



REDS Check (PTY) LTD PROTECTION OF PERSONAL INFORMATION (POPI) POLICY

POLICY STATEMENT

In terms of the Protection of Personal Information Act 4 of 2013 ("PoPI"), any responsible party that processes personal information must do so in accordance with the principles outlined in PoPI.

This policy forms part of REDS Check's internal business processes and procedures.

REDS Check's Board, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of REDS Check who are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.

Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

1. INTRODUCTION

The right to privacy is an integral human right recognised and protected in the South African Constitution and in PoPI. PoPI aims to promote the protection of privacy by providing guiding principles intended to be applied to the processing of personal information in a context-sensitive manner. Through the provision of services, REDS Check is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders. A person's right to privacy entails having control over their personal information and being able to conduct their affairs relatively free from unwanted intrusions. Given the importance of privacy, REDS Check is committed to effectively managing personal information in accordance with PoPI's provisions.

2. DEFINITIONS

2.1 Personal Information

Personal information is any information that can be used to identify a person. It relates to an identifiable, living, natural person, and, where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to, information concerning:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or
- mental health, disability, religion, conscience, belief, culture, language and birth of a person;

- information relating to the education or the 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;
- 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.

2.2 Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an individual client or customer, or a company that supplies REDS Check with products or other goods or services.

2.3 Responsible Party

The responsible party is the entity that requires the personal information for a particular purpose and determines the purpose and means of processing it. In this case, REDS Check is the responsible party.

2.4 Operator

An operator is a person who processes personal information for a responsible party under a contract or mandate, without being under that party's direct authority. For example, a third-party service provider that has contracted with REDS Check to shred documents containing personal information.

2.5 Information Officer

The Information Officer is responsible for ensuring REDS Check's compliance with PoPI.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under PoPIA before performing their duties. Deputy Information Officers may also be appointed to assist the Information Officer.

2.6 Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- 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 any restriction, degradation, erasure or destruction of information.

2.7 Record

Means any recorded information, regardless of form or medium, including:

- Writing on any material;
- Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.8 Filing System

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.9 Unique Identifier

Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2.10 De-Identify

This means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.11 Re-Identify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.12 Consent

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

2.13 Direct Marketing

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting or offering to supply, in the ordinary course of business, any services to the data subject; or
- Requesting the data subject to make a donation of any kind for any reason.

2.14 Biometrics

Means a technique of personal identification that is based on physical, physiological or behavioural characteristics, including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

3. POLICY PURPOSE

This policy demonstrates REDS Check's commitment to protecting the privacy rights of data subjects in the following manner:

- 3.1 Through stating desired behaviour and directing compliance with the provisions of PoPI and best practice.
- 3.2 By cultivating an organisational culture that recognises privacy as a valuable human right.
- 3.3 By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
- 3.4 By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of REDS Check.
- 3.5 By raising awareness through training and providing guidance to individuals who process personal information, enabling them to act confidently and consistently.

4. POLICY APPLICATION

This policy and its guiding principles apply to:

- 4.1 REDS Check's Board
- 4.2 All branches, business units and divisions of REDS Check
- 4.3 All employees and volunteers
- 4.4 All contractors, suppliers and other persons acting on behalf of REDS Check

The policy's guiding principles apply in all situations and must be read in conjunction with PoPI and REDS Check's PAIA Policy, as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with PoPI's provisions is activated in any situation where there is a processing of personal information entered into a record by or for a responsible person who is domiciled in South Africa.

PoPI does not apply in situations where the processing of personal information:

4.5 is concluded in the course of purely personal or household activities, or

4.6 where the personal information has been de-identified.

5. RIGHTS OF DATA SUBJECTS

Where appropriate, REDS Check will ensure that its clients are made aware of the rights conferred upon them as data subjects. REDS Check will ensure that it gives effect to the following six rights.

5.1 The Right to Access Personal Information

REDS Check recognises that a data subject has the right to establish whether REDS Check holds personal information relating to them, including the right to request access to that information.

An example of a “Personal Information Request Form” is provided in Annexure A.

5.2 The Right to have Personal Information Corrected or Deleted

The data subject has the right, where necessary, to request that their personal information be corrected or deleted where REDS Check is no longer authorised to retain it.

5.3 The Right to Object to the Processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of their personal information. In such circumstances, REDS Check will give due consideration to the request and to the requirements of PoPI. REDS Check may cease to use or disclose the data subject’s personal information and, subject to any statutory and contractual record-keeping requirements, may also approve the destruction of the personal information.

5.4 The Right to Object to Direct Marketing

The data subject has the right to object to the processing of their personal information for purposes of direct marketing by means of unsolicited electronic communications.

5.5 The Right to Complain to the Information Regulator

The data subject has the right to lodge a complaint with the Information Regulator regarding an alleged infringement of any of the rights protected under PoPI and to institute civil proceedings regarding alleged non-compliance with the protection of their personal information.

An example of a “PoPI Complaint Form” is provided in Annexure B.

5.6 The Right to be Informed

The data subject has the right to be notified that REDS Check is collecting their personal information. The data subject also has the right to be notified in any situation where REDS Check has reasonable grounds to believe that their personal information has been accessed or acquired by an unauthorised person.

6. GENERAL GUIDING PRINCIPLES

REDS Check manages and maintains an Industry Database to provide a central point of reference for employees in the banking, finance and related industries who have been dismissed for dishonesty-related offences, or found guilty of such offences following a post-termination enquiry. This can be used by all approved and registered users of the Industry Database as a reference when screening prospective employees to manage the risk of a repetition of such behaviour by a user. Therefore, acknowledging that REDS Check will hold the personal information of users and consenting employees, it is imperative that all employees and persons acting on behalf of REDS Check will at all times be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability

Failing to comply with PoPI could damage REDS Check's reputation or expose REDS Check to a civil claim for damages. The protection of personal information is therefore everyone's responsibility.

REDS Check will ensure that the provisions of PoPI and the guiding principles outlined in this policy are complied with. However, REDS Check will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

6.2 Processing Limitation

REDS Check will ensure that personal information under its control is processed:

- in a fair, lawful and non-excessive manner, and
- only with the informed consent of the data subject, and
- only for a specifically defined purpose.

REDS Check will inform the data subject of the reasons for collecting their personal information and obtain written consent before processing it.

REDS Check will, under no circumstances, distribute or share personal information between separate legal entities or with any individuals who are not directly involved in facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of REDS Check's business and be provided with the reasons for doing so.

6.3 Purpose Specification

REDS Check will process personal information only for specific, explicitly defined and legitimate purposes. REDS Check will inform data subjects of these purposes before collecting or recording their personal information.

6.4 Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Therefore, where REDS Check seeks to process personal information it holds for a purpose other than the original purpose for which it was collected, and where this secondary purpose is not compatible with the original purpose, REDS Check will first obtain additional consent from the data subject.

6.5 Information Quality

REDS Check will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. Where personal information is collected or received from third parties, REDS Check will take reasonable steps to confirm its accuracy by verifying it directly with the data subject or through independent sources.

6.6 Open Communication

REDS Check will take reasonable steps to ensure that data subjects are notified that their personal information is being collected, including the purpose for which it is collected and processed. REDS Check will establish and maintain a “contact us” facility for data subjects who want to:

- Enquire whether REDS Check holds related personal information, or
- Request access to related personal information, or
- Request REDS Check to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

6.7 Security Safeguards

REDS Check will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

REDS Check will continuously review its security controls, including regular testing of protocols and measures put in place to combat cyber-attacks on REDS Check’s IT network. REDS Check will ensure that all paper and electronic records comprising personal information are securely stored and accessible only to authorised individuals. All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which REDS Check is responsible. REDS Check’s operators and third-party service providers will be required to enter into data privacy agreements with REDS Check, under which the third party agrees to comply with PoPI and to the lawful processing of any personal information pursuant to the agreement.

6.8 Data Subject Participation

A data subject may request the correction or deletion of their personal information held by REDS Check. REDS Check will ensure that it provides a facility for data subjects who wish to request the correction or deletion of their personal information. Where applicable, REDS Check will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. INFORMATION OFFICERS

REDS Check appointed and registered an Information Officer and a Deputy Information Officer with the South African Information Regulator established under PoPI. The Deputy Information Officer will assist the Information Officer in performing his or her duties.

8. SPECIFIC DUTIES AND RESPONSIBILITIES

8.1 Board

8.1.1. REDS Check's board cannot delegate its accountability, and remains ultimately responsible for ensuring that REDS Check meets its legal obligations under PoPI. However, the board may delegate certain responsibilities under PoPI to management or other capable individuals.

8.1.2. The board is responsible for ensuring that:

8.1.2.1. All persons responsible for processing personal information on behalf of REDS Check:

8.1.2.2. are appropriately trained and supervised to do so,

8.1.2.3. understand that they are contractually obliged to protect the personal information they handle, and

8.1.2.4. are aware that a willful or negligent breach of this policy's processes and procedures may result in disciplinary action against them.

8.1.2.5. Data subjects who wish to enquire about their personal information are informed of the procedure that needs to be followed.

8.1.2.6. A periodic PoPI audit is scheduled to accurately assess and review how REDS Check collects, holds, uses, shares, discloses, destroys and processes personal information.

8.2 Information Officer

REDS Check's Information Officer is responsible for:

8.2.1 Taking steps to ensure REDS Check's reasonable compliance with the provisions of PoPI.

8.2.2 Keeping the board updated on REDS Check's information protection responsibilities under PoPI.

8.2.3 Continually analysing privacy regulations and aligning them with REDS Check's personal information processing procedures. This will include reviewing REDS Check's information protection procedures and related policies.

8.2.4 Ensuring that PoPI Audits are scheduled and conducted regularly.

- 8.2.5 Ensuring that REDS Check makes it convenient for data subjects who want to update their personal information or submit PoPI-related complaints to REDS Check.
- 8.2.6 Approving any contracts entered into with operators, employees and other third parties that may affect the personal information held by REDS Check.
- 8.2.7 Encouraging compliance with the conditions required for the lawful processing of personal information.
- 8.2.8 Ensuring that employees and other persons acting on behalf of REDS Check are fully aware of the risks associated with the processing of personal information and remain informed about REDS Check's security controls.
- 8.2.9 Organising and overseeing awareness training for employees and other individuals involved in the processing of personal information on behalf of REDS Check.
- 8.2.10 Addressing employees' PoPI-related questions.
- 8.2.11 Addressing all PoPI-related requests and complaints made by REDS Check's data subjects.
- 8.2.12 Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate regarding any other matter.

8.3 IT Manager

REDS Check's IT Manager/Service Provider is responsible for:

- 8.3.1. Ensuring that REDS Check's IT infrastructure, filing systems, and any other devices used to process personal information meet acceptable security standards.
- 8.3.2. Ensuring that all electronically held personal information is stored only on designated drives and servers and uploaded only to approved cloud computing services.
- 8.3.3. Ensuring that servers containing personal information are located in a secure location, away from general office space.
- 8.3.4. Ensuring that all electronically stored personal information is backed up and tested regularly.
- 8.3.5. Ensuring that all backups containing personal information are protected against unauthorised access, accidental deletion and malicious hacking attempts.
- 8.3.6. Ensuring that personal information being transferred electronically is encrypted.
- 8.3.7. Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- 8.3.8. Performing regular IT audits to ensure that REDS Check's hardware and software systems are functioning properly.

8.3.9. Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.

8.3.10. Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on REDS Check's behalf, for instance, cloud computing services.

8.4 Employees and other Persons acting on behalf of REDS Check

Employees and other persons acting on behalf of REDS Check will, during the course of their services, gain access to and become acquainted with the personal information of certain customers, suppliers and other employees. They are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of REDS Check may not, directly or indirectly, utilise, disclose or make public, in any manner, to any person or third party, whether within REDS Check or externally, any personal information, unless such information is already publicly known or the disclosure is necessary for the employee or person to perform their duties.

Employees and other persons acting on behalf of REDS Check must seek assistance from the Information Officer if they are unsure about any aspect of protecting a data subject's personal information. Employees and other persons acting on behalf of REDS Check will process personal information only where:

- 8.4.1 The data subject, or a competent person where the data subject is a child, consents to the processing; or
- 8.4.2 the processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- 8.4.3 the processing complies with an obligation imposed by law on the responsible party; or
- 8.4.4 the processing protects a legitimate interest of the data subject; or
- 8.4.5 the processing is necessary for pursuing the legitimate interests of REDS Check or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

- 8.4.6 granted REDS Check explicit written or verbally recorded consent to process their personal information.

Employees and other persons acting on behalf of REDS Check will, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose their personal information is needed and with whom it will be shared.

Consent can be obtained in written form, which includes any appropriate electronic medium that is accurately and readily reducible to printed form.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- 8.4.7 the personal information has been made public, or
- 8.4.8 where valid consent has been given to a third party, or
- 8.4.9 the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of REDS Check will under no circumstances:

- 8.4.10 Process or have access to personal information where such processing or access is not required to perform their respective work-related tasks or duties.
- 8.4.11 Save copies of personal information directly to their own private computers, laptops, or other mobile devices such as tablets or smartphones.
- 8.4.12 Share personal information informally. Access to personal information may be requested from the Information Officer.
- 8.4.13 Transfer personal information outside South Africa without the express permission of the Information Officer.

Employees and other persons acting on behalf of REDS Check are responsible for:

- 8.4.14 Keeping all personal information that they come into contact with secure by taking sensible precautions and following the guidelines outlined in this policy.
- 8.4.15 Ensuring that personal information is held in as few places as necessary. No unnecessary additional records, filing systems and data sets should therefore be created and ensuring that personal information is encrypted before it is sent or shared electronically. The IT Manager/Service Provider will assist employees and, where required, other persons acting on behalf of REDS Check, with the sending or sharing of personal information with authorised external persons.
- 8.4.16 Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password-protected. Passwords must be changed regularly and must not be shared with unauthorised persons.
- 8.4.17 Ensuring that computer screens and other devices are switched off or locked when not in use or when away from their desks.
- 8.4.18 Ensuring that, where personal information is stored on removable media such as external drives, CDs or DVDs, these are kept securely locked away when not in use.

- 8.4.19 Ensuring that, where personal information is stored on paper, such hard copy records are kept in a secure place where unauthorised people cannot access them, for instance, in a locked drawer of a filing cabinet.
- 8.4.20 Ensuring that, where personal information has been printed out, the paper printouts are not left unattended where unauthorised individuals could see or copy them, for instance, near the printer.
- 8.4.21 Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email.
- 8.4.22 Where a data subject's information is found to be out of date, authorisation must first be obtained from the Information Officer to update the information accordingly.
- 8.4.23 Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the Information Officer to delete or dispose of the personal information in the appropriate manner.
- 8.4.24 Undergoing PoPI awareness training from time to time.
- 8.4.25 Where an employee, or a person acting on behalf of REDS Check, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

9. POPI AUDIT

REDS Check's Information Officer will schedule periodic PoPI audits.

The purpose of a PoPI audit is to:

- 9.1 Identify the processes used to collect, record, store, disseminate and destroy personal information.
- 9.2 Determine the flow of personal information throughout REDS Check, including its divisions, business units and branches.
- 9.3 Redefine the purpose for gathering and processing personal information.
- 9.4 Ensure that the processing parameters remain adequately limited.
- 9.5 Ensure that new data subjects are made aware of the processing of their personal information.
- 9.6 Re-establish the rationale for any further processing when information is received via a third party.
- 9.7 Verify the quality and security of personal information.

- 9.8 Monitor the extent of compliance with PoPI and this policy.
- 9.9 Monitor the effectiveness of internal controls established to manage REDS Check's PoPI-related compliance risk.
- 9.10 In performing the PoPI audit, Information Officers will liaise with managers in order to identify areas within REDS Check's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

10. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

- 10.1 Data subjects have the right to:
 - 10.1.1 Request what personal information REDS Check holds about them and why.
 - 10.1.2 Request access to their personal information.
 - 10.1.3 Be informed about how to keep their personal information up to date.
- 10.2 Requests for access to information can be made by email addressed to the Information Officer.
- 10.3 The Information Officer will provide the data subject with a "Personal Information Request Form".

Once the completed form has been received, the Information Officer will verify the data subject's identity before providing any personal information. All requests will be processed and considered in accordance with REDS Check's PAIA Policy.

The Information Officer will process all requests within a reasonable time.

11. POPI COMPLAINTS PROCEDURE

- 11.1 Data subjects have the right to complain where any of their rights under PoPI have been infringed. REDS Check takes all complaints very seriously and will address all PoPI-related complaints in accordance with the following procedure:
 - 11.1.2 PoPI complaints must be submitted to REDS Check in writing. Where required, the Information Officer will provide the data subject with a "PoPI Complaint Form".
 - 11.1.3 If a complaint is received by anyone other than the Information Officer, that person will ensure the full details of the complaint reach the Information Officer within 1 working day.
- 11.2 The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days. The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve it fairly and in accordance with the principles outlined in PoPI.
- 11.3 The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and may have a wider impact on REDS Check's data subjects.

- 11.4 Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with REDS Check's board, after which the affected data subjects and the Information Regulator will be informed of this breach.
- 11.5 The Information Officer will respond to the complainant with a proposed solution and the option to escalate the complaint to REDS Check's board within 7 working days of receipt of the complaint. In all instances, REDS Check will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- 11.6 The Information Officer's response to the data subject may comprise any of the following:
 - 11.6.1 A suggested remedy for the complaint,
 - 11.6.2 A dismissal of the complaint and the reasons for the dismissal,
 - 11.6.3 An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- 11.7 Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- 11.8 The Information Officer will review the complaints process on a periodic basis to assess its effectiveness and improve it where it is found wanting. The reasons for any complaints will also be reviewed to ensure the avoidance of occurrences that give rise to PoPI-related complaints.

12. DISCIPLINARY ACTION

- 12.1 Where a PoPI complaint or a PoPI infringement investigation has been finalised, REDS Check may recommend any appropriate administrative, legal and/or disciplinary action against any employee reasonably suspected of involvement in any non-compliant activity outlined in this policy.
- 12.2 In the case of ignorance or minor negligence, REDS Check will provide further awareness training to the employee. Any gross negligence or willful mismanagement of personal information will be considered a serious form of misconduct for which REDS Check may summarily dismiss the employee.
- 12.3 Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.
- 12.4 Examples of immediate actions that may be taken following an investigation include:
 - 12.4.1 A recommendation to commence disciplinary action.
 - 12.4.2 A referral to appropriate law enforcement agencies for criminal investigation.
 - 12.4.3 Recovery of funds and assets to limit any prejudice or damage caused.

Document updated Date
June 2026

ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer:

Name: _____

Contact Number: _____

Email Address: _____

Please be aware that we may require you to provide proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject

Name & Surname: _____

Identity Number: _____

Postal Address: _____

Contact Number: _____

Email Address: _____

B. Request

I request REDS Check to:

- (a) Inform me whether it holds any of my personal information
- (b) Provide me with a record or description of my personal information
- (c) Correct or update my personal information
- (d) Destroy or delete a record of my personal information

C. Instructions

D. Signature Page

Signature: _____ Date: _____

ANNEXURE B: POPI COMPLAINT FORM

POPI COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

Please submit your complaint to the Information Officer:

Name: _____

Contact Number: _____

Email Address: _____

Where we are unable to resolve your complaint to your satisfaction, you have the right to complain to the Information Regulator.

The Information Regulator:

Email: inforreg@justice.gov.za

Website: <http://www.justice.gov.za/inforeg/index.html>

A. Particulars of Complainant

Name & Surname: _____

Identity Number: _____

Postal Address: _____

Contact Number: _____

Email Address: _____

B. Details of Complaint

C. Desired Outcome

D. Signature Page

Signature: _____ Date: _____