CJ BEZUIDENHOUT INC

Policy in terms of the Protection of Personal Information Act 4 of 2013, incorporating PAIA Manual in terms of section 51 of the Promotion of Access to Information Act 2 of 2000

POPIA/PAIA POLICY

Created Date:	5 August 2026
Review Period:	Annually
Review Date:	5 August 2027
Information Officer:	CJ Bezuidenhout
Deputy Information Officer:	None

This document is the property the above-mentioned responsible party ("RP") and may not be distributed without the consent of the head of the RP. Any unauthorised copying, alteration, or distribution is strictly prohibited and may incur penalties in law.

Purpose 3
Policy Statements 3
Definitions 3
Responsibilities and Accountability 6
Information/ Deputy Information Officer 7
Information Life Cycle 8
Conditions for Lawful Processing 8
How we Manager Personal Information:
- Data Collection 10
- Data Processing 11
- Data Storage 12
- Data Sharing 13
- Data Retention & Destruction 14

Internal Decision Making Rules 15
Data Subject Rights 18
Breach Procedure 20
Basic Security Safeguard 21
PAIA Manual:
- Nature of Records Held 22
- Recipients of Records Held 25
- Requesters of Records Held 25
- Remedies for Refusal by RP 25
- Requesting Procedure 26

POPIA Form 1: Objection to Processing 27
POPIA Form 2: Request for Correction/ Deletion 28
PAIA Form 2: Request for Access 30
PAIA Form 3: Outcome of Request 34
Internal Breach Report 36

PURPOSE

The purpose of this Policy is to:

- Provide guidance to all employees on the Responsible Party's approach to the lawful processing of personal information, including the allocation of responsibilities, clear decision-making principles, practical procedures for responding to personal information breaches, and the implementation of minimum-security measures to safeguard personal information.

- Inform data subjects of their rights under applicable data protection legislation and provide guidance on how to exercise those rights, including requests for access to personal information, confirmation of processing activities, objections to processing, and requests for the correction, deletion, or destruction of personal information.

POLICY STATEMENT

The Responsible Party is committed to ensuring accountability for compliance with the Protection of Personal Information Act, 2013 (POPIA), and will implement appropriate measures to give effect to all applicable conditions for the lawful processing of personal information. Personal information will be processed lawfully, reasonably, and in a manner that does not infringe the privacy of data subjects. The Responsible Party further commits to taking reasonably practicable steps to ensure that personal information is complete, accurate, not misleading, and updated where necessary, having regard to the purpose for which the information is processed.

DEFINITIONS

Child means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

Competent person means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

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

Data subject means the person to whom personal information relates.

Day means business days, unless otherwise indicated.

Deidentify 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.

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 any goods or services to the data subject; or
- Requesting the data subject to make a donation of any kind for any reason.

Electronic communication means any text, voice, sound, or image message sent over an electronic communications network that is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Employee means any director, partner, associate, manager or employee in the employ of the firm, including consultants

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.

Head means the proprietor, managing partner, or managing director of the firm, being the senior attorney in charge of the firm.

Information Officer in relation to a private body, means the head of a private body as contemplated in section 1 read with section 55 of the Act. This shall include a Information Officer appointed in terms of section 56 of the Act.

Operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

Person means a natural or juristic person.

Personal information means information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including but not limited to:

- Information relating to race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, 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 private or confidential.
- The views or opinions of another individual about the person.
- The name of the person if it appears with other personal information or if the disclosure of the name itself would reveal information about the person.

Processing 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.
- Merging, linking, as well as restriction, degradation, erasure, or destruction of information.

Public record means a record that is accessible in the public domain and which is in the possession of or under the control of a public body.

Record means any recorded information:

- Regardless of form or medium, including:
    - Writing on any material.
    - Information produced, recorded, or stored electronically.
    - Labels, markings, or other writings identifying or describing anything.
    - Books, maps, plans, graphs, or drawings.
    - Photographs, films, negatives, tapes, or other visual images.
- In the possession or under the control of a responsible party.
- Whether or not it was created by a responsible party.
- Regardless of when it came into existence.

Regulator means the Information Regulator established in terms of section 39 of the Act.

Re-identify in relation to personal information of a data subject, means to resurrect any information that has been de-identified.

Responsible party ("RP") means a public or private body or any other person which determines the purpose of and means for processing personal information. In terms of this policy, the **responsible party** is **CJ Bezuidenhout Inc** and its principal place of business is at **Law Chambers, 678 Trichardt Road, Boksburg**.

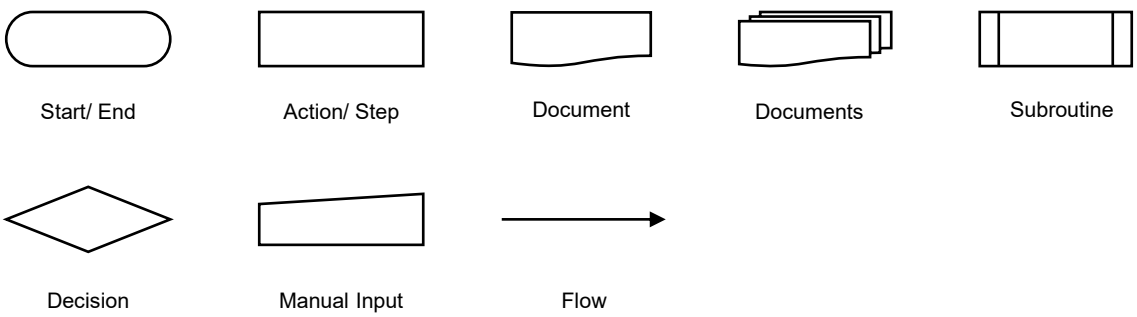
Restriction means to withhold from circulation, use, or publication any personal information but not delete or destroy such information.

Special personal information means personal information that is more sensitive in nature and is subject to stricter processing conditions under POPIA. Based on the provision you provided, it includes:

- Religious or philosophical beliefs
- Race or ethnic origin
- Trade union membership
- Political persuasion
- Health or sex life
- Biometric information
- Criminal behaviour, specifically:
    - The alleged commission of an offence by the data subject
    - Legal proceedings related to such offence or the outcome of those proceedings

  This type of information may not be processed unless specific exceptions under section 27 apply.

Unique identifier means any identifier assigned to a data subject that uniquely identifies that data subject in relation to a responsible party.





Head/ Information Officer

- Ultimate responsibility for POPIA governance.
- Overall compliance (monitor and enforce).
- Identify risks related to personal information.
- Develop, implement and enforce additional standards and procedures to attain compliance.

- Working with and engaging with Information Regulator as required (including reporting in terms of the Act).
- Assess the impact of any potential or actual data breaches and implement mitigation strategies as required.
- Delegate Deputy Information Officer/s if required.

The RP must take appropriate and reasonable organisational/ operational measures, having regard for the risks involved, to protect its information infrastructure (manual and electronic) against data breaches.



Deputy Information Officer

- Identify risks related to personal information.
- Develop, implement and enforce additional standards and procedures to attain compliance.

- Working with and engaging with Information Regulator as required (including reporting in terms of the Act).
- Assess the impact of any potential or actual data breaches and implement mitigation strategies as required.



Line Management Function

- Identify risks related to personal information.
- Monitoring and enforcing divisional compliance.

- Identify risks related to personal information.
- Monitoring and enforcing divisional compliance.



Human Resource Function

- Identify risks related to personal information.
- Monitoring and enforcing divisional compliance.
- Maintain employee records.

- Ensuring access control as required.
- Escalating divisional breaches to Information Officer.

Information Technology Function

- Identify system-based vulnerabilities and risks.
- Implement, monitor, and enforce appropriate safeguards to prevent data breaches.
- Implement, monitor, and enforce safe usage practices to prevent data breaches.

- Escalate any attempted or actual breaches to Information Officer.
- Take steps to safeguard electronic data in the event of a data breach.
- Assist with the assessment of impact of any potential or actual data breach and make recommendations to mitigate the risks.

The RP must take appropriate and reasonable technical measures, having regard for the risks involved, to protect its IT infrastructure against data breaches.

All Employees

- Identify risks related to personal information.
- Day-to-day compliance with policy provisions and implemented safeguards.

- Escalate non-compliance to line manager.
- Escalate any data breaches to line manager.

Information Officer/ Information Officer



The **Information Officer** is:

Name:	Coenie Bezuidenhout
Email Address:	coenie@bezuidenhoutinc.co.za
Contact Number:	082 300 0379



The **Information Officer** is:

Name:	None
Email Address:	None
Contact Number:	None

INFORMATION LIFE CYCLE

The information lifecycle illustrates the key stages through which personal information passes within the RP and provides an overview of the RP's approach to the protection of personal information.

1. Collection	2. Processing	3. Storage	4. Sharing	5. Retention	6. Destruction
We only collect the information we need, directly from you where possible.	We use your information lawfully, fairly, and for the purpose we told you about.	We keep your information secure and only for long as necessary.	We share your information only when allowed by law, with your consent, or with trusted parties.	We keep you information no longer than legally required.	We securely destroy or de-identify your information when we no longer need it.

CONDITIONS FOR LAWFUL PROCESSING

The RP adheres to the conditions for lawful processing in terms of **section 8 - 25** of POPIA. The following key principles guide how we deal with information throughout the information life cycle.



ACCOUNTABILITY

We are responsible for ensuring compliance with the Act.



PROCESSING LIMITATION

We process information lawfully, fairly, and in a reasonable manner.



PURPOSE SPECIFICATION

We collect for specific, explicit, and lawful purposes.



FURTHER PROCESSING LIMITATION

We use the information only for the purpose collected, or compatible purposes.



INFORMATION QUALITY

We ensure that information is accurate, complete, and up to date.



OPENNESS

We are open and transparent about how we collects and use information.



SECURITY SAFEGUARDS

We protect information with appropriate technical and organisational measures.



DATA SUBJECT PARTICIPATION

We allow access to your information when you request it and enable corrections.

Take note of how we manage information



Practical Rule: Personal information shall only be collected by an authorised person for a specific and lawful purpose, using only the information necessary to achieve that purpose. Where reasonably practicable, information will always be collected directly from the data subject, after the required privacy notice has been provided and where a lawful basis for processing exists. The collection of special personal information and children's personal information is subject to additional justification and consent.

Who may collect information?

Personal information may only be collected by authorised employees, which include our **support staff** and **attorneys**.

What information may be collected?

The RP will only collect personal information that is **necessary**, **relevant**, and **proportionate** to a specific, lawful, and legitimate business purpose.

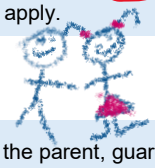
Collection Purposes

- Provision of legal and related services.
- Billing and invoicing.
- Case management.
- Communication (this may include 3rd parties).
- Client identification and verification (FICA).
- Compliance with legal and regulatory obligations.
- Conducting legal research and case preparation.
- Employment related (recruitment, HR records, payroll).
- Instructing service providers.
- Handling complaints or disputes.
- Handling requests for access to personal information.
- Maintaining transaction records and agreements
- Other (subject to informing you).

What about special personal information?

We generally don't collect special personal information, but if we need to, we will ask consent from the data subject, unless one of the exclusions in terms of section 27(1) apply.

What about kids?



We will always ask for consent from the parent, guardian, or other competent person unless…

- It is necessary to defend a child or to enforce their rights under law.
- It is necessary to comply with an international law obligation.
- The child made information available publicly with the consent of a competent person.

From whom may it be collected?

We will always aim to collect it **directly from the data subject** (except in the case of kids, we ask the parent or guardian). Sometimes we collect from 3rd parties with the data subject's knowledge, unless it is to advance the data subject's legitimate interests, and subject to non-prejudice. If the information is publicly available, we are required by law, it's required for proceedings in a court or other tribunal, is in the interest of national security, is to maintain the data subject's legitimate interests, or its not practical, we may collect from anywhere necessary.

How/when is consent obtained?

The RP will obtain consent **prior** to processing any personal information.

Consent is deemed affirmative if the data subject submits the information after it was requested.

Data Subject Notifications

could be in writing or verbally...

- **What** we collect (sometimes this is clear based on the questions we ask or the forms you complete), and from who (if it is a third party).
- What we will **use** the information for, if it does not align with our generally usage purposes.
- Whether it is **mandatory/ voluntary** to submit the information.
- What would **happen** if you don't provide the information.
- If the information is required **in terms of a law**.
- Whether the information will be **shared** with a 3rd party, who they are, and when information will be shared with someone outside SA.
- Your rights, which is included.

Data Subject Rights

- To ask us what information about you we have.
- To object to us processing your information.
- To withdraw your consent for processing.
- To request rectification of your information.
- To lay a complaint with the Information Regulator.



Practical Rule: Personal information will only be processed for the specific purpose for which it was collected. Access to personal information is restricted to authorised persons only who require the information to execute their duties. Further processing will only occur where is it compatible with the original purpose for collection or where the exclusion in terms of the Act applies. Processing will stop once the purpose was fulfilled, an objection was received, or the lawful basis for processing no longer exists.

What information may be processed?

We process the information we collected subject to it being relevant and necessary for the work you want us to do. We call this '**to fulfil our mandate**'. When the information relates to children or special personal information, we will seek consent, unless one of the exclusions in terms of the Act applies.

What is the intended purpose of the information?

Processing Purposes

- Provision of legal and related services.
- Billing and invoicing.
- Case management.
- Communication (this may include 3rd parties).
- Client identification and verification (FICA).
- Compliance with legal and regulatory obligations.
- Conducting legal research and case preparation.
- Employment related (recruitment, HR records, payroll).
- Instructing service providers.
- Handling complaints or disputes.
- Handling requests for access to personal information.
- Maintaining transaction records and agreements
- Other (subject to informing you).

same as collection purpose...nothing more!

Who may access the information?

Personal information may only be accessed by authorised employees, which include our **support staff** and **attorneys**. Sometimes we share information with authorised 3rd parties such as services providers (including systems) and government agencies instrumental to the fulfilment of our mandate. We typically don't make use of 'operators' to process data on our behalf. All 3rd parties are required to comply with POPIA, but we keep a close eye.

When must processing activities be stopped?

- If the data subject raises concerns about information accuracy and would like to review it.
- Once our mandate has been discharged/ fulfilled.
- If the data subject alleges the processing was unlawful and requests retention rather than destruction.
- If the data subject requested us to transfer the information to another automated processing system.

Who about further processing?

We may perform further processing, subject to:

- The data subject's consent.
- If it aligns with the original purpose for which we collected the information.
- If we de-identified the information, including uses for statistical or similar purposes (subject to appropriate safeguards).
- If permitted in law: the information is public, required by law, or to mitigate or prevent a serious threat to public safety.

What systems may be used?

The Act does not prescribe…but it must include appropriate and reasonable technical and organisational safeguards.

We use systems that help us verify the identity of clients, that help us perform case management, manage client accounts, obtain information important to our instructions, and specific systems such as government databases etc to upload information that is legally required about our clients and employees. We also use email, local servers, and cloud storage.

Consider the original and new purpose: the nature of the information: consequences for the data subject: how the information was collected: contractual rights between the parties.



Practical Rule: Personal information is stored in physical and electronic form, subject to appropriate technical and organisational safeguards being implemented to protect its confidentiality, integrity, and availability. Only authorised persons will have access to stored information. Our storage risks are assessed regularly and where it is stored by 3rd parties, they are required to comply with the provisions of POPIA. We do not store any information outside South Africa.

What we use!

- [x] Physical systems such as filing cabinets and filing rooms
- [ ] Internal servers
- [x] Cloud-based systems
- [x] Third-party service providers
- [ ] Off-site archives
- [ ] International data centres

Where may information be stored?

The Act does not prescribe…but it must include appropriate and reasonable technical and organisational safeguards.

We make sure that all our systems are protected against loss, damage, unauthorised destruction, unlawful access, and unlawful processing.

What measures are taken to protect physical and electronic records?

Physical Protection…

- [x] Secure filing cabinets and storage facilities
- [ ] Controlled key management
- [x] Restricted access to authorised personnel only
- [ ] Visitor access controls
- [x] Alarm systems/ physical security measures
- [x] Protection against fire, flood, and environmental damage
- [ ] Secure transportation records
- [x] Clean desk practices where appropriate
- [x] Procedures for reporting loss or theft of records

Digital Protection…

- [x] User authentication and password controls
- [x] Role-based access permissions
- [ ] Multi-factor authentication where appropriate
- [ ] Encryption of sensitive information
- [x] Secure backups
- [x] Antivirus and malware protection
- [x] Firewalls and network security controls
- [ ] Logging and monitoring of access
- [ ] Secure disposal of electronic media
- [ ] Regular vulnerability assessments and security reviews
- [ ] Patch and update management
- [ ] Incident response procedures



Practical Rule: Personal information will only be disclosed where there is a lawful basis for the disclosure, the disclosure is necessary for a legitimate business, legal, or operational purpose, and the recipient is authorised to receive information. Prior to disclosure we will confirm the identity of the recipient, only share necessary information, apply appropriate and reasonable safeguards, and obtain consent if required. Any disclosures outside of South Africa will comply with section 72 of POPIA.

When may information be disclosed?

Sometimes we share information with authorised 3rd parties such as services providers (including systems) and government agencies instrumental to the fulfilment of our mandate. We typically don't make use of 'operators' to process data on our behalf. All 3rd parties are required to comply with POPIA, but we keep a close eye.

We may disclose information under the following lawful circumstances:

- It is compatible with the original purposes for which the information was obtained.
- It is consistent with the notice of collection we gave to the data subject.
- Internationally, if the data subject consented, the transfer is necessary, it benefits the data subject, and the recipient has similar privacy laws in place.

Examples of Lawful Disclosures

- The data subject consented.
- When necessary to fulfil a contract with the data subject.
- When required by law or a court order.
- When necessary to protect the legitimate interests of the data subject.
- When necessary to protect the legitimate interest of the RP.
- When necessary to prevent or investigate unlawful conduct.
- To an authorised operator.

What measures are in place?

We make use of a disclosure checklist. Attorneys and support staff are provided with training so that the checklist is incorporated in their day-today procedures.

Disclosure Checklist...

- [ ] The recipient's identity has been verified
- [ ] The recipient has a lawful right to receive the information
- [ ] The disclosure is necessary and aligned with the purpose
- [ ] There is a lawful basis for the disclosure
- [ ] Any consent requirements have been satisfied
- [ ] Appropriate confidentiality obligations exists
- [ ] Disclosure is approved as part of an official internal procedure
- [ ] There is a clear and accessible audit trail of the disclosure

Practical Rule: Personal information will only be retained for as long as necessary to fulfil our mandate and as required by law. Once the retention period has expired and no lawful basis for continued retention exists, the information will be securely destroyed, deleted, or de-identified in a manner that prevents reconstruction or recovery.

How long will information be retained?

Generally, information will not be retained any longer than necessary to achieve the purpose for which it was collected, but it can be retained longer if:

- The data subject consented.
- Retention is required by law.
- The RP requires it for lawful purposes related to its functions and activities.
- Retention is required by virtue of a contract between the parties.

In terms of the Legal Practice Act, attorneys are required to retain all records related to an instruction for at least 7 years.

Legal Practice Act requirements...

After retention we...

- Destroy; or
- Delete; or
- De-identify (as applicable).

Where will records be retained?

We use the below storage locations all subject to appropriate and reasonable technical and organisational safeguards.

- ☐ Secure filing facilities (onsite)
- ☐ Secure filing facilities (off-site)
- ☑ Electronic or cloud storage (on-site)
- ☐ Electronic or cloud storage (off-site)

Which One?

Information must be destroyed or deleted so that it can not be reconstructed in an intelligible form. The method we choose considers:

- The nature of the information.
- The degree of sensitivity.
- Who would have access to the information.
- If the chosen method is adequate to prevent reconstruction.

Which methods are used?

Physical Records..

- ☑ Shredding
- ☐ Incineration
- ☐ Destruction by an accredited service provider

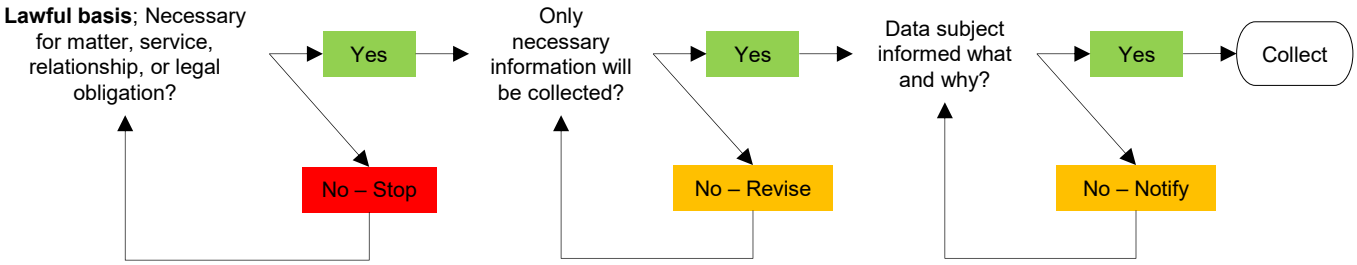
Electronic Records..

- ☑ Secure deletion (using recognised tools)
- ☐ Cryptographic erasure
- ☐ Physical destruction of storage media
- ☐ Destruction be an accredited service provider

The purpose of these Internal Decision-Making Rules is to provide employees with practical guidance for the lawful handling of personal information throughout its lifecycle. These rules are intended to support compliance with POPIA by establishing clear principles and decision-making criteria for the collection, processing, storage, sharing, retention and destruction of personal information.

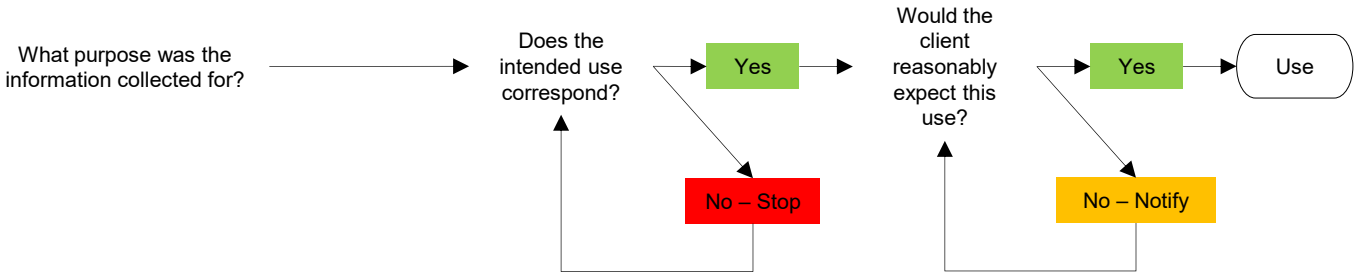
COLLECTION RULE

Do I need this information?



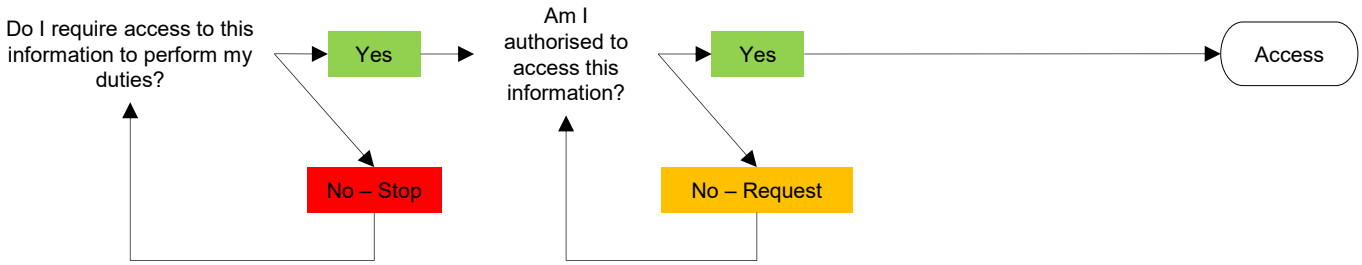
PURPOSE RULE

Why do I need this information?



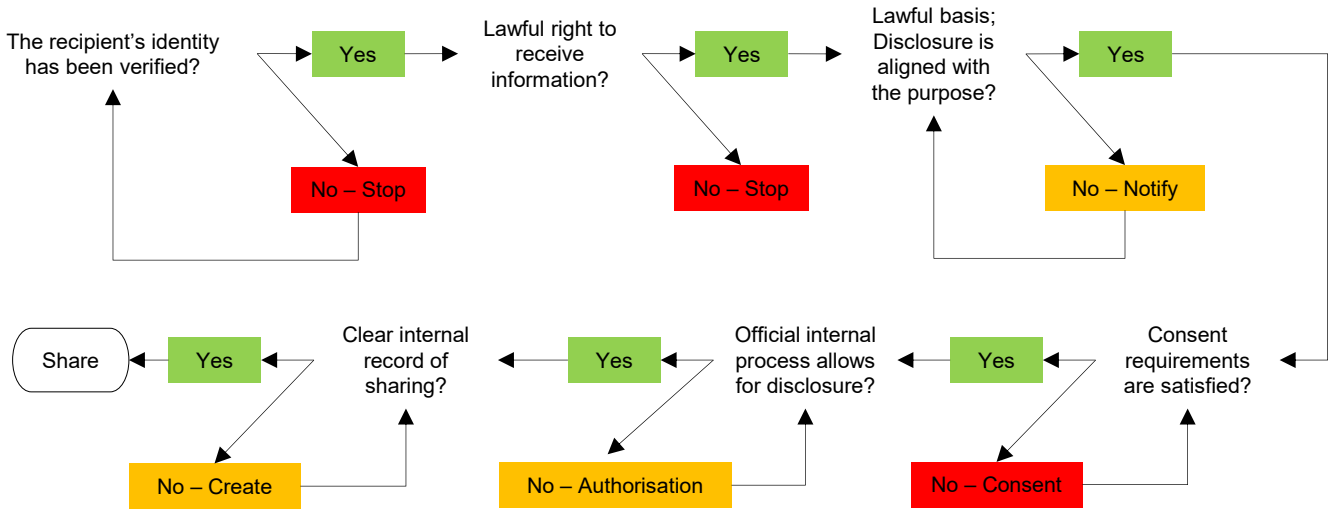
NEED-TO-KNOW RULE

Do I need access to this information?



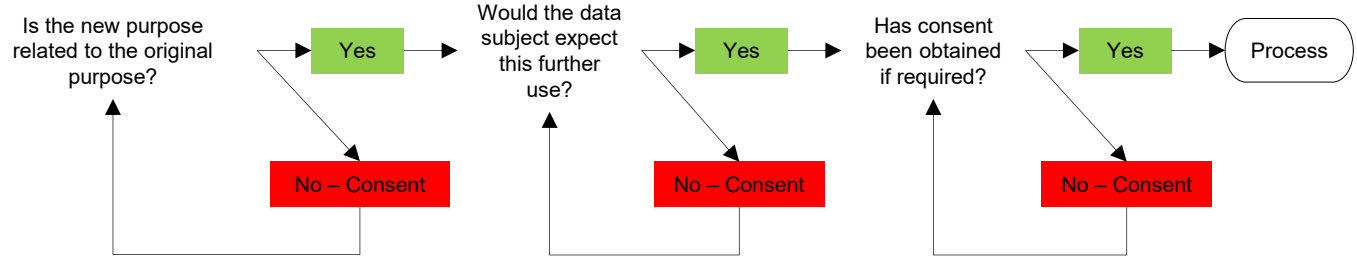
SHARING RULE

Should I disclose this information? (ALSO REFER TO THE CHECKLIST)



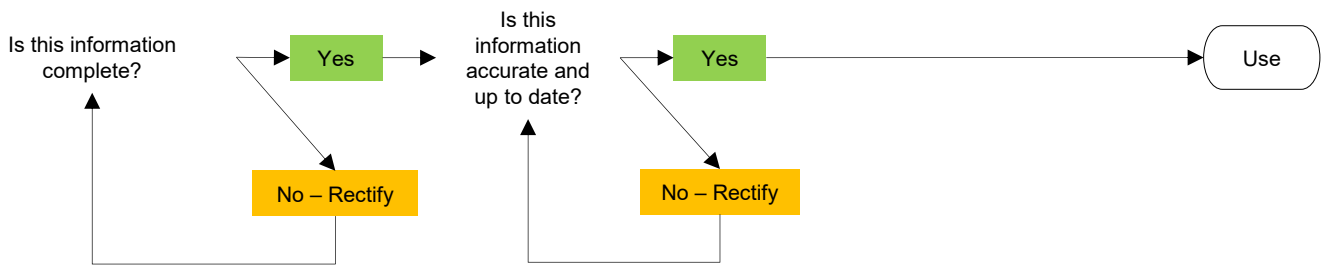
FURTHER PROCESSING RULE

Can I use this information for another purpose?



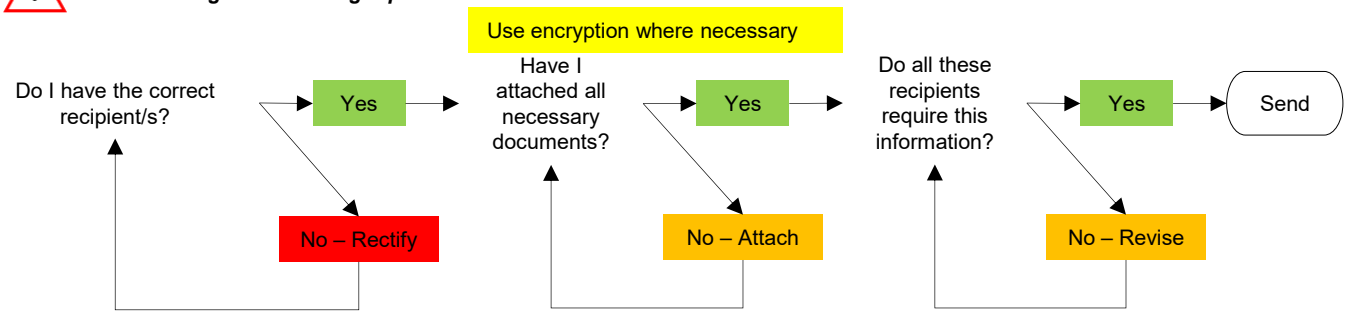
ACCURACY RULE

Can I rely on this information?



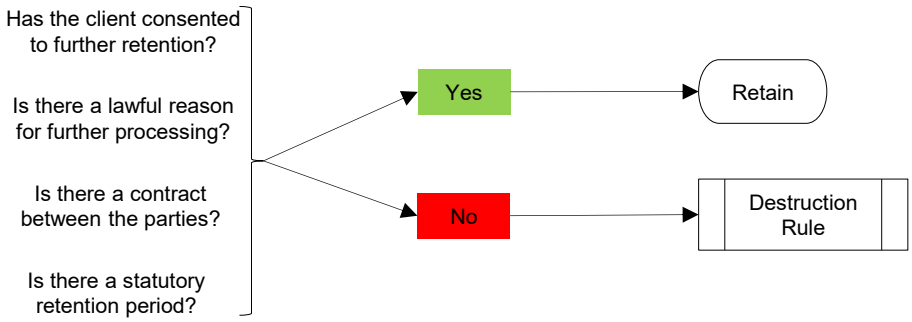
EMAIL RULE

Am I sending this to the right person?



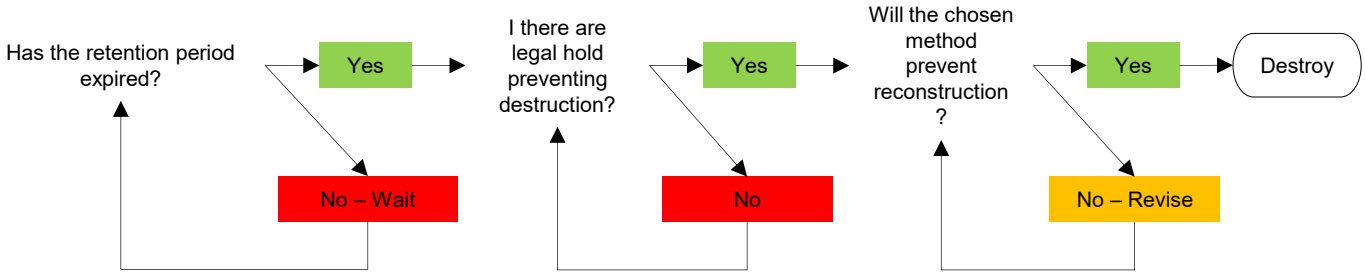
RETENTION RULE

Are we required to retain this information?



DESTRUCTION RULE

Can this information be destroyed?



Golden Rule: Before collecting, accessing, using, sharing, retaining, or destroying personal information, ask: "Is this necessary, authorised, secure and consistent with the purpose for which the information was obtained?" If the answer is uncertain, **stop and seek guidance from the Information Officer or Information Officer**.

POPIA affords data subjects various rights in relation to the processing of their personal information. In this section, the RP identifies those rights and explains the measures and procedures implemented to ensure that they are effectively recognised, facilitated and complied with.

1 The data subject has the right to be notified when personal information is collected or accessed by an unauthorised person.

In the event of a breach, the RP will promptly notify the Information Regulator and affected data subjects. Notifications will be issued in writing via mail, email, website, media, or as directed by the Information Regulator.

The notice will outline the nature of the breach, corrective actions taken, recommended protective measures, and, if known, the identity of the unauthorised party.

If necessary, the RP will publicly disclose the breach to ensure data subjects are informed and protected, always prioritising transparency and compliance with regulatory requirements.

2 The data subject has the right to establish whether the RP holds any personal information and to request access to it.

Any person, upon proving their identity, may request confirmation, free of charge, on whether the RP holds their personal information. They may also request access to that information, including details of third-party access, subject to a reasonable fee.

The RP will provide a fee estimate and may request a deposit prior to providing the information. If information is held by the RP, the data subject has the right to request correction of that information.

Access to information may be refused if valid grounds under the Promotion of Access to Information Act apply, but non-exempt information will still be disclosed.

3 The data subject has the right to request correction, deletion or destruction of personal information.

A data subject may request the correction or deletion of their personal information if it is inaccurate, outdated, irrelevant, or unlawfully obtained, or request its destruction if the RP is no longer authorised to retain it. Upon request, the RP will act promptly by correcting, deleting, or justifying the information, or noting the unresolved dispute.

If changes affect past or future decisions, affected third parties will be informed where practicable/ applicable. The RP will also notify you of the action taken in response to the request.

The above may be requested by completing and submitting **POPIA - form 2** to the Information Officer.

4 The data subject has the right to object to the processing of personal information on reasonable grounds (including for direct marketing purposes).

A data subject has the right to object to the processing of their personal information on reasonable grounds relating to their specific situation.

Once an objection is lodged, the RP will no longer process the information unless legislation permits it, or compelling legitimate grounds can be demonstrated that override the interests, rights, and freedoms of the data subject. 19/…

It must be understood that an objection to processing of certain information may result in the RP being unable to execute its mandate, which may result in termination of the mandate by the RP.

The above may be requested by completing and submitting **POPIA - form 1**, to the Information Officer.

5 The data subject has the right not to be subjected to decisions based solely on automated processing of personal information.

A data subject will not be subject to decisions with legal or significant effects based solely on automated processing, such as profiling for work performance, creditworthiness, or health. Exceptions apply if the decision is linked to a contract and protects the data subject's interests, or if governed by law or a code of conduct with safeguards.

In such cases, the RP will allow the data subject to make representations and provide enough information on the logic behind the automated decision to enable an informed response.

6 The data subject has the right to submit complaints to the Information Regulator.

A data subject may submit a written complaint to the Information Regulator, in the prescribed manner and form, if they believe their personal information has been interfered with or unlawfully processed.

Additionally, an RP or data subject may lodge a complaint if aggrieved by an adjudicator's decision under section 63(3). The Regulator must provide reasonable assistance to individuals who require help in submitting their complaint.

For more information on how to lodge a complaint with the Regulator, please visit their website on https://inforegulator.org.za/complaints/.

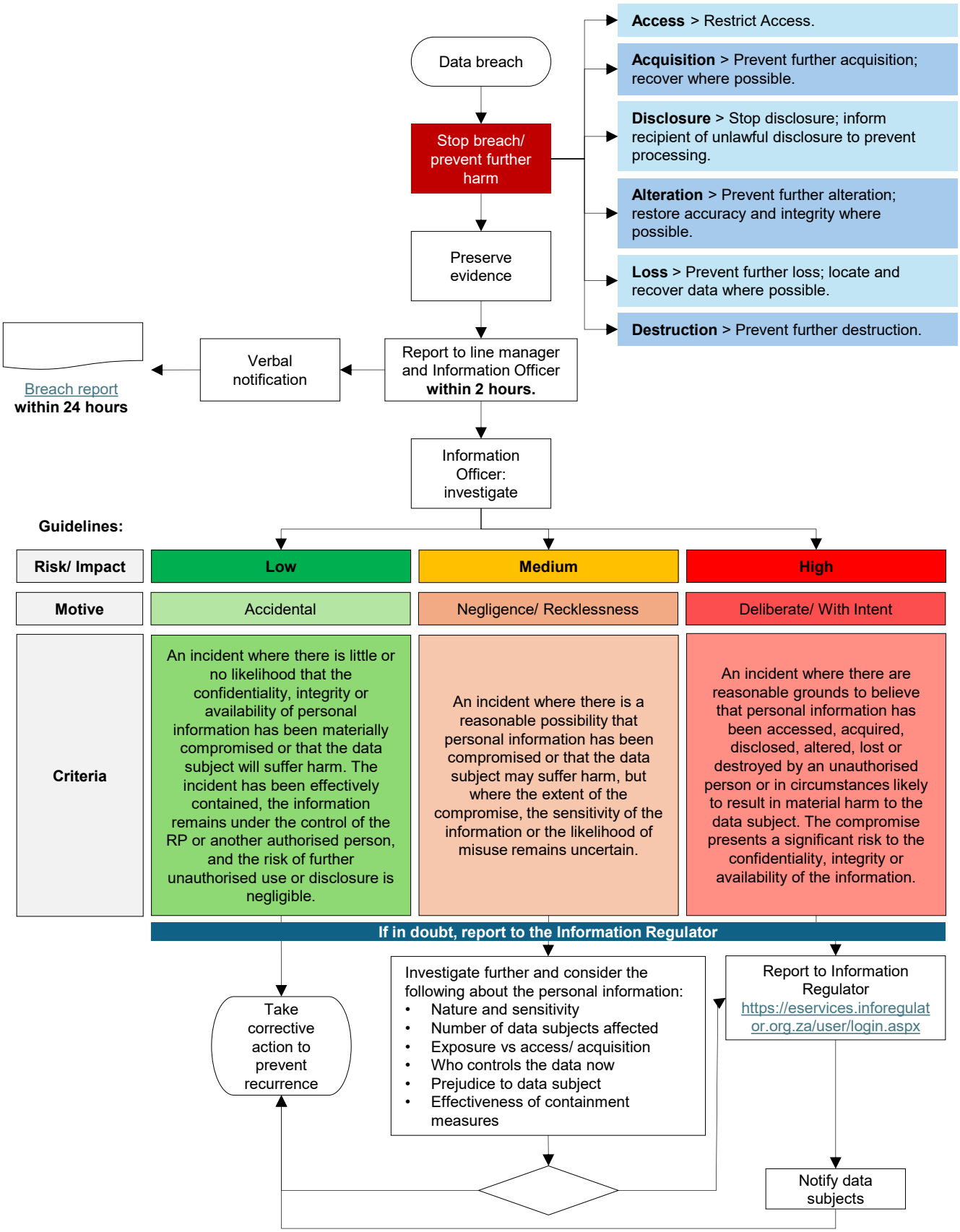
7 The data subject has the right to institute civil proceedings for interference with the protection of personal information.

A data subject, or the Information Regulator on their behalf, may institute civil action for damages against a responsible party for breach of POPIA, regardless of intent or negligence.

Defences include *vis major*, Plaintiff's consent or fault, impracticality, or exemption by the Information Regulator.

Courts may award compensation for patrimonial and non-patrimonial loss, aggravated damages, interest, and legal costs.

A data breach may involve electronic records, physical records or verbal disclosures and can result from human error, system failures, cyberattacks, theft or inadequate security measures. A data breach occurs when personal information is accessed, acquired, disclosed, altered, lost, or destroyed, either accidentally or unlawfully by an unauthorised person/s.





Practical Rule: POPIA does not require enterprise-grade cybersecurity for small law firms. The test under section 19 is whether the firm has taken appropriate, reasonable technical and organisational measures, having regard for the risks involved. The following basic security measures are used.

Access Control | Access is controlled as follows:

- [x] Role based access
- [x] Offices and physical storage areas not accessible by unauthorised persons (access-controlled doors/ areas)
- [ ] Filing room locked after hours
- [x] Clear desk policy

Backup Strategy | We use the following:

- [x] Manual backup eg: hard drive disk
- [x] Cloud based backup (eg: OneDrive)

Document Disposal | We use the following:

- [x] Cross-cut shredding
- [x] Electronic wiping
- [ ] Professional secure destruction services

Email Security | Minimum controls include:

- [x] Disclosure checklist
- [x] Password-protected documents where applicable
- [x] Passwords are sent separately

Artificial Intelligence | Anonymisation techniques:

- [x] Physical redaction before processing
- [x] Removal of personal information before processing
- [ ] We do not use artificial intelligence

Device Security | Every computer has:

- [x] Microsoft Defender or equivalent: Enabled
- [x] Automatic operating system updates: Enabled
- [x] Automatic software updates: Enabled
- [x] Screen lock after 3 minutes
- [x] Strong passwords: At least 8 characters including 1 upper case, 1 lower case, 1 number, and 1 special character.
- [x] Computers are password protected

Multi-Factor Authentication | MFA is enabled on:

- [x] Microsoft 365
- [ ] Cloud storage
- [ ] Practice management software

This section of the policy constitutes the RP's PAIA manual prepared in terms of section 51 of the **Promotion of Access to Information Act 2 of 2000**. If any person (natural or juristic) wishes to obtain records from the RP, the provisions of this manual applies and must be observed strictly. A free copy of this manual may be requested by sending an email to the Information Officer. This manual is available in **English** and may also be inspected at our offices during office hours. For PAIA guides in all other languages, visit https://inforegulator.org.za/paia-guidelines/

NATURE OF RECORDS HELD

The following categories of records are held by the RP and **may be requested without having to submit a formal request** in terms of this manual:

Category of Record	Types of Records	Website	Available on Email Request
Policy document	POPIA Policy		X
Policy document	PAIA Manual		X
Internal documents	Client engagement forms		X

The following categories of records are held by the RP in terms of legislation. **Kindly note**: The inclusion of any type of record should not be taken to mean that records failing within that category will be automatically be made available under PAIA as it may be subject to legitimate grounds of refusal.

Applicable Legislation	Types of Records
Companies Act 71 of 2008	• Memorandum of Incorporation (MOI) & amendments, other incorporation documents. • Notices, agendas and minutes of committee meetings, written resolutions. • All accounting records and annual financial statements, audit reports.
Basic Conditions of Employment Act 75 of 1997	• For each employee: name/occupation, hours worked, remuneration & deductions, leave, written particulars of employment, and any other prescribed information.
Employment Equity Act 55 of 1998	• Workforce profiles & analysis, barriers/remedial measures, minutes of consultations, Employment Equity Plan (EEP), implementation proof, annual EEA2 reports, EEA4 income differentials statement, evidence of communication/training.
Financial Intelligence Centre Act 38 of 2001	• Client due-diligence (KYC) records: identities, addresses, legal status, beneficial ownership, source of funds, ongoing due-diligence/monitoring. • Transaction records: nature, amount, parties, accounts, dates, identifying numbers; RMCP; STR/CTR/TPrR submissions & internal reports; training & compliance audit records.
Income Tax Act 58 of 1962	• All tax returns and supporting documents (company ITR14s, EMP201/501 schedules, PAYE/UIF/SDL workings, VAT invoices/bills of entry, ledgers, contracts, bank statements).
Labour Relations Act 66 of 1995	• Employment contracts/variations, disciplinary/grievance records, CCMA/Labour Court awards/settlements.

NATURE OF RECORDS HELD (continued)

Applicable Legislation	Types of Records
Legal Practice Act 28 of 2014	• Trust accounting & business accounting records: client/trust ledgers, bank statements, EFT proofs, fee notes, invoices, deposit slips, journals, reconciliations; Fee/Trust transfer authorities; cost estimates; engagement letters and FICA/KYC files.
Occupational Health and Safety Act 85 of 1993	• Risk assessments, H&S policy, training registers, incident/accident records, H&S committee minutes/recommendations.
Prevention and Combating of Corrupt Activities Act 12 of 2004	• Section 34 report copies/affidavits, internal investigation files, whistleblowing reports and related correspondence
Promotion of Access to Information Act 2 of 2000	• Section 51 PAIA Manual (current, published & available). • Records of PAIA requests (Form 2), fees/deposits, decision letters, third-party notifications/representations, and any disclosures made under PAIA.
Protection of Personal Information Act 4 of 2013	• Policies (privacy, security, data subject rights), PAIA/POPIA manual, operator agreements, consent/objection/withdrawal records, PAIA/POPIA request logs, breach logs & Regulator notifications, PIA/impact assessments, operator due-diligence.
Skills Development Levies Act 97 of 1998	• Register per employee of remuneration paid, employees' tax deducted/withheld, SDL deducted, UIF contributions, and the employee's income tax reference number. • EMP201s/EMP501s, proof of SDL payments, SETA classification details, and supporting payroll workings.
Unemployment Insurance Act 63 of 2001	• Register per employee showing remuneration paid and the UIF contribution deducted/paid; including personal particulars, financial details and the employee's income tax reference number. • EMP201s, EMP501s, proof of payments, payroll journals, and any supporting workings linking payroll to declarations. • UI-19 declarations/submissions (and proof of submission) made to the UI Commissioner.

NATURE OF RECORDS HELD (continued)

The following categories of records are held by the RP in terms of specific data subjects. **Kindly note**: The inclusion of any type of record should not be taken to mean that records failing within that category will be automatically be made available under PAIA as it may be subject to legitimate grounds of refusal.

Applicable Legislation	Types of Records
Employee records (including those of practice members)	• General personal information; • Records provided by a third party relating to personnel, example copy of identification document; • Conditions of employment and other employee related contractual and quasi-legal records; • Correspondence relating to employees; and • Training schedules and material.
Client related records	• Incorporation documents and related information; • Records pertaining to the legal matters of the clients/ members/ beneficiaries of the company; • Records provided by a client/ member/ beneficiary to a third party acting for or on behalf of the company; • Records provided by a third party; and • Records generated by or within the company relating to its clients/ members/ beneficiaries.
Supplier related records	• Supplier onboarding documents; and • Purchase orders, credit notes, remittance advices, invoices, delivery notes, statements of account, and other related documents.
The RP	• Internal policies and procedures; financial records; operational records; service records; communications; information management and technology; administrative records; statutory records; insurance; supplier information and agreement; and marketing and branding.

RECIPIENTS OF RECORDS HELD BY RP

Depending on the nature of the data, the RP may supply information or records to the following categories of recipients, subject to compliance with POPIA:

- Statutory oversight bodies, regulators or judicial commissions of enquiry making a request for data;
- Any court, administrative or judicial forum, arbitration, statutory commission, or ombudsman making a request for data or discovery in terms of the applicable rules;
- The Competition Commission in terms of the Competition Act No. 89 of 1998;
- South African Revenue Services, or another similar authority;
- Anyone making a successful application for access in terms of PAIA; and
- Subject to a legitimate interest, a person who conducts business with the RP.

REQUESTERS OF RECORDS HELD BY RP

Records held by the RP may be accessed by a requester only once the prerequisite requirements for access have been met.

A requester is any person requesting access to a record of or held by the RP, including a:

- Personal requester seeking access to a record containing personal information about the requester. The RP will voluntarily provide the requested information or give access to any record with regard to the requester's personal information. A prescribed fee for the reproduction of the information requested may be charged.

- Other requesters requested access to information on behalf of third parties. The RP is not obliged to grant access voluntarily. The requester must fulfil the prerequisite requirements for access in terms of the Act, including the payment of a request and access fee.

REMEDIES FOR REFUSAL BY RP

The RP does not have any internal appeal procedures at the disposal of a requester whose request was declined, or where the Information Officer has failed to respond to the request.

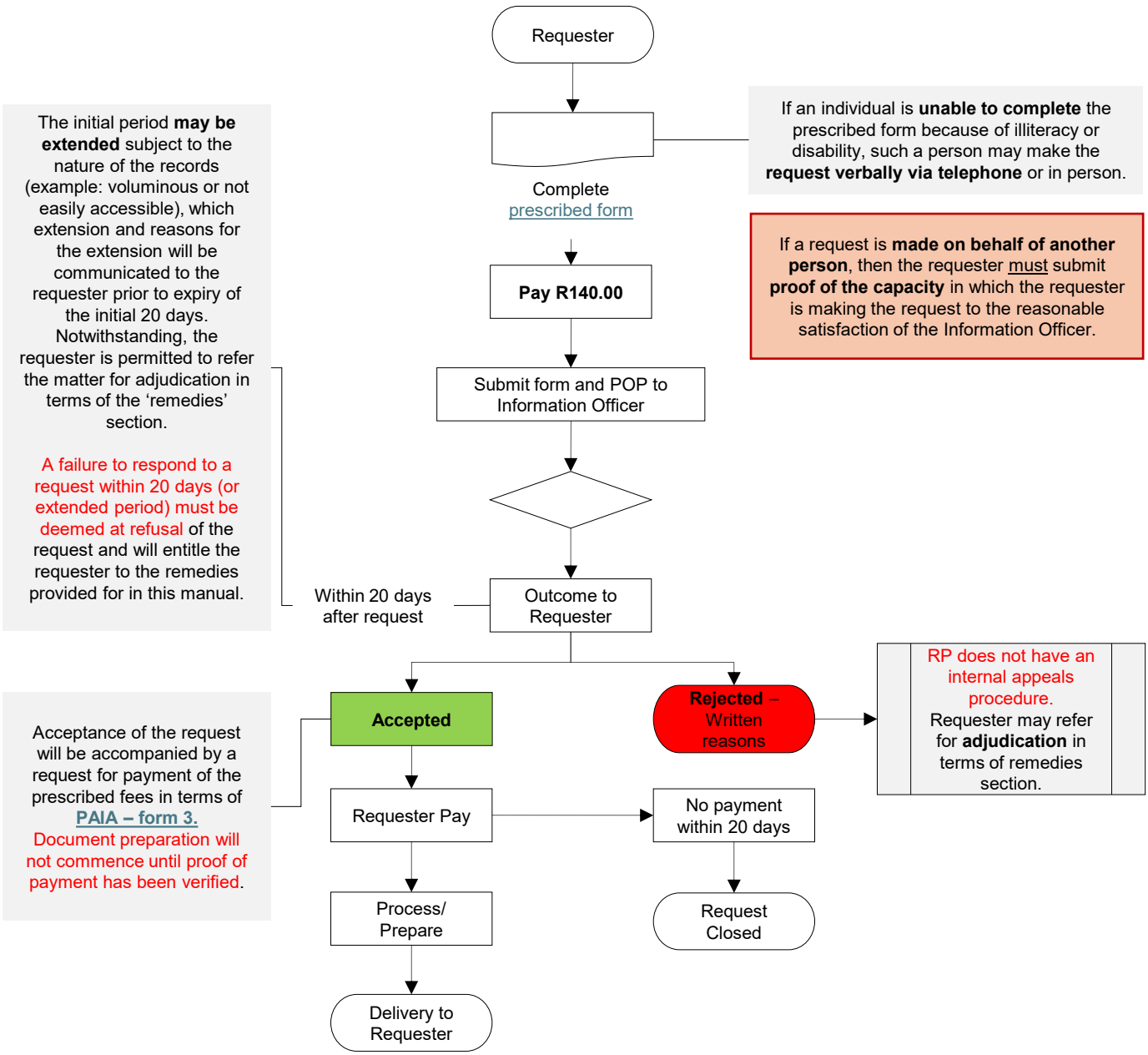
A dissatisfied requester may seek recourse as follows:

- **Lodging a complaint** with the Information Regulator **within 180 days** of the date on which the decision (or failure to take a decision) was made by completing **form 5** (available online). The complaints procedure and applicable forms can be accessed at https://inforegulator.org.za/complaints/.

- Apply to court (magistrate's or high court) in terms of section 82 of PAIA (subject to first lodging a complaint with the regulator).

The relief that may be granted by the regulator or a court is set out in the Act.

REQUESTING PROCEDURE



If an individual is **unable to complete** the prescribed form because of illiteracy or disability, such a person may make the **request verbally via telephone** or in person.

If a request is **made on behalf of another person**, then the requester must submit **proof of the capacity** in which the requester is making the request to the reasonable satisfaction of the Information Officer.

The initial period **may be extended** subject to the nature of the records (example: voluminous or not easily accessible), which extension and reasons for the extension will be communicated to the requester prior to expiry of the initial 20 days. Notwithstanding, the requester is permitted to refer the matter for adjudication in terms of the 'remedies' section.

A failure to respond to a request within 20 days (or extended period) must be deemed at refusal of the request and will entitle the requester to the remedies provided for in this manual.

Acceptance of the request will be accompanied by a request for payment of the prescribed fees in terms of **PAIA – form 3.** Document preparation will not commence until proof of payment has been verified.

RP does not have an internal appeals procedure. Requester may refer for **adjudication** in terms of remedies section.

MANDATORY GROUNDS FOR REFUSAL:

- Mandatory protection of privacy of third party who is a natural person, if the disclosure amounts to an unreasonable disclosure.
- Mandatory protection of commercial information of a third party, such as trade secrets, or any other information that will threaten the third party's commercial interests.
- Mandatory protection of certain confidential information, and protection of certain other confidential information, of a third party where disclosure would result in a breach of duty of confidence.
- Mandatory protection of safety of individuals, and protection of property where the disclosure of information could compromise the safety of and individual or the security of a building or property.
- Mandatory protection of records privileged from production in legal proceedings, unless legal privilege was waived.
- Mandatory protection of research information of third party, and protection of research information of public or private body where disclosure would expose the researcher, a third party, or place the research subject at serious disadvantage.
- Requests for information that are clearly frivolous or vexatious or which involve an unreasonable diversion of resources will be refused.

POPIA FORM 1: OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION

Kindly Note: Where applicable, you may attach documentary evidence/ affidavit/s in support of your objection. If any space provided in this form is inadequate, please submit a signed annexure/s with the relevant information together with this form.

DATA SUBJECT DETAILS

Full Names/ Registered Name	
Identity/ Registration Number	
Physical Address	
Contact Number and Email Address	

RESPONSIBLE PARTY DETAILS

Full Names/ Registered Name	
Identity/ Registration Number	
Physical Address	
Contact Number and Email Address	

REASONS FOR OBJECTION

Please provide detailed reasons for the objection. Attach additional pages where necessary.	

Date: _____ Signature: _____

POPIA FORM 2: REQUEST FOR CORRECTION, DELETION OR DESTRUCTION OF A RECORD OR PERSONAL INFORMATION

Kindly Note: Where applicable, you may attach documentary evidence/ affidavit/s in support of your objection. If any space provided in this form is inadequate, please submit a signed annexure/s with the relevant information together with this form.

Mark with "X"

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

DATA SUBJECT DETAILS

Full Names/ Registered Name	
Identity/ Registration Number	
Physical Address	
Contact Number and Email Address	

RESPONSIBLE PARTY DETAILS

Full Names/ Registered Name	
Identity/ Registration Number	
Physical Address	
Contact Number and Email Address	

INFORMATION TO BE CORRECTED, DELETED, OR DESTROYED

Please provide details about the information. Attach additional pages where necessary.	

REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24 (1) (a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24 (1) (b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN.

Please provide detailed reasons. Attach additional pages where necessary.	

Date: Signature:

Kindly Note: Proof of identity must be submitted with the request form. If a request is made on behalf of another person, proof of authorisation must also be submitted with the request form. If any space provided in this form is inadequate, please submit a signed annexure/s with the relevant information together with this form.

To the Information Officer | Entity Name

Name:

Email Address:

REQUESTER DETAILS

Mark with "X"

☐ The request is made in my own name.

☐ The request is made on behalf of another person.

Full Names/ Registered Name	
Identity/ Registration Number	
Physical Address	
Contact Number and Email Address	

Complete the following section if the request is made in a representative capacity. If the requester and data subject is the same, leave blank.

DATA SUBJECT DETAILS

In what capacity are you requesting?	
Full Names/ Registered Name	
Identity/ Registration Number	
Physical Address	
Contact Number and Email Address	

PARTICULARS OF RECORD/S REQUESTED

Provide **full particulars of the record** to which access is requested, including the reference number if that is known to you, to enable the record to be located. (If the provided space is inadequate, please continue a separate page and attach it to this form. **All additional pages must be signed**.)

Record Type. Mark with "X"

- ☐ Written form
- ☐ Printed form
- ☐ Record comprises virtual images (this includes photographs, slides, video recordings, computer-generated images, sketches, etc).
- ☐ Record consists of recorded words or information which can be reproduced in sound.
- ☐ Record is held on a computer or in an electronic, or machine-readable form.

Form of Access Required. Mark with "X"

- ☐ Printed copy of record (including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form).
- ☐ Written or printed transcription of virtual images (this includes photographs, slides, video recordings, computer-generated images, sketches, etc).
- ☐ Transcription of soundtrack (written or printed document).
- ☐ Copy of record on flash drive (including virtual images and soundtracks).
- ☐ Copy of record saved on cloud storage server.

Manner of Access Required. Mark with "X"

- ☐ Personal inspection of record at registered address of RP (including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form).
- ☐ Collection from RP address.
- ☐ Courier delivery to requester address.
- ☐ Email delivery, if possible.
- ☐ Cloud share/ file transfer.

Preferred Language	

Kindly note: If the record is not available in the language you prefer, access may only be granted in the language in which the record is available.

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED

Indicate which right is to be exercised or protected. Attach additional pages where necessary.	

Explain why the record requested is required for the exercise or protection of the aforementioned right:. Attach additional pages where necessary.	

FEES

A request fee of **R140.00** is payable before the request will be considered. *If you qualify for exemption of the payment of any fee, please state the reason for exemption*

Kindly note: You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence.

Mark with "X"

☐ Postal Address

☐ Email

☐ Other, please specify _____

Date: _____ Signature: _____

FOR OFFICE USE ONLY

Reference Number	
Request Received By	
Date Received	
Request Fee Paid	

Date: _____ Signature: _____

PAIA FORM 3: OUTCOME OF REQUEST AND FEES PAYABLE REGULATION 8

Kindly Note: If your request is granted the fees are payable before your request will be processed. Records will only be released once proof of full payment is received. Please use the below reference number in all future correspondence.

Reference Number	

REQUESTER DETAILS

Full Names/ Registered Name	
Identity/ Registration Number	
Physical Address	
Contact Number and Email Address	
Date of Request	

Dear Requester,

We refer to the records/ information your requested in form 2, which is attached hereto for ease of reference. You are hereby informed that your request is:

☐ Approved, the following fees are due and payable before the records/ information are released.

Item	Description	Fee per Unit	Units	Total Amount
1	Photocopy/ print (black & white) per A4 page or part thereof	R2.00		
2	For a copy in a computer-readable format on a USB Drive (to be provided by requester)	R40.00		
3	For a transcription of visual images per A4 page (outsourced – per quotation)			
4	Copy of visual images (outsourced – per quotation)			
5	For a transcription of an audio record per A4 page	R24.00		
6	For a copy of an audio record on a USB drive (to be provided by requestor)	R40.00		
7	To search for and prepare the record for disclosure for each hour or party of an hour, excluding the first hour, reasonably required for such search and preparation, not exceeding R435.00.	R145.00		
8	Postage, email or any other electronic transfer (at cost)			
			Total Payable	

Kindly refer to the attached pro-forma invoice for further payment details.

☐ Rejected, please see the details below.

The RP does not have any internal appeal procedures at the disposal of a requester whose request was declined, or where the Information Officer has failed to respond to the request.

A dissatisfied requester may seek recourse as follows:

- **Lodging a complaint** with the Information Regulator **within 180 days** of the date on which the decision (or failure to take a decision) was made by completing **form 5** (available online). The complaints procedure and applicable forms can be accessed at https://inforegulator.org.za/complaints/.

- Apply to court (magistrate's or high court) in terms of section 82 of PAIA (subject to first lodging a complaint with the regulator).

The relief that may be granted by the regulator or a court is set out in the Act.

Date: Signature:

INTERNAL DATA BREACH REPORT

IMPORTANT: This report must be completed and submitted to the Information Officer within **24 Hours** from the date of data breach.

REPORTER DETAILS

Full Names	
Position/ Department	
Contact Number and Email Address	

INCIDENT DETAILS

Date and Time incident was discovered	

What is the nature of the incident?

☐ Unauthorised access ☐ Acquisition ☐ Unauthorised disclosure ☐ Alteration

☐ Loss ☐ Destruction ☐ Other: _____

Provide a **factual description** of what occurred and how the incident was identified. Attach additional pages where necessary.

What **type of personal information** is affected? Attach additional pages where necessary.

Number of records affected (if known)	
Number of data subjects affected (if known)	
Who are the **parties involved**, and in what way? Attach additional pages where necessary.	

What **immediate steps** were taken to contain the incident. Attach additional pages where necessary.

The incident is:

☐ Ongoing ☐ Contained

Date and Time: Signature: