MessageIQ

POPIA Compliance Manual

Protection of Personal Information Act, 4 of 2013

Version 1.0	March 2025	Confidential

Prepared by: MessageIQ (Pty) Ltd

Johannesburg, South Africa

Contact: info1@messageiq.co.za | messageiq.co.za

1. Introduction & Scope

MessageIQ (Pty) Ltd ("MessageIQ", "we", "us") provides email, SMS, and WhatsApp campaign management services to small and medium enterprises across South Africa. This manual sets out our commitment to complying with the **Protection of Personal Information Act 4 of 2013 (POPIA)** and the eight Conditions for Lawful Processing.

Who This Manual Covers

This policy applies to all MessageIQ staff, contractors, and third-party processors who collect, store, use, or transmit personal information on behalf of MessageIQ or its clients.

Responsible Party: MessageIQ (Pty) Ltd, Johannesburg, Gauteng

Information Officer: [Name & Title — insert before publishing]

Deputy Information Officer: [Name — insert before publishing]

Contact: info1@messageiq.co.za

Eight POPIA Conditions at a Glance

1. **Accountability** — MessageIQ is responsible for all personal information in its possession.
2. **Processing Limitation** — Data collected only for a specific, lawful purpose.
3. **Purpose Specification** — Purpose communicated at point of collection.
4. **Further Processing Limitation** — No incompatible secondary use without consent.
5. **Information Quality** — Data kept accurate, complete, and up to date.
6. **Openness** — Data subjects informed of their rights and our practices.
7. **Security Safeguards** — Technical and organisational measures to prevent loss or breach.
8. **Data Subject Participation** — Right to access, correct, and delete personal information.

2. Data Processing & Lawful Basis

MessageIQ processes personal information only when at least one lawful ground exists. The table below maps the types of data we process to the applicable legal basis.

Category of Data	Purpose	Lawful Basis
Client contact details (name, email, phone)	Service delivery, invoicing, account management	Contractual necessity
Campaign recipient lists (provided by clients)	Email / SMS / WhatsApp campaign delivery	Client consent or legitimate interest (B2B)
Website visitor data (IP, cookies, analytics)	Performance analytics, security monitoring	Legitimate interest / cookie consent
Billing information	Payment processing	Contractual necessity / legal obligation
Staff HR records	Employment administration, payroll	Legal obligation / contract

Minimum Information Principle: MessageIQ collects only the personal information strictly necessary for the stated purpose. Unnecessary fields are not captured.

Retention Periods: Client data is retained for the duration of the contract plus five (5) years for audit purposes, after which it is securely deleted or anonymised. Campaign recipient data provided by clients is deleted within 30 days of contract termination unless legally required to retain.

3. Email, SMS & WhatsApp Marketing Consent

As a digital marketing platform, consent is the cornerstone of MessageIQ's operations. We distinguish between our own marketing activities and campaigns we execute on behalf of clients.

3.1 MessageIQ's Own Marketing

- Opt-in consent is obtained at the point of contact capture (e.g. website forms, events).
- Every marketing message includes a clear, one-click **unsubscribe** mechanism.
- Unsubscribe requests are processed within **5 business days** and the contact is suppressed permanently.
- We do not send unsolicited commercial communications (SPAM) as defined under POPIA s.69 and the CPA.
- Suppression lists are maintained and checked before every send.

3.2 Client Campaign Obligations

When executing campaigns on behalf of clients, MessageIQ requires the following contractual commitments:

Requirement	MessageIQ Action if Not Met
Client confirms recipient list is consent-based	Campaign withheld pending evidence of consent
Client provides data processing agreement (DPA)	Onboarding suspended until DPA is signed
Recipient data limited to what is needed for the campaign	Excess fields flagged and not imported
Opt-out / unsubscribe mechanism in place	Campaign template modified to include opt-out

3.3 Channel-Specific Consent Notes

Channel	Key Consent Requirement
Email	Express or implied consent. CAN-SPAM / POPIA s.69 opt-out required in footer.
SMS	Express written consent required. WASPA Code compliance. No bulk SMS to purchased lists.
WhatsApp	Opt-in via WhatsApp Business Policy required. Template messages pre-approved by Meta. Users must have initiated c

4. Data Subject Rights & Requests

Under POPIA, every data subject has the following rights. MessageIQ is committed to honouring these rights within the prescribed timeframes.

Right	Description	Response Time
Access (s.23)	Request a copy of personal information held by MessageIQ	30 days
Correction (s.24)	Request that inaccurate or incomplete data be corrected	30 days
Deletion (s.24)	Request deletion of data no longer required or processed unlawfully	30 days
Object (s.11(3))	Object to processing based on legitimate interest	Assessed promptly
Lodge Complaint	Complain to the Information Regulator if rights are not upheld	Regulator's timeline

How to Submit a Request

Data subjects may submit requests by email to **info1@messageiq.co.za** with the subject line "POPIA Data Request". We may request proof of identity before processing any access or deletion request.

Requests will be acknowledged within **3 business days** and resolved within **30 days**. If an extension is required, the data subject will be notified in writing.

The Information Regulator of South Africa can be contacted at: **inforeg@justice.gov.za** | JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001.

5. Data Breach Response Procedures

A personal information breach is any unauthorised access to, loss of, destruction of, or disclosure of personal information. MessageIQ follows a structured four-phase response.

Phase 1: Detect & Contain (0–24 hrs)	Affected systems isolated. Incident logged with timestamp, nature, and scope. Information Officer notified immediately. Temporary access credentials revoked.
Phase 2: Assess (24–48 hrs)	Severity assessed: data type, number of subjects affected, likelihood of harm. Forensic investigation initiated. Legal counsel engaged if criminal activity suspected.
Phase 3: Notify (72 hrs from discovery)	POPIA s.22: Information Regulator notified within 72 hours if the breach is likely to cause harm. Affected data subjects notified as soon as reasonably possible. Notification to include nature of breach, data involved, steps taken, and contact details for further queries.
Phase 4: Remediate & Review	Root cause analysis completed. Technical or procedural controls updated. Staff re-trained if required. Incident report filed and retained for 5 years. PAIA Manual updated if necessary.

Key Contacts for Breach Incidents

Information Regulator: inforeg@justice.gov.za | +27 (0)10 023 5200

MessageIQ Information Officer: info1@messageiq.co.za

SAPS Cybercrime Unit (if criminal activity): 10111

6. Security Safeguards

MessageIQ implements appropriate technical and organisational measures to protect personal information against loss, damage, destruction, or unlawful access.

Technical Controls	Organisational Controls
TLS/SSL encryption in transit	POPIA training for all staff (annual)
AES-256 encryption at rest	Background checks for staff with data access
Role-based access controls (RBAC)	Confidentiality clauses in employment contracts
Multi-factor authentication (MFA)	Signed data processing agreements with vendors
Regular penetration testing	Clean desk & screen lock policy
Automated vulnerability scanning	Vendor due diligence checklist before onboarding
Audit logs retained 12 months	Annual POPIA compliance review

7. Policy Acknowledgement & Review

This manual is reviewed annually or whenever there is a material change in MessageIQ's data processing activities or applicable legislation.

Document Owner: Information Officer, MessageIQ (Pty) Ltd

Next Review Date: March 2026

Version: 1.0 — March 2025

All staff are required to read, understand, and sign this policy. Signed acknowledgement forms are retained in each employee's HR file.

Information Officer Signature

[Name & Title]

Date

20 March 2026