ATTORNEYS | NOTARIES | CONVEYANCERS

PAIA MANUAL

Prepared in terms of section 51 of the Promotion of Access to Information Act 2 of 2000 (as amended)

DATE OF COMPILATION: 01/11/2023
DATE OF REVISION: 22/09/2025

1. LIST OF ACRONYMS AND ABBREVIATIONS

1.1	**"IO"**	Information Officer;
1.2	**"Minister"**	Minister of Justice and Correctional Services;
1.3	**"PAIA"**	Promotion of Access to Information Act No. 2 of 2000 (as Amended);
1.4	**"POPIA"**	Protection of Personal Information Act No.4 of 2013;
1.5	**"Regulator"**	Information Regulator; and
1.6	**"Republic"**	Republic of South Africa

2. INTRODUCTION

This manual is prepared in accordance with the provisions of the *Promotion of Access to Information* Act (Act No. 2 of 2000) and sets out the procedures and guidelines for requesting access to information held by NVZA Incorporated Attorneys. The Act promotes transparency, accountability, and access to information within the organisation.

3. THE ACT

The *Promotion of Access to Information* Act, No. 2 of 2000 ("The Act") was enacted on 3 February 2000, giving effect to the right of access to any information held by the Government, as well as any information held by another person who is required for the exercising or protection of any rights. This right is entrenched in the Bill of Rights in the *Constitution of South Africa*. Where a request is made in terms of the Act, the body to which the request is made is not obligated to release information, except where the Act expressly provides that the information may be released. The Act sets out the requisite procedural issues attached to such a request.

4. PURPOSE OF PAIA MANUAL

In order to promote effective governance of private bodies, it is necessary to ensure that everyone is empowered and educated to understand their rights in terms of the Act, in order for them to exercise their rights in relation to public and private bodies.

Section 9 of the Act, however, recognises that such a right to access to information cannot be unlimited and should be subject to justifiable limitations, including but not limited to:

- Limitations aimed at the reasonable protection of privacy;
- Commercial confidentiality; and
- Effective, efficient, and good governance.

And in a manner that balances that right with any other rights, including such rights contained in the Bill of Rights in the Constitution.

Wherever reference is made to “Private Body” in this manual, it will refer to NVZA Incorporated Attorneys.

This PAIA Manual is useful for the public to-

4.1 check the categories of records held by a body which are available without a person having to submit a formal PAIA request;

4.2 have a sufficient understanding of how to make a request for access to a record of the body, by providing a description of the subjects on which the body holds records and the categories of records held on each subject;

4.3 know the description of the records of the body which are available in accordance with any other legislation;

4.4 access all the relevant contact details of the Information Officer and Deputy Information Officer who will assist the public with the records they intend to access;

4.5 know the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;

4.6 know if the body will process personal information, the purpose of processing of personal information and the description of the categories of data subjects and of the information or categories of information relating thereto;

4.7 know the description of the categories of data subjects and of the information or categories of information relating thereto;

4.8 know the recipients or categories of recipients to whom the personal information may be supplied;

4.9 know if the body has planned to transfer or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied; and

4.10 know whether the body has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

5. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF NVZA INCORPORATED ATTORNEYS

5.1. **Chief Information Officer**

Name: Nadia Reyneke

Email: nadiar@nvza.co.za

5.2 **Access to information: general contacts**

Email: admin@nvza.co.za

5.3 **National or Head Office**

Physical Address: 544 Lois Avenue, Erasmuskloof, Pretoria, Gauteng Province, 0048

Telephone: 012 347 1089

Email: admin@nvza.co.za
Website: https://nvza.co.za/

6. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

6.1. The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made available the revised Guide on how to use PAIA ("Guide"), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

6.2. The Guide is available in each of the official languages and in braille.

6.3. The aforesaid Guide contains the description of-

6.3.1. the objects of PAIA and POPIA;

6.3.2. the postal and street address, phone and fax number and, if available, electronic mail address of-

6.3.2.1. the Information Officer of every public body, and

6.3.2.2. every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA[1] and section 56 of POPIA[2];

6.3.3. the manner and form of a request for-

[1] Section 17(1) of PAIA- *For the purposes of PAIA, each public body must, subject to legislation governing the employment of personnel of the public body concerned, designate such number of persons as deputy information officers as are necessary to render the public body as accessible as reasonably possible for requesters of its records.*

[2] *Section 56(a) of POPIA- Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of POPIA.*

6.3.3.1. access to a record of a public body contemplated in section 11[3]; and

6.3.3.2. access to a record of a private body contemplated in section 50[4];

6.3.4. the assistance available from the IO of a public body in terms of PAIA and POPIA;

6.3.5. the assistance available from the Regulator in terms of PAIA and POPIA;

6.3.6. all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging-

6.3.6.1. an internal appeal;

6.3.6.2. a complaint to the Regulator; and

6.3.6.3. an application with a court against a decision by the information officer of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body;

[3] *Section 11(1) of PAIA- A requester must be given access to a record of a public body if that requester complies with all the procedural requirements in PAIA relating to a request for access to that record; and access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.*

[4] *Section 50(1) of PAIA- A requester must be given access to any record of a private body if-*

a) that record is required for the exercise or protection of any rights;
b) that person complies with the procedural requirements in PAIA relating to a request for access to that record; and
c) access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

6.3.7. the provisions of sections 14[5] and 51[6] requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;

6.3.8. the provisions of sections 15[7] and 52[8] providing for the voluntary disclosure of categories of records by a public body and private body, respectively;

6.3.9. the notices issued in terms of sections 22[9] and 54[10] regarding fees to be paid in relation to requests for access; and

6.3.10. the regulations made in terms of section 92[11].

6.4. Members of the public can inspect or make copies of the Guide from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.

6.5. The Guide can also be obtained-

6.5.1. upon request to the Information Officer;

---

[5] *Section 14(1) of PAIA- The information officer of a public body must, in at least three official languages, make available a manual containing information listed in paragraph 4 above.*

[6] *Section 51(1) of PAIA- The head of a private body must make available a manual containing the description of the information listed in paragraph 4 above.*

[7] *Section 15(1) of PAIA- The information officer of a public body, must make available in the prescribed manner a description of the categories of records of the public body that are automatically available without a person having to request access*

[8] *Section 52(1) of PAIA- The head of a private body may, on a voluntary basis, make available in the prescribed manner a description of the categories of records of the private body that are automatically available without a person having to request access*

[9] *Section 22(1) of PAIA- The information officer of a public body to whom a request for access is made, must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.*

[10] *Section 54(1) of PAIA- The head of a private body to whom a request for access is made must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.*

[11] *Section 92(1) of PAIA provides that –"The Minister may, by notice in the Gazette, make regulations regarding-*
(a) any matter which is required or permitted by this Act to be prescribed;
(b) any matter relating to the fees contemplated in sections 22 and 54;
(c) any notice required by this Act;
(d) uniform criteria to be applied by the information officer of a public body when deciding which categories of records are to be made available in terms of section 15; and
(e) any administrative or procedural matter necessary to give effect to the provisions of this Act."

6.5.2. from the website of the Regulator (https://inforegulator.org.za).

6.6 A copy of the Guide is also available in the following two official languages, for public inspection during normal office hours-

6.6.1 Afrikaans

6.6.2 English

7. CATEGORIES OF RECORDS OF NVZA INCORPORATED ATTORNEYS WHICH ARE AVAILABLE WITHOUT A PERSON HAVING TO REQUEST ACCESS

No records of NVZA Incorporated Attorneys shall automatically be available to the public, all requests pertaining to records shall be made in accordance with a formal request.

8. RECORDS OF NVZA INCORPORATED ATTORNEYS WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION

Companies Act 71 of 2008

Promotion of Access to Information Act 2 of 2000

Labour Relations Act 66 of 1995 – Basic Conditions of Employment Act 75 of 1997

Electronic Communications and Transactions Act, 36 of 2005

Compensation for Occupational Injuries and Diseases Act 130 of 1993

Constitution of the Republic of South Africa 108 of 1996

Unemployment Insurance Act 63 of 2001

Income Tax Act, 58 of 1962

Protection of Personal Information Act 4 of 2013

Legal Practice Act 28 of 2014

Employment Equity Act 55 of 1998

National Credit Act 34 of 2005

Consumer Protection Act 68 of 2008

Financial Intelligence Act 38 of 2001

Prescription Act 68 of 1969

9. DESCRIPTION OF THE SUBJECTS ON WHICH THE BODY HOLDS RECORDS AND CATEGORIES OF RECORDS HELD ON EACH SUBJECT BY NVZA INCORPORATED ATTORNEYS

Subjects on which the body holds records	Categories of records
General records	- Financial and accounting records - Insurance records - Client, supplier and document databases - Law Society records, including Fidelity Fund Certificate. - Internal and External correspondence - Tax compliance documents - Bank Statements - Invoices
Employees	- Employment contracts - Disciplinary records - Salaries and wages records - Disciplinary code - Leave records - PAYE records - Income tax documents - Payments made to SARS on behalf of employees - UIF
Third-party services	- Mandates - Fee Structures - Contact information - Records provided by the third-party - Invoices - Records generated by NVZA Incorporated Attorneys

Subjects on which the body holds records	Categories of records
	- Compliance documents
Clients	- FICA documents - Records provided by a client to a third party - Records provided by third parties - Records generated by NVZA Incorporated Attorneys - Client files - Invoices - Fee agreements, quotations and mandates

The above information may only be made available subject to the provisions of the Act and access to records may be refused due to attorney-client privilege.

10. PROCESSING OF PERSONAL INFORMATION

10.1 Purpose of Processing Personal Information

We only process personal information for: -

- Employees – Employment contracts, Payroll, SARS, Department of Labour, UIF/WCC, etc.;
- Third party service – Use of consultation services;
- Clients – Executing mandate in line with our clear instructions.

10.2 Description of the categories of Data Subjects and of the information or categories of information relating thereto

Categories of Data Subjects	Personal Information that may be processed
Clients	• name and surname, • nationality / citizenship, • home and work address,

Categories of Data Subjects	Personal Information that may be processed
	• registration numbers or identity numbers, • employment status, • marital status, • SARS number, • banking details, • financial records, and • contact information.
Employees	• name and surname, • nationality / citizenship, • home address, • identity number, • bank details, • marital status, • qualifications, • gender and • race
Third-party Services	• identity / registration number, • work / home address, • bank details, • gender, • name and surname, • contact number, • email address, • marital status, • qualifications.

10.3 **The recipients or categories of recipients to whom the personal information may be supplied**

Category of personal information	Recipients or Categories of Recipients to whom the personal information may be supplied
Identity and registration number, addresses, contact information, marital status, gender, race, citizenship, nationality, and names	Organisations and software used to compile, verify, and confirm personal information in line and with the consent of our mandate.
Qualifications, for qualification verifications	South African Qualifications Authority
Credit and payment history, for credit information	Credit Bureaus

10.4 **Planned transborder flows of personal information**

None.

10.5 **General description of Information Security Measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information**

10.5.1 Company POPI Information security policies are in place;

10.5.2 Anti-virus on all computers which are regularly used;

10.5.3 Staff awareness of physical and cyber security measures;

10.5.4 Regular audits are done on the security status;

10.5.5 POPI Training done with staff.

11. AVAILABILITY OF THE MANUAL

11.1 A copy of the Manual is available-

11.1.1 the office of NVZA Incorporated Attorneys for public inspection during normal business hours;

11.1.2 to any person upon request and upon the payment of a reasonable prescribed fee;

11.1.3 website of NVZA Incorporated Attorneys; and

11.1.4 to the Information Regulator upon request.

11.2 A fee for a copy of the Manual, as contemplated in annexure B of the Regulations, shall be payable per each A4-size photocopy made.

12. REQUEST PROCEDURE FOR OBTAINING INFORMATION

Records held by the Private Body may be accessed by request only once the prerequisites for access have been met.

The requester must fulfil the prerequisite for access in terms of the Act, including the payment of the requested access fee.

The requester must complete the prescribed Form and submit same, as well as payment of a request fee and a deposit, if applicable, to the office's physical address or electronic mail address as stated herein.

The prescribed form must be filled in with enough particulars to at least enable the offices to identify;

- The record or records requested;
- The identity of the requester;
- Which form of access is required, if the request is granted;
- The postal address or email address of the requester.

The requester must state that he/she requires the information in order to exercise or protect a right, and clearly state what the nature of the right to be exercised or protected is. In addition, the requester must clearly specify why the record is necessary to exercise or protect such a right.

The Private Body will process the request within 30 days unless the requester has stated a special reason that would satisfy the Information Officer that circumstances dictate that the above time periods are not complied with.

The requester shall be informed whether access has been granted or denied. If, in addition, the requester requires the reason for the decision in any other manner, he/she must state the manner and the particulars so required.

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

If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally.

The requester must pay the prescribed fee before any further processing can take place.

13. FEES

When the office receives the request, such official shall by notice require the requester to pay the prescribed request fee before any further processing of the request takes place.

If the search for the record has been made in the preparation of the record for disclosure, including arrangements to make it available in the requested form, and it requires more than the hours prescribed in the regulation for this purpose, the office official shall notify the requester to pay as a deposit the prescribed portion of the access fee which would be payable if the request is granted.

The office official shall withhold a record until the requester has paid the Fees as indicated.

A requester, whose request for access to a record has been granted, must pay an access fee for reproduction and for the search and preparation, and for any time reasonably required in excess of the prescribed hours to search for and prepare the record for disclosure, including making arrangements to make it available in the requested form.

If a deposit has been paid in respect of a request for access, which is refused, then the Information Offices concerned must repay the deposit to the requester.

14. GROUNDS FOR REFUSAL OF ACCESS TO INFORMATION

The main reason for the Private Body to refuse a request for information relates to the:

14.1 Mandatory protection of the privacy of a third party that is a natural person, that would involve the unreasonable disclosure of personal information of that natural person;[12]

14.2 Mandatory protection of the commercial information of a third party, if the record contains:[13]

14.2.1 Trade secrets of that third party;

14.2.2 Financial, commercial, scientific, or technical information, disclosure of which could likely cause harm to the financial or commercial interests of that third party;

14.2.3 Information disclosed in confidence by a third party to the Private Body, if the disclosure could put that third party at a disadvantage in negotiations or commercial competition.

14.3 Mandatory protection of confidential information of third parties if it is protected in terms of any agreement;[14]

14.4 Mandatory protection of confidential information of the protection of property;[15]

14.5 Mandatory protection of records that would be regarded as privileged in legal proceedings;[16]

14.6 The commercial activities of the Private Body, which may include:[17]

14.6.1 Trade secrets of the Private Body;

14.6.2 Financial, commercial, scientific, or technical information, disclosure, which could likely cause to the financial or commercial interest of the Private Body;

14.6.3 Information which, if disclosed could put the Private Body at a disadvantage in negotiations or commercial competition;

14.6.4 A computer program, owned by the Private Body, and protected by copyright.

[12] Section 63 of the *Promotion of Access to Information Act* 2 of 2000.
[13] Section 64 of the *Promotion of Access to Information Act* 2 of 2000.
[14] Section 65 of the *Promotion of Access to Information Act* 2 of 2000.
[15] Section 66 of the *Promotion of Access to Information Act* 2 of 2000.
[16] Section 67 of the *Promotion of Access to Information Act* 2 of 2000.
[17] Section 68 of the *Promotion of Access to Information Act* 2 of 2000.

14.7 The research information of the Private Body or third party, if its disclosure would reveal the identity of the Private Body, the researcher, or the subject matter of the research and would place the research at a serious disadvantage;[18]

14.8 Requested for the purpose of criminal or civil proceedings after the commencement of such proceedings.[19]

15. DECISIONS

The Private Body will within 30 days of receipt of the request, decide whether to grant or refuse the request, which may be extended for a further period of not more than thirty days if the request is for a large amount of information, or the request requires a search for information held at another office of the Private Body and the information cannot reasonably be obtained within the original 30 day period. The Private Body will notify the requester in writing should an extension be sought.

16. POPIA BREACH DETECTION PROCEDURE

16.1 Monitoring & Alerts

16.1.1 IT systems must generate alerts on:

16.1.1.1 unusual file-access patterns,

16.1.1.2 repeated failed logins,

16.1.1.3 mass-download behaviour, or

16.1.1.4 malware detection.

16.1.2 Periodic (at least quarterly) vulnerability scans and penetration tests.

16.2 Staff Vigilance

16.2.1 All personnel must watch for:

16.2.1.1 lost devices,

16.2.1.2 mis-sent emails,

16.2.1.3 abnormal system prompts.

16.2.2 Any suspicion triggers immediate reporting.

17. POPIA BREACH REPORTING PROCEDURE

17.1 Immediate Reporting

[18] Section 69 of the *Promotion of Access to Information Act* 2 of 2000.
[19] Section 7 of the *Promotion of Access to Information Act* 2 of 2000.

17.1.1 Within 4 hours, the employee notifies the Information Officer by email and phone (24-hour contact list).

17.1.2 Include: date/time, description, systems involved, suspected records.

17.2 Preliminary Assessment

17.2.1 Within 8 hours, the IT Manager and the IO convene to classify the incident:

17.2.1.1 Category A: High-risk (sensitive personal information or large volume).

17.2.1.2 Category B: Medium-risk (limited data, no special categories)

17.2.1.3 Category C: Low-risk (no actual disclosure).

17.2.2 Level 1 (Low): Non-sensitive data; single user device; no client data impacted.

17.2.3 2. Level 2 (Medium): Internal firm data or limited client data; small user group; no external exposure.

17.2.4 3. Level 3 (High/Critical): Bulk client data, privileged accounts, ransomware, or evidence of data exfiltration.

17.3 Containment & Evidence Preservation

17.3.1 IT Manager disconnect affected systems, capture forensic images, preserve logs.

17.3.2 HR secures any physical evidence (e.g. access cards).

18. POPIA BREACH MANAGEMENT & NOTIFICATION

18.1 Notification to Regulator

18.1.1 If Category A or B, the Information Officer must notify the Information Regulator within 72 hours of becoming aware.

18.1.2 Notification includes:

18.1.2.1 nature of breach,

18.1.2.2 categories of data,

18.1.2.3 likely consequences, and

18.1.2.4 remedial measures taken.

18.2 Notification to Data Subjects

18.2.1 Where the breach is likely to result in harm, notify each affected data subject promptly, via written notice or email.

18.2.2 Include: description of breach, recommended steps to mitigate harm, contact details of IO.

18.3 Remediation & Follow-up

18.3.1 Implement corrective measures (e.g. password resets, additional staff training).

18.3.2 Prepare a post-mortem report within 14 days, to be reviewed by senior management and retained for at least 5 years.

19. DETECTION & REPORTING

19.1 Automated Monitoring

19.1.1 SIEM alerts on anomalous logins, privilege escalations, data exfiltration patterns.

19.1.2 Endpoint detection on malware, abnormal process behaviour.

19.2 Manual Reporting

19.2.1 Any staff member who suspects a compromise must notify the IO by email.

19.2.2 Report within 2 hours of detection, including: date/time, assets involved, nature of suspicion.

20. RESPONSE PHASES

20.1 Identification

20.1.1 IO convenes immediately upon notification.

20.1.2 Initial triage: confirm whether compromise is actual, determine scope, systems affected, data at risk.

20.2 Containment

20.2.1 Short-term:

20.2.1.1 Isolate affected hosts from the network.

20.2.1.2 Change credentials for compromised accounts.

20.2.1.3 Block malicious IPs or domains at firewall.

20.2.2 Long-term:

20.2.2.1 Apply ACL changes, patch vulnerable services, implement additional network segmentation.

20.3 Eradication

20.3.1 Remove malware, backdoors and unauthorised accounts.

20.3.2 Patch operating systems, applications and firmware to the latest vendor-recommended versions.

20.3.3 Conduct root-cause analysis with your forensic partner.

20.4 Recovery

20.4.1 Restore systems from known-good backups.

20.4.2 Validate integrity of restored data and applications.

20.4.3 Bring systems back online in a controlled, phased manner.

20.4.4 Monitor closely for recurrence of malicious activity.

20.5 Lessons Learned

20.5.1 Within 7 days, IO produces a Post-Incident Report covering:

20.5.1.1 Timeline of events

20.5.1.2 Technical root cause

20.5.1.3 Effectiveness of containment and recovery

20.5.1.4 Compliance notifications made (e.g. Information Regulator under POPIA, affected data-subjects)

20.5.1.5 Recommendations for policy or technical improvements

20.5.1.6 Review and update this response plan, train all staff on new procedures within *30 days*.

21. COMMUNICATION PROTOCOL

21.1 Internal:

21.1.1 Safety-first briefing to all staff within 24 hours of Level 2/3 incidents.

21.1.2 Ongoing status updates via secure channel (e.g. encrypted group chat).

21.2 External:

21.2.1 Regulatory notifications (Information Regulator, Law Society) triggered for Level 2/3 per POPIA.

21.2.2 Client notifications by letter or encrypted email where client data is impacted, including remedial advice.

21.2.3 Media statements approved by Managing Partner and Communications Lead.

22. DOCUMENTATION & RECORD-KEEPING

22.1 Incident Log: capture every step, decision and action (retained ≥ 5 years).

22.2 Evidence Archive: securely store forensic images, logs, chain-of-custody records.

22.3 Policy Updates: track revisions to this plan in a versioned document control register.

23. TRAINING & TESTING

23.1 Annual Tabletop Exercises: simulate Level 1–3 incidents with IO and executive management.

23.2 Quarterly Phishing Drills: ensure staff vigilance remains high.

23.3 Continuous Awareness: monthly security bulletins highlighting emerging threats and best practices.

24. TRAINING & AWARENESS

24.1 Annual mandatory POPIA & PAIA training for all staff.

24.2 Quarterly refreshers on breach indicators and reporting channels.

24.3 Testing of incident-response drills at least once per year.

25. RECORD-KEEPING & REVIEW

25.1 Breach Register: all incidents, reports, notifications, remediation actions (retain 5 years).

25.2 PAIA Register: all requests, decisions, disclosures, appeals (retain 5 years).

25.3 Annual compliance audit by an independent reviewer; report findings to senior management.

26. AVAILABILITY OF THE MANUAL

The Manual of the Private Body is available on the premises of the Private Body, upon request, on the website, and at the Regulator.

27. UPDATING OF THE MANUAL

The head of NVZA Incorporated Attorneys will on a regular basis update this manual.

Issued by

_____

Nadia Reyneke (Unsigned and sent electronically)

CEO