Personal Information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to Processing on this ground. You also have the right to object where we are Processing your Personal Information for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your Personal Information which override your right to object to Processing.
- **Request restriction of Processing your Personal Information.** This enables you to ask us to suspend the Processing of your Personal Information in the following scenarios:
 - If you want us to establish the information's accuracy.
 - Where we no longer need the information for the purpose for which the information was initially collected but we need it for purposes of proof.
 - Where our use of the information is unlawful but you do not want us to erase it.
 - If you want us to transmit your information into another automated processing system.



- **Withdraw consent.** You have the right to withdraw your consent at any time where we are relying on consent to Process your Personal Information. However, this will not affect the lawfulness of any Processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain Services to you. We will usually advise you if this is the case at the time you withdraw your consent.
- **Submit a complaint to the Information Regulator.** You have the right to submit a complaint to the Information Regulator regarding an alleged interference with the protection of your Personal Information.
- If you wish to exercise any of the rights set out above, please contact us.

9.2. Time limit to respond

We try to respond to all legitimate requests as soon as reasonably possible.

10. Glossary

“Member” means any person with whom the SAFPS concludes a membership agreement to provide access to a shared database containing data that relates to incidents of fraud or suspected fraud and includes data of persons involved in such incidents.

“Personal Information” means information relating to you, and includes Identity Information, Contact Information, Financial Information, Transaction Information, Technical Information, Profile Information, Usage Information, Marketing and Communications Information, and Special Personal Information.



“Privacy Policy” means this Privacy Policy issued by SAFPS.

“Process” means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including-

- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, as well as restriction, degradation, erasure or destruction of information, and

“Processing” and **“Processed”** have corresponding meanings.

“Responsible Party” means SAFPS.

“Secure Citizen App” is the mobile application developed by or on behalf of Secure Citizen (Pty) Ltd (<https://securecitizen.co.za/>), and aims to protect your identity digitally by providing an integrated multi-modal biometric platform. The platform employs the latest technologies and facilitates ongoing verification, validation and eKYC (electronic Know Your Customer) solutions.

“Services” includes the following:

- **SAFPS database:** A database of persons involved in fraudulent behaviours which is capable of identifying individual and syndicate-type fraud;
- **Fraud victim registration:** Where a consumer whose identity has been fraudulently used by another, and/or whose details are reported by the Member to us for the purposes of such consumer’s protection, we will



file the consumer's details on our database as a "victim of impersonation";

- Protective registration: An internet-based service to the general public for the registration of lost or stolen identity books and passports and victims of identity fraud;
- Employment application fraud and employee fraud database: A database of persons involved in fraudulent activities during the recruitment process and in the workplace;
- Data analysis service: Produces matches across a variety of data fields in milliseconds and portrays the data in graphic format; and
- Secure Citizen App: We have partnered with Secure Citizen (Pty) Ltd to provide you some of the services made available through the Secure Citizen App. You are referred to the privacy policy of Secure Citizen (Pty) Ltd [Secure Citizen Private Policy Link](#)
- to the extent that any Processing of your Personal Information through the Secure Citizen App falls under the scope of that privacy policy.

"Special Personal Information" includes personal information concerning race or ethnic origin, trade union membership, health or biometric information of a data subject; or 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 or the disposal of such proceedings.

For further details regarding the above services, please visit our website.