GRC SHOP

Governance | Risk | Compliance

POPIA Data Protection Policy

Comprehensive Data Protection Framework

Version 2.0 | March 2026 | Classification: Public Document

1. Executive Summary

1.1 Purpose and Scope

02X (Pty) Ltd (trading as GRC Shop)'s comprehensive framework for protecting personal information in accordance with the Protection of Personal Information Act 4 of 2013 and its amended regulations (April 2025). As a specialised GRC compliance consulting provider, we process personal information of clients, employees, and business partners while delivering professional services including document preparation, regulatory advisory, and compliance training.

As a GRC consulting provider, GRC Shop holds its own data protection practices to the same rigorous standard it advises clients to adopt.

1.2 Critical POPIA Obligations

Our compliance framework addresses the eight core POPIA processing conditions:

- Accountability: Demonstrable compliance with comprehensive documentation
- Processing Limitation: Lawful, reasonable, and necessary processing only
- Purpose Specification: Clear, specific purposes communicated at collection.
- Further Processing Limitation: Compatible use with original purposes
- Information Quality: Accurate, complete, and up-to-date data maintenance
- Openness: Transparent processing with accessible privacy notices
- Security Safeguards: Appropriate technical and organisational measures
- Data Subject Participation: Respect for individual rights and participation

1.3 Risk-Based Approach

GRC Shop employs a risk-based approach to data protection, with enhanced controls for:

- High-risk processing: Special personal information, international transfers
- Medium-risk processing: Employee data, training records, client communications
- Standard processing: General business communications, marketing activities

1.4 Target Audience

This policy applies to all GRC Shop personnel, contractors, operators, and business partners involved in personal information processing activities.

2. Legal Framework and Regulatory Basis

2.1 Primary Legislation

Legislation	Application	Key Requirements
Protection of Personal Information Act 4 of 2013	Primary data protection framework	Eight processing conditions, data subject rights, accountability
POPIA Regulations (as amended April 2025)	Implementation guidance and procedures	Enhanced consent requirements, streamlined objection processes
Promotion of Access to Information Act 2 of 2000	Access to information framework	PAIA manual requirements, access procedures
Electronic Communications and Transactions Act 25 of 2002	Electronic communications	Direct marketing restrictions, electronic consent

2.2 Sector-Specific Requirements

- Labour Relations Act 66 of 1995: Employee information processing
- Skills Development Act 97 of 1998: Training record requirements
- Occupational Health and Safety Act 85 of 1993: Health surveillance data
- Companies Act 71 of 2008: Corporate record-keeping obligations.

2.3 Regulatory Updates Integration

This policy has been updated to reflect the April 2025 amended POPIA Regulations, including:

- Enhanced positive consent requirements for direct marketing.
- Streamlined data subject objection and correction processes.
- Expanded Information Officer duties for continuous compliance improvement.
- Clarified definitions and complaint handling procedures.

3. Policy Statement and Scope

3.1 Policy Statement

02X (Pty) Ltd (trading as GRC Shop) is committed to protecting the privacy and personal information of all individuals whose data we process. We recognise that personal information is a valuable asset requiring careful handling in accordance with legal requirements and ethical principles.

Our Enhanced Commitments:

- Process personal information lawfully, fairly, and transparently with demonstrable accountability.
- Collect personal information only for legitimate, specified business purposes.
- Maintain accurate, complete, and up-to-date personal information through regular verification.
- Implement appropriate technical and organisational security measures with continuous improvement.
- Respect individual rights with efficient, accessible exercise mechanisms.
- Ensure comprehensive accountability through documented compliance evidence.

3.2 Scope of Application

Organisational Scope

- 02X (Pty) Ltd (trading as GRC Shop) as responsible party
- All employees, contractors, consultants, and temporary staff
- Third-party operators and service providers under written agreements
- Business partners and joint processing arrangements

Processing Scope

- All personal information regardless of format (electronic, paper, verbal, biometric)
- All processing activities including collection, storage, use, disclosure, and destruction
- All business operations including consulting, training, document preparation, and administration
- All locations including offices, client sites, remote work environments, and cloud systems

Geographic Scope

- Primary operations within South Africa
- International transfers subject to enhanced safeguards and documentation
- Cross-border processing through cloud services and international operators

---

4. POPIA Processing Conditions Framework

4.1 Eight Processing Conditions Compliance Matrix

Processing Condition	GRC Shop Implementation	Responsible Role	Monitoring Frequency
1. Accountability	Comprehensive documentation, regular audits, demonstrable compliance	Information Officer	Quarterly
2. Processing Limitation	Lawful basis assessment, necessity testing, proportionality review	Information Officer	Per processing activity
3. Purpose Specification	Clear purpose statements, collection notices, purpose limitation	Information Officer	At collection
4. Further Processing Limitation	Compatibility assessments, consent for new purposes	Information Officer	Before new processing
5. Information Quality	Data accuracy procedures, regular updates, correction mechanisms	Information Officer	Monthly
6. Openness	Privacy notices, transparent communication, accessible information	Information Officer	Annually
7. Security Safeguards	Technical and organisational measures, regular security reviews	IT Administrator	Continuously
8. Data Subject Participation	Rights exercise procedures, complaint handling, participation mechanisms	Information Officer	Per request

Processing Condition	GRC Shop Implementation	Responsible Role	Monitoring Frequency

ℹ Where a specific responsible role is not filled, responsibility defaults to the Information Officer.

5. Definitions and Key Terms

5.1 POPIA Definitions

Term	Definition	GRC Shop Context
Personal Information	Information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person	Client contacts, employee data, training records, business communications
Processing	Any operation concerning personal information, including collection, receipt, recording, organisation, storage, updating, retrieval, alteration, consultation, use, dissemination, merging, linking, restriction, degradation, erasure, or destruction	All GRC Shop business activities involving personal information
Data Subject	The person to whom personal information relates	Clients, employees, training participants, website visitors
Responsible Party	02X (Pty) Ltd (trading as GRC Shop) as the entity determining processing purposes and means	GRC Shop as primary responsible party
Operator	Any person processing personal information on behalf of GRC Shop under written agreement	Cloud providers, IT support, professional services
Special Personal Information	Information concerning religious beliefs, race, ethnic origin, political opinions, health, sex life, biometric information, criminal behaviour, trade union membership	Limited processing for OHS compliance and security clearances

5.2 Enhanced Definitions (April 2025 Amendments)

Term	Enhanced Definition	Implementation
Complaint	Any expression of dissatisfaction regarding personal information processing	Formal complaint handling procedure with written responses
Writing	Includes electronic communication and digital formats	Email, digital forms, electronic signatures accepted
Positive Consent	Clear affirmative action indicating agreement to processing	Opt-in mechanisms, explicit consent checkboxes, documented agreements

6. Personal Information We Process

6.1 Categories of Personal Information

Category	Examples	Processing Purpose	Legal Basis	Risk Level
Client Contact Information	Names, job titles, business contact details, company affiliations, professional qualifications	Service delivery, relationship management, compliance consulting	Legitimate Interest / Contract	Medium
Employee Information	Personal identifiers, contact info, employment history, qualifications, performance data, payroll	Employment management, compliance, benefits administration	Contract / Legal Obligation	Medium
Training Records	Completion certificates, competency assessments, professional development records, certification tracking	Skills development compliance, professional certification	Legal Obligation / Legitimate Interest	Medium
Special Personal Information	Health info (OHS compliance), criminal behaviour (security clearances), biometric data (access control)	Regulatory compliance, security management	Legal Obligation / Explicit Consent	High
Marketing Information	Communication preferences, engagement history, newsletter subscriptions	Marketing communications, business development	Consent / Legitimate Interest	Low

6.2 Sources of Personal Information

Source Category	Specific Sources	Collection Method	Verification Process
Direct Collection	Client registration forms, employee applications, training registrations, website forms	Online forms, paper applications, verbal communication	Identity verification, document validation
Client Organisations	Organisational charts, contact lists, appointment letters, compliance documentation	Client-provided documents, authorised disclosures	Client authorisation, data accuracy confirmation
Public Sources	Professional directories, regulatory databases, company websites, LinkedIn profiles	Automated collection, manual research	Source verification, accuracy checking
Third-Party Providers	Training organisations, certification bodies, regulatory authorities, background check providers	Formal data sharing agreements, authorised requests	Provider verification, data quality assessment

6.3 Special Personal Information Processing

⚠ Enhanced Safeguards: Special personal information processing requires explicit consent or clear legal obligation, enhanced security measures, restricted access, and regular necessity reviews.

Limited Processing Circumstances:

- Health Information: Only for occupational health and safety compliance purposes under OHS Act requirements.
- Criminal Behaviour Information: Only for security clearance verification or regulatory compliance requirements
- Biometric Information: Only for secure access control systems with explicit consent
- Trade Union Membership: Only where disclosed for workplace representation purposes

7. Lawful Basis for Processing

7.1 Primary Lawful Bases with Practical Examples

Lawful Basis	Legal Reference	Business Context	Practical Example	Assessment Criteria
Legitimate Interest	Section 11(1)(f)	Client relationship management, business operations, professional development	Using client work email to send regulatory updates affecting their industry	Necessity test, balancing assessment, data subject interests
Contractual Necessity	Section 11(1)(b)	Employment contracts, client service agreements, supplier contracts	Processing new hire bank details for salary payment setup	Contract performance requirement, essential processing
Legal Obligation	Section 11(1)(c)	Regulatory reporting, tax compliance, health and safety legislation	Maintaining OHS training records for 5 years per Skills Development Act	Statutory requirement, compliance necessity
Consent	Section 11(1)(a)	Marketing communications, optional services, voluntary programs	Newsletter subscriptions with explicit opt-in consent	Freely given, specific, informed, unambiguous

7.2 Legitimate Interest Assessments (LIA)

Enhanced LIA Process

1. Purpose Test: Clearly identify the legitimate interest pursued.
2. Necessity Test: Demonstrate processing is necessary for the legitimate interest.
3. Balancing Test: Assess impact on data subject rights and interests.
4. Safeguards Assessment: Identify measures to protect data subject interests.
5. Documentation: Maintain written LIA records for audit purposes

LIA Documentation Requirements

- Detailed legitimate interest identification
- Necessity justification with alternatives considered.
- Data subject impact assessment
- Balancing test results with risk mitigation measures
- Regular review and update schedule

8. Data Subject Rights

8.1 Comprehensive Rights Framework

Right	Legal Reference	Description	Response Timeline	Fee Structure
Right to Access	Section 23	Confirmation of processing, copies of personal information, processing details	30 days (extendable to 60 days)	Generally free; reasonable fee for excessive requests
Right to Correction	Section 24	Correction of inaccurate information, completion of incomplete information	30 days	Free
Right to Deletion	Section 17	Deletion when retention no longer necessary, processing unlawful, consent withdrawn	30 days	Free
Right to Object	Section 11(3)	Object to direct marketing, legitimate interest processing, automated decision-making	Immediate for marketing; 30 days for other objections	Free
Right to Restrict Processing	Enhanced framework	Temporary restriction pending correction or objection resolution	30 days	Free

8.2 Enhanced Rights Exercise Process

Submission Methods

- Primary: compliance@grcshop.co.za with 'Data Subject Request' in subject line
- Online Portal: Coming soon — GRC Shop's secure data subject portal is currently in development. Please submit requests via email in the interim.
- PAIA Manual: Cross-reference to formal PAIA manual for access requests
- Phone: 082 835 4731 during business hours (followed by written confirmation)
- Post: 11 Knights Court, Sandton, Gauteng, 2191 with proof of identity

Required Information

- Proof of identity (certified copy of ID document or passport)
- Specific details of the request with clear description
- Preferred response method and format
- Authorisation if acting on behalf of another person.
- Relevant reference numbers or account details

Response Process

6. Acknowledgment: Within 5 (five) business days with reference number
7. Identity Verification: Confirm requester identity and authority.
8. Request Assessment: Determine validity, scope, and applicable fees.
9. Information Gathering: Collect relevant personal information.
10. Response Preparation: Prepare comprehensive response with explanations.
11. Delivery: Provide response in requested format with appeal information

Refusal Criteria and Process

- Manifestly Unfounded: Clearly frivolous or vexatious requests
- Excessive: Repetitive requests without reasonable intervals
- Third-Party Rights: Requests affecting other individuals' rights.
- Legal Privilege: Information subject to legal professional privilege
- Written Reasons: All refusals include detailed written justification and appeal rights.

---

9. Data Sharing and Transfers

9.1 Enhanced Regulatory Body Sharing

Mandatory Sharing Circumstances

- Department of Employment and Labour: OHS compliance data, training records, incident reports.
- South African Revenue Service: Tax compliance information, payroll data, financial records
- Professional Regulatory Bodies: Certification data, competency records, compliance status
- Law Enforcement: Only when legally compelled with proper authorisation
- Information Regulator: Breach notifications, compliance reports, investigation responses

Sharing Safeguards

- Minimum necessary information principle
- Proper legal authorisation verification
- Documented sharing decisions with justification
- Data subject notification where legally required.
- Secure transmission methods with encryption

9.2 Enhanced Operator Management

Operator Type	Examples	Due Diligence Requirements	Contract Clauses
IT Service Providers	Cloud hosting, software providers, IT support	Security certifications, data location disclosure, breach procedures	Data protection clauses, security standards, audit rights
Professional Services	Legal advisors, accounting firms, consultants	Professional indemnity, confidentiality agreements, competency verification	Confidentiality, purpose limitation, return/destruction
Training Providers	Certification bodies, training organisations, assessment providers	Accreditation verification, data handling procedures, security measures	Data minimisation, retention limits, secure transmission
Administrative Services	Document management, courier services, facilities management	Background checks, security protocols, access controls	Access restrictions, confidentiality, incident reporting

Enhanced Operator Requirements

- Written Agreements: Mandatory data protection clauses in all operator contracts
- Due Diligence: Pre-appointment security and compliance assessment

- Security Standards: Minimum technical and organisational measures specification
- Audit Rights: Annual compliance verification and audit access.
- Breach Notification: Immediate notification of suspected or actual breaches
- Data Return/Destruction: Secure return or certified destruction upon contract termination

9.3 International Transfers Framework

Transfer Assessment Process

12. Necessity Assessment: Confirm transfer is necessary for legitimate business purpose.
13. Destination Analysis: Evaluate receiving country data protection adequacy.
14. Safeguards Selection: Choose appropriate safeguards per Section 72 POPIA
15. Documentation: Maintain transfer register with all relevant details
16. Data Subject Notification: Inform data subjects of international transfers where required.

Destination	Adequacy Status	Required Safeguards	Documentation
EU / EEA Countries	Adequate protection	Standard contractual clauses	Transfer agreement, adequacy confirmation
Other Countries	Case-by-case assessment	Binding corporate rules, contractual clauses, certification schemes	Adequacy assessment, supplementary measures
Cloud Services	Provider-dependent	Data processing agreements, encryption, access controls	Service agreement, security specifications

10. Data Security and Protection

10.1 Technical Safeguards Framework

Access Controls

- Multi-Factor Authentication (MFA): Mandatory for all system access
- Role-Based Access Control (RBAC): Principle of least privilege implementation
- Regular Access Reviews: Quarterly access rights verification and cleanup
- Strong Password Policies: Minimum complexity requirements with regular updates
- Privileged Account Management: Enhanced controls for administrative access

Data Encryption

- Data at Rest: AES-256 encryption for stored data and backups
- Data in Transit: TLS 1.3 minimum for all data transmissions
- Email Encryption: Mandatory for sensitive personal information transmission.
- Mobile Device Encryption: Full device encryption for all business devices
- Cloud Storage Encryption: Client-side encryption for cloud-stored data

System Security

- Regular Security Updates: Automated patching with emergency update procedures
- Endpoint Detection and Response (EDR): Advanced threat detection and response
- Network Security: Firewall protection with intrusion detection systems.

- Vulnerability Management: Regular penetration testing and vulnerability assessments
- Backup Security: Encrypted, tested backups with secure off-site storage.

10.2 Organisational Safeguards Framework

Staff Training and Awareness

- Mandatory POPIA Training: Annual comprehensive data protection training
- Role-Specific Training: Targeted training based on data handling responsibilities.
- Security Awareness: Regular phishing simulations and security updates
- Incident Response Training: Practical breach response exercises
- Continuous Education: Ongoing updates on regulatory changes and best practices

Physical Security

- Secure Premises: Access-controlled office environments with visitor management
- Clean Desk Policy: Mandatory clear desk and screen lock requirements
- Secure Storage: Locked filing systems for physical documents
- Device Security: Laptop locks, secure storage, and tracking systems
- Disposal Security: Certified destruction of physical documents and storage media

10.3 Enhanced Data Breach Response — C.O.N.T.A.I.N. Framework

Immediate Response (0–24 hours) — C.O.N.T.A.I.N.

- C — Contain: Immediately contain the breach and prevent further unauthorised access
- O — Observe: Document all available evidence without compromising the investigation
- N — Notify: Inform Information Officer immediately (within 1 hour of discovery)
- T — Technical: Engage technical team to assess scope and implement additional safeguards
- A — Assess: Evaluate risk to data subjects and determine notification requirements
- I — Inform: Notify Information Regulator as soon as reasonably possible if high-risk
- N — Notify: Inform affected data subjects without undue delay if high-risk.

Assessment Phase (24–72 hours)

- Risk Evaluation: Comprehensive assessment of potential harm to data subjects.
- Scope Determination: Full identification of affected individuals and data categories
- Notification Preparation: Draft breach notifications for regulator and data subjects
- Remediation Planning: Develop comprehensive remediation and prevention measures.
- Legal Assessment: Evaluate potential legal implications and regulatory requirements.

Notification Requirements

- Information Regulator: As soon as reasonably possible after becoming aware
- Data Subjects: As soon as reasonably possible if likely to cause harm.
- Relevant Authorities: As required by sector-specific legislation.
- Internal Stakeholders: According to incident response plan hierarchy

Post-Incident Activities

- Lessons Learned Review: Comprehensive analysis of incident causes and response effectiveness.
- System Improvements: Implementation of additional safeguards based on incident analysis.

- Policy Updates: Revision of policies and procedures to prevent similar incidents.
- Staff Training: Additional training based on incident findings and prevention measures.

11. Data Retention and Disposal

11.1 Retention Principles

- Legal Compliance: Adherence to statutory retention requirements
- Business Necessity: Retention only while needed for legitimate business purposes.
- Data Minimisation: Regular review and deletion of unnecessary information
- Secure Storage: Appropriate security measures throughout retention period
- Documented Decisions: Written justification for all retention decisions

11.2 Comprehensive Retention Schedule

Information Category	Retention Period	Legal Basis	Disposal Trigger	Disposal Method	Responsible Role
Client Contact Information	Relationship + 5 years	Business Records Act	5 years after final invoice	Secure deletion / certified shredding	Information Officer
Client Engagement Files	Relationship + 7 years	Professional liability	7 years after project completion	Secure deletion / certified shredding	Information Officer
Employee Personal Records	Employment + 5 years	Labour Relations Act	5 years after termination	Secure deletion / certified shredding	Information Officer
Employee Payroll Records	Employment + 5 years	Income Tax Act	5 years after final payment	Secure deletion / certified shredding	Information Officer
Training Records	5 years from completion	Skills Development Act	5 years after completion	Secure deletion / certified shredding	Information Officer
Health & Safety Records	40 years from creation	OHS Act	40 years after record creation	Secure deletion / certified shredding	Information Officer
Financial Records	5 years from creation	Income Tax Act	5 years after financial year end	Secure deletion / certified shredding	Information Officer
Marketing Databases	Until consent withdrawn + 1 year	POPIA compliance	1 year after consent withdrawal	Secure deletion / suppression	Information Officer
Incident Records	3 years minimum	POPIA requirements	3 years after resolution	Secure deletion / certified shredding	Information Officer
CCTV Recordings	30 days standard	Security necessity	30 days after recording (unless incident)	Automatic overwrite / secure deletion	Information Officer
Website Analytics	2 years maximum	Legitimate interest	2 years after collection	Automatic deletion / anonymisation	Information Officer
Backup Systems	Aligned with source data	Technical necessity	Same as source data retention	Secure deletion / media destruction	Information Officer

ℹ Where a specific responsible role is not yet assigned, the Information Officer holds accountability for all retention

Information Category	Retention Period	Legal Basis	Disposal Trigger	Disposal Method	Responsible Role

and disposal activities.

11.3 Legal Hold Procedures

Legal Hold Triggers

- Litigation commenced or reasonably anticipated.
- Regulatory investigation or inquiry initiated.
- Internal investigation requiring data preservation.
- Formal complaint or dispute resolution process
- Court order or regulatory directive

Legal Hold Process

17. Hold Notice: Immediate suspension of normal disposal activities.
18. Scope Identification: Determine affected data categories and locations.
19. Stakeholder Notification: Inform all relevant data controllers and processors.
20. Documentation: Maintain detailed records of hold scope and duration
21. Regular Review: Periodic assessment of continued hold necessity
22. Release Process: Formal authorisation required for hold release

11.4 Secure Disposal Framework

Electronic Data Disposal

- Secure Deletion: NIST 800-88 compliant data sanitisation methods
- Media Destruction: Physical destruction of storage media for highly sensitive data
- Verification: Certificate of destruction for all disposal activities
- Cloud Data: Verified deletion from all cloud storage locations and backups.

Physical Document Disposal

- Cross-Cut Shredding: Minimum security level for confidential documents
- Certified Destruction: Professional destruction service for large volumes
- Witnessed Destruction: On-site witnessing for highly confidential records.
- Chain of Custody: Documented handling from collection to destruction

12. Governance and Accountability

12.1 Roles and Responsibilities Matrix

Role	Primary Responsibilities	Reporting Line	Key Accountabilities
Information Officer	POPIA compliance oversight, breach management, data subject requests, regulatory liaison	Executive Management	Overall compliance, regulatory reporting, policy implementation

Role	Primary Responsibilities	Reporting Line	Key Accountabilities
IT Administrator	Technical security measures, system access controls, backup management	Information Officer	Technical safeguards, system security, access management
HR Manager	Employee data processing, training coordination, policy communication	Information Officer	Employee data compliance, training delivery, policy awareness
Operations Manager	Client data processing, service delivery compliance, vendor management	Information Officer	Client data protection, service compliance, operator oversight
Finance Manager	Financial data processing, retention compliance, audit support	Information Officer	Financial data security, retention compliance, audit coordination

ℹ Where a named role is currently unfilled, all responsibilities and accountabilities for that role revert to the Information Officer until the role is formally appointed.

12.2 Accountability Documentation Framework

Mandatory Documentation

- Records of Processing Activities (RoPA): Comprehensive inventory of all processing activities
- Legitimate Interest Assessments (LIA): Detailed assessments for all legitimate interest processing
- Data Protection Impact Assessments (DPIA): Risk assessments for high-risk processing activities
- Operator Agreements: Written agreements with all third-party processors
- Training Records: Evidence of staff data protection training and competency
- Consent Records: Documentation of all consent collection and withdrawal.
- Breach Register: Comprehensive log of all security incidents and responses
- Transfer Register: Record of all international data transfers and safeguards.

Compliance Monitoring

- Quarterly Reviews: Comprehensive compliance assessment and gap analysis
- Annual Audits: Independent internal audit of data protection practices
- Performance Indicators: Key metrics for compliance effectiveness measurement
- Continuous Improvement: Regular enhancement of policies and procedures

12.3 Information Officer Registration and Duties

Detail	Information
Name	Philip de Witt
Registration Status	Registered with Information Regulator (Registration No: 2026-002803)
Email	compliance@grcshop.co.za
Phone	082 835 4731
Business Address	11 Knights Court, Sandton, Gauteng, 2191

Enhanced Duties (April 2025 Amendments)

- Develop and continuously improve POPIA compliance framework.
- Conduct regular compliance assessments and gap analyses.
- Manage data subject requests and complaint resolution.
- Coordinate breach response and regulatory notifications.
- Oversee operator management and international transfer safeguards.
- Provide compliance training and awareness programs.
- Maintain comprehensive compliance documentation.
- Report compliance status to executive management.

---

13. Contact Information and Complaints

13.1 GRC Shop Contact Details

Contact Type	Details
Information Officer	Philip de Witt
Compliance Email	compliance@grcshop.co.za
General Inquiries	info@grcshop.co.za
Phone	082 835 4731
Website	[WEBSITE_URL]
Business Hours	Monday to Friday, 08:00–17:00
Business Address	11 Knights Court, Sandton, Gauteng, 2191

13.2 Enhanced Complaint Process

Internal Complaint Procedure

23. Submission: Submit complaint to Information Officer via email, phone, or post
24. Acknowledgment: Written acknowledgment within 5 (five) business days with reference number
25. Investigation: Thorough investigation with stakeholder consultation (up to 30 days)
26. Response: Comprehensive written response including outcome, rationale, and remedial actions
27. Appeal: Internal appeal process if unsatisfied with initial response
28. Documentation: Complete record of complaint handling and resolution

13.3 External Complaint Options — Information Regulator of South Africa

Contact Type	Details
Website	www.justice.gov.za/inforeg
Email	inforeg@justice.gov.za
Phone	012 406 4818
Physical Address	JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
Postal Address	P.O. Box 31533, Braamfontein, 2017

ℹ GRC Shop maintains a comprehensive PAIA Manual in accordance with Section 51 of PAIA. Requests for access to information must follow the procedures outlined in the PAIA Manual, available at [PAIA_MANUAL_URL] or upon request from the Information Officer.

14. Policy Implementation and Review

14.1 Implementation Timeline

Phase	Actions
Immediate (0–30 days)	Policy communication to all staff and contractors; Information Officer registration verification; critical system access reviews; client notification; operator agreement reviews.
Short-term (30–90 days)	Comprehensive staff training program delivery; detailed procedure documentation; technical safeguard enhancement; vendor due diligence assessments; compliance documentation system.
Medium-term (90–180 days)	Advanced monitoring system deployment; international transfer safeguard implementation; enhanced breach response procedure testing; comprehensive compliance audit; performance indicator baseline.
Ongoing	Continuous compliance monitoring and improvement; regular training updates; annual policy review; regulatory development monitoring and integration.

14.2 Enhanced Review Framework

- Monthly: Operational compliance monitoring and issue identification
- Quarterly: Comprehensive compliance review and gap analysis
- Annually: Full policy review, regulatory update integration, and stakeholder feedback
- Triggered: Immediate review for significant regulatory changes, major incidents, or business changes

Review Triggers

- Significant regulatory amendments or new legislation
- Major business process changes or system implementations
- Security incidents or data breaches
- Stakeholder concerns or complaint patterns
- Regulatory guidance updates or enforcement actions
- Technology changes affecting data processing.
- Organisational restructuring or role changes

14.3 Version Control and Document Management

Version	Date	Changes	Reviewed By	Next Review
2.0	17 March 2026	Enhanced policy with April 2025 regulatory updates, comprehensive accountability framework, improved operational procedures	Philip de Witt	17 March 2027

Conclusion

02X (Pty) Ltd (trading as GRC Shop)'s comprehensive commitment to data protection excellence is reflected in this policy. By maintaining clear handling procedures, strong security protocols, proven accountability, and honouring personal rights, we responsibly manage personal information in strict compliance with legal standards.

The enhanced framework incorporates the latest regulatory developments, industry best practices, and operational excellence principles to provide superior data protection while supporting business objectives. All personnel are required to familiarise themselves with this policy, complete mandatory training, and comply with all requirements.

For questions, concerns, or requests related to this policy or personal information processing, please contact our Information Officer at compliance@grcshop.co.za or 082 835 4731.

Document Control	Details
Policy Owner	Information Officer
Approval Authority	02X (Pty) Ltd Executive Management
Effective Date	17 March 2026
Review Frequency	Annual (minimum) plus triggered reviews
Distribution	All staff, contractors, operators, website publication
Classification	Public Document

References

29. [1] Republic of South Africa. (2013). Protection of Personal Information Act 4 of 2013. Government Gazette No. 37067. https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf
30. [2] Information Regulator South Africa. (2025). Protection of Personal Information Act Regulations, as amended April 2025. Government Gazette. https://www.justice.gov.za/inforeg/
31. [3] Republic of South Africa. (2000). Promotion of Access to Information Act 2 of 2000. Government Gazette. https://www.gov.za/sites/default/files/gcis_document/201409/a2-00.pdf
32. [4] Information Regulator South Africa. (2025). POPIA Compliance Framework Guidelines — Enhanced Edition. https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIAComplianceFramework-202506.pdf
33. [5] Republic of South Africa. (2002). Electronic Communications and Transactions Act 25 of 2002. Government Gazette. https://www.gov.za/sites/default/files/gcis_document/201409/a25-02_0.pdf

⚠ Legal Note: Reference [4] links to a document dated June 2025. Please verify this URL is publicly accessible before distributing this policy. If unavailable, remove or update the reference.