NINETY8 PROJECTS

(PTY) LTD

POPIA COMPLIANCE POLICY, PRIVACY NOTICE AND DATA SUBJECT RIGHTS PROCEDURE

Prepared for internal governance, website publication support, client onboarding, supplier engagement and general privacy compliance.

Legal name	NINETY8 PROJECTS (PTY) LTD
Registration number	2025/784588/07
Information Officer	Junior Machwisa Maduane Maraatsile
Role	Sole Director and Information Officer
Company contact email	letswork@ninety8projects.co.za
Director email	junior@ninety8.co.za
Company phone	065 887 4301
Registered office	20 Jan Steyl Avenue, Roodewal, Bloemfontein, Free State, 9301
Document status	Version 1.0
Effective date	8 March 2026

Approved and signed at Bloemfontein on 08/03/2026

Junior Machwisa Maduane Maraatsile
Sole Director and Information Officer

1. Purpose of this document

This document sets out how NINETY8 PROJECTS (PTY) LTD processes personal information, protects the privacy rights of data subjects and gives practical effect to the Protection of Personal Information Act, 4 of 2013. It is drafted to serve as the company's internal POPIA compliance policy, its external privacy notice where relevant, and its operating procedure for receiving, assessing and responding to privacy-related requests, objections, complaints and incidents.

This document must be read together with the company's PAIA Manual, its client and supplier agreements, employment-related documentation where applicable, website terms and conditions, cookie notice where deployed, and any service-specific privacy notices issued from time to time. Where a contract, law or regulator requirement imposes a stricter obligation than this policy, the stricter requirement prevails.

2. Scope

This policy applies to all personal information processed by or on behalf of the company in the course of its business activities, whether in hard copy, electronic, verbal or any other recorded form. It applies to information relating to customers, prospective customers, suppliers, service providers, job applicants, employees if later engaged, website visitors, professional contacts, contractors and any other identifiable natural person and, where applicable, juristic persons.

The policy applies to processing undertaken through email, telephonic engagement, tender submissions, websites, forms, invoices, quotations, marketing campaigns, social media inboxes, cloud services, banking records, supplier databases, internal documents and any other business process in which personal information is collected, stored, used, disclosed, archived or destroyed.

3. Responsible party and accountability

NINETY8 PROJECTS (PTY) LTD is the responsible party for purposes of POPIA to the extent that it determines the purpose of and means for processing personal information. The company remains accountable for personal information processed on its behalf by operators, contractors, software providers, hosting environments and other third parties.

The company is presently founder-led. All strategic, commercial, administrative, compliance and operational functions are currently managed by Junior Machwisa Maduane Maraatsile in his capacity as sole director and Information Officer. No Deputy Information Officer has been appointed at the date of this document. If one is appointed later, this policy must be updated without delay.

4. Information Officer details

Information Officer: Junior Machwisa Maduane Maraatsile
Title: Sole Director and Information Officer
Company email: letswork@ninety8projects.co.za

Direct email: junior@ninety8.co.za
Telephone: 065 887 4301
Registered office: 20 Jan Steyl Avenue, Roodewal, Bloemfontein, Free State, 9301

The Information Officer is responsible for encouraging compliance with POPIA and PAIA, approving internal controls, overseeing request and complaint handling, maintaining or supervising records of processing activities, monitoring operator management, guiding incident response and serving as the point of contact with the Information Regulator.

5. Definitions and interpretation

In this document, unless the context indicates otherwise, the terms personal information, processing, data subject, responsible party, operator, special personal information, unique identifier, de-identify, filing system and Information Regulator bear the meanings assigned to them in POPIA. References to the company, we, us or our mean NINETY8 PROJECTS (PTY) LTD. References to you or your mean the relevant data subject or lawful representative.

6. POPIA processing principles adopted by the company

The company adopts and applies the eight conditions for lawful processing as practical operating rules:

6.1 Accountability. The company accepts responsibility for every processing activity carried out under its authority.
6.2 Processing limitation. Personal information will be processed lawfully, minimally and in a manner that does not unreasonably infringe privacy.
6.3 Purpose specification. Information will be collected for a specific, explicitly defined and lawful purpose connected to a real business need.
6.4 Further processing limitation. Re-use of information must be compatible with the original purpose or otherwise justified by law or consent.
6.5 Information quality. Reasonable steps must be taken to ensure that personal information is complete, accurate, not misleading and kept updated where necessary.
6.6 Openness. Data subjects must be informed of relevant collection and processing practices except where the law permits otherwise.
6.7 Security safeguards. Appropriate technical and organisational measures must be maintained to guard against loss, damage, unauthorised access, disclosure or unlawful processing.
6.8 Data subject participation. Data subjects may access, correct, object to or complain about certain processing, subject to lawful limits.

7. Categories of personal information the company may process

Depending on the service, engagement or interaction, the company may process some or all of the following categories of personal information:

7.1 Identification and contact details, including names, surnames, identity numbers, registration numbers, business names, addresses, email addresses, phone numbers and job titles.
7.2 Commercial and transaction information, including quotations, purchase orders, invoices, proof of payment, banking details, tax numbers, tender records, supplier records and service histories.
7.3 Communication records, including email correspondence, call notes, meeting notes, WhatsApp or similar business communication records, support requests and website enquiry submissions.
7.4 Marketing and digital interaction data, including campaign engagement records, website analytics data, cookie-related data where cookies are enabled, IP addresses, browser or device information and form submissions.
7.5 Compliance and risk information, including tax status information, CSD-related records, B-BBEE support records, due diligence documentation, mandates, contractual records and complaint records.
7.6 Recruitment or staffing information, if applicable in future, including curriculum vitae, qualifications, references, right-to-work verification details and onboarding records.
7.7 Limited special personal information only where strictly lawful and necessary, such as disability information for accommodation purposes or biometric verification where specifically justified and lawfully controlled. The company does not intentionally seek to collect special personal information unless a lawful ground clearly exists.

8. Sources of personal information

Personal information may be obtained directly from the data subject, from the data subject's employer or organisation, from public sources, from lawful service providers, from tender portals, from government databases where access is lawful, from banks and payment processors, from cookies or website technologies, from social media interactions initiated by the data subject, or from third parties where the law permits and adequate notice is given where required.

9. Purposes for processing personal information

The company may process personal information for one or more of the following purposes:

9.1 To provide products or services, issue quotations, respond to enquiries, conclude and perform contracts, manage projects and support client relationships.
9.2 To source goods and services, manage suppliers, verify counterparties, process procurement and perform operational logistics.
9.3 To invoice, collect payment, manage accounting records, conduct financial administration and meet tax and audit obligations.
9.4 To register on supplier databases, submit bids or tenders, perform due diligence, manage compliance records and demonstrate legal, regulatory or commercial capability.
9.5 To recruit, contract, onboard and manage personnel or contractors if and when the company expands.
9.6 To maintain internal records, governance controls, risk management, security monitoring and dispute

resolution files.
9.7 To market the company's own lawful products and services where permitted by POPIA and other applicable law, and always subject to consent, opt-out rights or existing customer rules where relevant.
9.8 To operate and improve the website, digital channels, analytics environment, service performance and user experience.
9.9 To comply with legal obligations, lawful requests, court orders, subpoenas, regulator instructions and legitimate reporting duties.

10. Lawful grounds relied on for processing

The company will only process personal information where a lawful basis exists. Depending on the context, the company may rely on:
10.1 the data subject's consent,
10.2 the conclusion or performance of a contract,
10.3 compliance with a legal obligation imposed on the company,
10.4 protection of a legitimate interest of the data subject,
10.5 performance of a public law duty by a public body where applicable to a particular interaction, or
10.6 the company's legitimate interests or those of a third party, provided such interests are not overridden by the data subject's rights and the processing remains lawful, necessary and proportionate.

Where consent is used, the company will keep a record of it where reasonably possible. Where consent is withdrawn, the company will stop the relevant consent-based processing unless another lawful ground applies.

11. Children and special personal information

The company does not knowingly collect personal information relating to children unless this is strictly necessary, lawful and supported by consent from a competent person or another lawful exception under POPIA. If the company becomes aware that children's information has been obtained without a valid basis, it will take appropriate remedial steps.

The company will not process special personal information unless the law clearly permits it and adequate additional safeguards are in place. Any future processing of health information, biometric information, religious beliefs, race information, trade union membership, criminal behaviour information or similar high-risk data must be specifically assessed and approved by the Information Officer before implementation.

12. Direct marketing rules

The company may conduct direct marketing of its own products or services by electronic communication only where the requirements of POPIA are met. Prospective customers who are not existing customers may only be approached after proper consent is obtained in the prescribed manner. Existing customers

may be approached regarding the company's own similar products or services only where their contact details were obtained in the context of a sale or service and they were given a reasonable opportunity to object at the time of collection and with every communication thereafter.

The company will not sell personal information for marketing lists. Every electronic marketing communication must contain a simple opt-out or unsubscribe mechanism that is honoured promptly.

13. Disclosure of personal information

The company may disclose personal information to third parties only where the disclosure is lawful, necessary and appropriately controlled. Recipients may include banks, payment processors, accountants, legal advisers, auditors, cloud service providers, web hosting providers, domain or email service providers, analytics providers, customer relationship tools, insurers, couriers, print providers, government bodies, procurement portals and other operators or counterparties involved in delivering services or complying with legal obligations.

Personal information will not be disclosed in a blanket or excessive manner. Sharing will be limited to what is reasonably required for the relevant purpose and, where appropriate, subject to written confidentiality, data processing or service terms.

14. Cross-border transfers

The company may store or process information using systems whose servers or support teams are located outside South Africa, or may disclose information across borders where a service model requires it. Cross-border transfers will only occur where one of the lawful grounds in POPIA is present, including adequate protection by the recipient, data subject consent, contractual necessity, benefit to the data subject or another recognised legal basis.

Where foreign-hosted platforms are used, the company must assess vendor safeguards, contractual protections and access controls before or as soon as reasonably possible after deployment. The company will update its operator schedule when its final software and hosting stack is confirmed.

15. Operators and service providers

The company may appoint operators to process personal information on its behalf. Operators must be chosen with due regard to security, reliability, confidentiality and legal compliance. Where reasonably practicable, operator relationships must be governed by written terms requiring the operator to:

15.1 process information only with the knowledge or authorisation of the company,

15.2 treat information as confidential,

15.3 maintain appropriate security measures,

15.4 notify the company without undue delay of any actual or suspected security compromise,

15.5 return, delete or de-identify information when the engagement ends, subject to lawful retention

duties, and

15.6 assist with information requests, deletion workflows, audits or incident response where relevant.

At the date of this document, the company's final confirmed operator list for hosting, email, analytics, CRM and related services is still being formalised. Until the register is finalised, no internal team member may onboard a new processor or software tool that touches personal information without the Information Officer's approval.

16. Security safeguards

The company implements and will continue to strengthen reasonable technical and organisational measures to prevent loss, misuse, unauthorised access, unlawful disclosure, alteration, destruction or other compromise of personal information. Measures include role-based access discipline, device passcodes, strong passwords, email hygiene, limited sharing, secure record storage, contractual confidentiality controls, anti-fraud vigilance, basic vendor due diligence and prompt restriction of access where risk is identified.

As the business scales, the company will progressively formalise additional controls, including documented access matrices, secure backup procedures, password manager adoption, multi-factor authentication, endpoint protection, website security headers, form submission controls, encrypted storage where appropriate, incident registers, deletion logs and operator due diligence records.

No security control can guarantee absolute protection. For that reason, every person acting for or on behalf of the company must immediately report a suspected compromise, mistaken disclosure, phishing event, lost device, unauthorised access or privacy incident to the Information Officer.

17. Security compromise response

If there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, the company will investigate the incident promptly, contain the risk, preserve evidence where possible, assess the categories and volume of affected information, identify affected data subjects, evaluate harm and comply with notification duties to the Information Regulator and affected data subjects where required by law.

Notifications will be made as soon as reasonably possible and will describe, to the extent known, the nature of the compromise, the information concerned, the measures taken by the company, recommended steps for affected persons and the contact details for further assistance. Internal incident records must be retained as compliance evidence.

18. Retention and destruction

The company will retain personal information only for as long as reasonably necessary to achieve the purpose for which it was collected, to comply with legal or contractual duties, to defend or exercise legal rights or to maintain lawful business records. Once retention is no longer required, the information must

be securely destroyed, deleted or de-identified in a manner appropriate to the medium and sensitivity of the record.

Until the company's final detailed retention matrix is approved, the following default schedule applies unless a law, contract, regulator instruction or litigation hold requires longer retention:
18.1 Corporate formation, governance and statutory records: retain for the life of the company and thereafter as required by law.
18.2 Contracts, quotations, invoices, accounting records and tax records: retain for at least the minimum period required by applicable tax, company, procurement and audit laws, and generally not less than five years after the end of the relevant financial period unless longer retention is justified.
18.3 Tender, supplier and due diligence records: retain for the bid cycle, contract period and a reasonable limitation period thereafter.
18.4 Website enquiries, general correspondence and dormant prospect records: review periodically and delete or de-identify when no longer necessary.
18.5 Complaint, incident and legal dispute records: retain for the life of the matter and an appropriate period thereafter.
18.6 Recruitment records of unsuccessful applicants: retain only as long as reasonably necessary for the recruitment process and any lawful challenge period unless consent is obtained for longer retention.
18.7 Marketing consent and unsubscribe records: retain as compliance evidence for as long as reasonably required.

19. Data subject rights

Subject to POPIA, PAIA and any lawful limitation, data subjects may have the right to:
19.1 be notified that personal information is being collected,
19.2 be notified of certain security compromises,
19.3 request confirmation of whether the company holds personal information about them,
19.4 request access to their personal information or to records containing it, subject where applicable to PAIA procedures and lawful grounds of refusal,
19.5 request correction, updating, destruction or deletion of inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained personal information,
19.6 object, on reasonable grounds, to processing in certain circumstances,
19.7 object to direct marketing by means of unsolicited electronic communications,
19.8 withdraw consent where processing depends on consent, and
19.9 lodge a complaint with the Information Regulator or pursue civil remedies where available.

20. Requests for access, correction, deletion or objection

Requests must be submitted to the Information Officer in writing using sufficient detail to identify the requester, the right being exercised and the information concerned. The company may request proof of identity, authority or representation before acting on a request. Where access to records is requested,

the company may require the requester to follow the company's PAIA procedure and prescribed forms where applicable.

The company will assess each request on its merits, having regard to POPIA, PAIA, other applicable laws, confidentiality duties, legal privilege, third-party rights, record integrity, fraud prevention and operational feasibility. A request may be granted in whole or in part, or refused where the law permits. The company may also ask for clarification where the request is vague, overbroad or impossible to process responsibly.

Requests and privacy complaints should be sent to letswork@ninety8projects.co.za, copied to junior@ninety8.co.za where appropriate, with the subject line 'POPIA Request' or 'POPIA Complaint'.

21. Information quality and minimisation

Before collecting or reusing personal information, the company must ask whether the information is truly needed, whether the purpose is clear, whether a less intrusive method is available and whether the record can be de-identified, shortened or avoided entirely. Data quality must be checked when information is collected, when material decisions are made using it and when a data subject requests correction.

22. Website privacy, cookies and analytics

Where the company operates a website, landing page or online form, it may collect limited technical and engagement information necessary to operate the website, secure the service, analyse usage, respond to form submissions and improve user experience. If cookies, pixels or similar technologies are deployed, a suitable cookie notice and preference mechanism must be implemented where required, especially for non-essential analytics or marketing technologies.

Website forms should collect only the fields reasonably required for the relevant purpose. If analytics, CRM integrations, newsletter systems, reCAPTCHA, embedded maps, chat tools or similar services are activated, this document and the website privacy notice must be updated to reflect the actual stack and relevant third-party processing.

23. Staff and contractor responsibilities

Any person acting for or on behalf of the company who handles personal information must:
23.1 process information only for authorised business purposes,
23.2 keep information confidential,
23.3 not share records casually, publicly or through unsecured channels,
23.4 verify recipients before sending information,
23.5 report incidents immediately,
23.6 follow deletion and retention instructions,

23.7 avoid storing unnecessary copies of personal information, and
23.8 co-operate with compliance reviews, request handling and remediation steps.

Because the company is currently founder-led, these obligations fall primarily on the Information Officer. As new employees or contractors are appointed, POPIA duties must be written into their onboarding, confidentiality and operational controls.

24. Complaints and contact with the Information Regulator

A data subject who believes that the company has interfered with a privacy right may first contact the Information Officer so that the matter can be assessed and, where appropriate, corrected promptly. A data subject may also lodge a complaint with the Information Regulator of South Africa.

Information Regulator (South Africa)
General email: enquiries@inforegulator.org.za
Complaints email: complaints.IR@justice.gov.za
Website: www.inforegulator.org.za

The company may update these contact details in future if the Regulator changes them on its official channels.

25. Policy governance and review

This policy is a living governance document. It must be reviewed whenever there is a material change in the company's services, staffing model, website stack, operator list, retention framework, marketing model, incident history or legal environment, and in any event at least annually.

Where this document identifies a schedule, list or control as 'to be confirmed' or 'to be updated', that wording does not suspend compliance. It means the company must continue to act in accordance with POPIA using lawful, minimal and reasonable processing until the formal schedule is finalised. No person may treat a placeholder as permission to process information carelessly or without purpose.

26. Important current implementation notes for NINETY8 PROJECTS

At the date of this version:
26.1 the company is solely owned and managed by Junior Machwisa Maduane Maraatsile,
26.2 the company is a private company registered under number 2025/784588/07,
26.3 the primary company email is letswork@ninety8projects.co.za,
26.4 the director's direct email is junior@ninety8.co.za,
26.5 the company phone number is 065 887 4301,
26.6 no Deputy Information Officer has been appointed,
26.7 the detailed operator register for hosting, email, analytics, CRM, cloud storage and related services must still be finalised and documented, and

26.8 the retention schedule in section 18 is the current default framework and must be refined once the full records map is completed.

These implementation notes are included so that this document can be used immediately while the company continues to mature its systems and controls.

27. Signature

Signed by the undersigned, being duly authorised on behalf of NINETY8 PROJECTS (PTY) LTD, to confirm adoption of this POPIA Compliance Policy, Privacy Notice and Data Subject Rights Procedure.

Annexure A. Suggested request checklist

- Full name and contact details of requester
- Capacity of requester and proof of authority if acting for another person or entity
- Description of the information, record or right involved
- Reason for access, correction, deletion or objection where required
- Supporting identity verification documents
- Preferred method of response

Annexure B. Immediate internal action list for privacy incidents

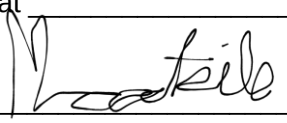
- Stop the exposure or isolate the affected system, account, device or document
- Preserve evidence and note dates, times, recipients and systems involved
- Assess what categories of personal information may be affected
- Identify how many data subjects may be affected
- Reset access credentials or revoke access where necessary
- Notify the Information Officer immediately
- Document containment, recovery and notification decisions

Annexure C. Controlled placeholders still to be completed as the company stack matures

Item	Current status	Required action
Website and hosting operator register	Not yet fully confirmed	Record the final website host, domain provider, form tools, SSL/security layers and any CDN or content services.
Email and collaboration operator register	Partially known	Record the actual email platform, mailbox administrator,

		storage environment and access rights.
Analytics and marketing tool register	Not yet fully confirmed	Record analytics, advertising pixels, newsletter systems, CRM tools and consent controls before activation.
Detailed retention matrix	Default framework only	Map each record type to a lawful retention period, destruction method and owner.

Signed at Bloemfontein on 08/03/2026



Junior Machwisa Maduane Maraatsile
Sole Director and Information Officer