BYC AQUA PAIA and POPIA Compliance Manual

1. Document control

Item	Detail
Document title	PAIA and POPIA Compliance Manual
Company	BYC AQUA SOLUTIONS
Registration number	2026-062054
Version	[Version Number]
Effective date	[Effective Date]
Approval date	[Approval Date]
Approved by	[Board / CEO / Managing Director]
Document owner	[Information Officer]
Next review date	[Review Date]
Status	Approved / Draft / Superseded

1.1 Approval register

Role	Name	Date
Chief Executive / Head of Private Body	Anthony Marlowe	[Date]
Information Officer	Nathaneal Richards	[Date]
Compliance / Legal	Alison Emery	[Date]

1.2 Version history

Version	Date	Summary of changes	Author
[1.0]	[Date]	Initial issue	[Name]
[1.1]	[Date]	[Summary]	[Name]

1.3 Currency and legal review notice

This manual is drafted as current to 27 July 2026. PAIA, POPIA, subordinate regulations, fee schedules, Information Regulator guidance, and sector codes may change. The Company shall check legal requirements, forms, prescribed fees, Regulator guidance, and industry rules periodically and update this manual when required, but in any event no less often than once per calendar year.

2. Executive summary

This document is a combined section 51 PAIA manual and POPIA compliance handbook for BYC Aqua Solutions ("BYC Aqua") and its affiliated companies. PAIA requires private bodies to compile and make available a manual describing access-to-record procedures and record categories, while POPIA requires responsible parties to process personal information lawfully, reasonably, and securely, and gives special attention to direct marketing by electronic communications, including telephone calls. The Company's main area of business involves telephone communications and the Company acknowledges that the Information Regulator's 3 December 2024 direct-marketing guidance expressly states its view that telephone calling is falls under the definition of "electronic communication".

For BYC Aqua the highest-risk compliance areas are typically: lead sourcing, purchased lists, client-supplied campaign lists, consent evidence, customer exception misuse, do-not-contact suppression, call recording, outsourced operator controls, cross-border technology stacks, security safeguards, breach response, employee access controls, and data-subject requests. POPIA also requires documentation of processing operations, data-subject notices, security measures, and rules for objection, access, correction, deletion, and automated decision-making.

3. Company particulars

3.1 Registered details

Item	Detail
Full legal name	**BYC AQUA SOLUTIONS**
Registration number	**2026-062054**
VAT number	**4930258704**
Physical address	**4th Floor, Harbour View Building, 12 Long Street, Cape Town, 8001**
Postal address	**PO Box 4567, Cape Town, 8000**
Main telephone	**021-531 9949**
Email	**nathaneal.richards@byc-aqua.com**
Website	**www.mcisouthafrica.co.za**

3.2 Information Officer and Deputy Information Officers

Role	Name	Title	Email	Telephone	Address
Information Officer/Head of Private Body for POPIA and PAIA purposes	**Nathaneal Richards**	**Reporting Finance Manager**	**nathaneal.richards@byc-aqua.com**	**021-531 9949**	**4th Floor, Harbour View Building, 12 Long Street, Cape Town, 8001**

3.3 Head of private body

For PAIA purposes, the head of a private body is designated with responsibility for the section 51 manual. For POPIA purposes, Information Officer duties include encouraging

lawful processing compliance, handling requests, working with the Regulator, and otherwise ensuring POPIA compliance. Officers may act only after registration with the Regulator, and private bodies must provide for Deputy Information Officers as necessary.

4. Purpose, scope, audience, and legal framework

4.1 Purpose

The purpose of this manual is to:

• comply with section 51 of PAIA;

• set out the Company's POPIA governance and operational controls;

• explain how persons may request access to records and exercise data-subject rights;

• govern the Company's use of personal information in telemarketing, customer service, lead management, quality assurance, and campaign execution; and

• define practical internal rules for staff, managers, clients, operators, and service providers.

4.2 Scope

This manual applies to all processing and records relating to:

• prospects, leads, customers, complainants, suppliers, employees, applicants, visitors, and contractors;

• outbound campaigns, inbound service lines, after-sales contact, collections support, quality assurance, and analytics;

• voice, text, email, CRM, diallers, recordings, tickets, scripts, and campaign reports;

• processing performed by the Company as responsible party or operator; and

• personal information held in South Africa or transferred outside South Africa.

4.3 Legal framework

This manual is based principally on:

• the Constitution of the Republic of South Africa, 1996;

• the Promotion of Access to Information Act 2 of 2000 (PAIA);

• the Protection of Personal Information Act 4 of 2013 (POPIA);

• the Information Regulator's PAIA Guide;

• the Information Regulator's Guidance Note on Direct Marketing dated 3 December 2024;

• the POPIA Regulations and prescribed forms;

• the PAIA Regulations and prescribed forms and fees; and

• all applicable industry codes, contractual obligations, labour laws, and record-retention requirements.

5. Definitions

For this manual:

• **"The Company"** means BYC Aqua Solutions.

• "**Head of Private Body**" means CEO / managing director / equivalent senior officer, unless that person has formally authorised someone else to act as the Information Officer.

• **"PAIA"** means the Promotion of Access to Information Act 2 of 2000.

• **"POPIA"** means the Protection of Personal Information Act 4 of 2013.

• **"Information Officer" / "IO"** means the person responsible under POPIA and PAIA for the duties assigned by law.

• **"Deputy Information Officer" / "DIO"** means a person designated to support or act under delegated powers.

• **"Responsible party"** means the party determining the purpose and means of processing.

• **"Operator"** means a person processing information for a responsible party under contract or mandate.

• **"Data subject"** means the person to whom personal information relates.

• **"Direct marketing"** means approaching a data subject in person, by mail, or by electronic communication for the direct or indirect purpose of promoting goods or services or soliciting a donation.

• **"Nice-to-have data"** means information that is useful operational, explanatory, benchmarking, for or monitoring purposes, but that the organization is not expressly required by applicable legislation or regulations to collect, maintain, publish, submit, or include in a prescribed document.

• **"Electronic communication"** includes, for POPIA section 69 purposes, email, SMS, automatic calling machines, fax, and, in the Regulator's view, telephone calls.

• **"Personal requester"** under PAIA means a requester seeking access to a record containing personal information about the requester.

6. Governance and accountability

6.1 Governance model

The Company adopts a **three-line** compliance model:

Line	Responsibility
Business operations	campaign design, list intake, scripting, quality assurance, frontline execution
Compliance / IO function	legal review, registrations, notices, forms, rights handling, training, monitoring
Internal audit / management oversight	testing, remediation, board reporting, incident review

The Company acknowledges that POPIA places **accountability** on the responsible party and requires the responsible party to ensure the conditions for lawful processing are met when determining the purpose and means of processing and during processing itself.

6.2 Information Officer duties

The Information Officer shall, at minimum:

• encourage compliance with the conditions for lawful processing;

• deal with requests made under POPIA and PAIA;

• work with the Information Regulator during investigations;

• ensure internal compliance and policy maintenance;

• oversee manual publication, training, and monitoring; and

• maintain records, registers, and evidence of compliance.

6.3 Registration and appointment

The Company shall ensure that the Information Officer and appointed Deputy Information Officers are registered with the Information Regulator through the Regulator's portal before taking up their duties.

7. PAIA manual section

7.1 Statutory basis

PAIA gives access to records of private bodies where the requester requires the record for the exercise or protection of a right, complies with the procedural requirements, and no refusal ground applies. The Company acknowledges that Section 51 requires a private body to compile a manual containing specified information, including contact details, the PAIA guide, automatically available records, records available under other laws, and record subjects/categories.

7.2 Availability of the Information Regulator guide

The Information Regulator has published a Guide on How to Use PAIA. The PAIA guide explains how to make requests, identify the correct contact person, understand available remedies, and understand whether a body processes personal information, for what purpose, which data-subject categories are affected, whether cross-border transfers occur, and whether security measures are in place.

The Company will:

• make this manual available at 4th Floor, Harbour View Building, 12 Long Street, Cape Town, 8001

• publish it on BYC-Aqua Solutions/Privacy

• provide a printed copy on request, subject to any lawful reproduction fee; and

• on request, direct requesters to the Information Regulator's PAIA Guide.

7.3 Language and accessibility

The Company acknowledges that private bodies must make a copy of their PAIA manual freely available, although the PAIA Guide indicates private bodies are not required to publish in more than one language or in a specific language; English is recommended, and additional official languages are recommended where the audience warrants it. The Company shall therefore maintain at least an English version and, where commercially and operationally appropriate, isiZulu / isiXhosa / Afrikaans / Sesotho / other versions or accessibility alternatives.

7.4 Categories of records held by the Company

The Company may hold records in the following broad categories:

Subject area	Typical record categories
Corporate governance	incorporation records, shareholder records, board minutes, resolutions, policies
Regulatory and compliance	PAIA manual, POPIA policies, registers, training records, audit reports, incident logs
Finance and tax	invoices, ledgers, bank records, tax submissions, payroll data
Human resources	contracts, leave records, disciplinary records, performance records, recruitment files
Clients and campaigns	MSAs, SOWs, campaign briefs, scripts, quality reports, service levels
Lead and prospect data	list source records, consent records, suppression lists, enrichment logs
Customers and service users	account records, interactions, complaints, tickets, recordings, preferences
Technology and security	access logs, system configs, backups, incident reports, vendor assessments
Legal	litigation holds, legal opinions, claims, settlements, privileged communications
Premises and surveillance	visitor logs, CCTV notices, security access data

These categories are included to facilitate PAIA requests and POPIA documentation obligations. The Company also acknowledges that POPIA requires responsible parties to maintain documentation of processing operations.

7.5 Automatically available records

The Company may make some records available without requiring a formal PAIA request. Under PAIA, automatically available records for private entities are voluntary. Examples may include:

• website terms and privacy notices;

• product/service brochures;

• recruitment notices;

• complaints channels;

• this PAIA/POPIA manual;

• standard client service descriptions; and

• published corporate and contact information. (dirco.gov.za)

7.6 Records available under other legislation

Without limiting the Company's obligations, records may also be created, retained, or disclosed under other legislation applicable to companies, tax, labour, telecommunications, consumer protection, employment equity, health and safety, electronic communications, and financial reporting. Requesters must note that availability under another law depends on that law's own conditions. The Company acknowledges that PAIA itself preserves access routes created by other legislation.

8. PAIA request procedure

8.1 How to submit a request

A requester seeking access to applicable Company records under PAIA must submit the prescribed PAIA Form 2 to the Information Officer or Deputy Information Officer. The request must contain sufficient particulars to identify the requester and the record, state the form of access sought, provide an address in the Republic, identify the right to be exercised or protected, explain why the record is required, and include proof of authority where the request is made on another's behalf.

Submission channels

Email: nathaneal.richards@byc-aqua.com
Physical delivery: 4th Floor, Harbour View Building, 12 Long Street, Cape Town, 8001
Post: PO Box 4567, Cape Town, 8000

8.2 PAIA process flow

Step	Requirement
1. Submission	requester submits **Form 2** with supporting detail
2. Fee check	request fee may be payable for non-personal requesters
3. Validation	IO/DIO checks scope, clarity, jurisdiction, and identity
4. Search and review	identify records, consult business, check refusal grounds
5. Third-party notice	issue where sections 63, 64, 65, or 69 may be implicated
6. Decision	grant, partially grant, or refuse with reasons
7. Access / outcome notice	notify via **Form 3** and collect lawful access fees if applicable
8. Complaint / court remedy	requester may complain to the Regulator and/or approach court, as applicable

8.3 Fees

The Company will require a prescribed request fee from a requester other than a personal requester (a third-party requester) before processing the request. If search and preparation exceed the prescribed threshold, the Company may require the requester to pay a deposit of up to one-third of the access fee that would be payable if access is granted. Current publicly referenced PAIA material indicates a private-body request fee of R140.00, but the

Company shall always verify the then-permitted prescribed schedule before invoicing. That schedule can be located at PAIA-Fees-structure.pdf.

8.4 Timelines

The Company must decide the request within the period prescribed by PAIA, subject to lawful extension. If third-party notification is required, that process must be handled within the statutory framework. The Company considering a request that may affect specified third-party interests must take reasonable steps to notify the third party within 21 days after receipt of the request.

8.5 Grounds for refusal

The Company may be required or entitled to decline the request on grounds including:

• privacy of a third party who is a natural person;

• commercial information of a third party;

• certain confidential information of a third party;

• safety of individuals and protection of property;

• legally privileged records;

• commercial information of the private body;

• research information of a third party or the private body; and

• manifestly frivolous or vexatious requests or unreasonable diversion of resources, where applicable under PAIA's framework.

Where only part of a record is exempt, the Company shall provide the remainder if reasonably severable. POPIA likewise requires partial disclosure where only part of requested personal information may or must be refused.

8.6 Remedies, complaints, and court applications

For private bodies, there is generally no internal appeal equivalent to the public-body internal appeal mechanism. A requester dissatisfied with a decision may complain to the Information Regulator and/or apply to court for appropriate relief, subject to PAIA's requirements and time periods. Should a requester submit a complaint to the Company, the Information Officer shall consult with the Company's Chief Compliance Officer to determine how to proceed further.

9. POPIA compliance framework

9.1 The eight conditions

The Company adopts controls aligned to POPIA's eight conditions:

Condition	Core requirement	Company control theme
1. Accountability	responsible party must ensure compliance	governance, roles, oversight
2. Processing limitation	lawful, reasonable, minimal processing	legal basis, consent, minimality
3. Purpose specification	specific purpose and retention limits	campaign purpose controls, retention schedule
4. Further processing limitation	compatibility with original purpose	lead sharing/list use controls
5. Information quality	complete, accurate, not misleading	data hygiene, QA, source validation
6. Openness	documentation and notices	RoPA, privacy notices, scripts
7. Security safeguards	appropriate technical and organisational measures	access control, encryption, incident response
8. Data-subject participation	access, correction, objection	request workflows and forms

These conditions are reflected in Chapter 3 of POPIA.

9.2 Processing inventory / record of processing

The Company shall maintain a record of processing activities that includes at least:

- processing activity name;
- business owner;
- responsible party / operator role;
- categories of data subjects;
- categories of personal information;
- purpose;
- lawful basis under section 11;
- source of information;
- recipients;
- systems used;
- retention period;
- security classification;
- cross-border transfers;

• direct-marketing status;

• whether special personal information, children's data, profiling, or automated decision-making is involved.

9.3 Categories of data subjects

Typical data-subject categories include:

• leads and prospects;

• current customers;

• former customers;

• inbound callers and complainants;

• client representatives;

• employees and contractors;

• job applicants;

• visitors and CCTV subjects; and

• suppliers and service-provider personnel.

9.4 Categories of personal information

Typical categories include:

• identifiers and contact details;

• demographic and preference data;

• communication records and call notes;

• call recordings and transcripts;

• account and contract data;

• complaint histories;

• employee and applicant records;

• device, log, and access data;

• biometric data where used, such as voice biometrics; and

• special personal information where exceptionally processed. Voice biometrics is treated here as biometric information, which is a category of special personal information; that classification is an inference from POPIA's treatment of biometric information.

10. Lawful basis, minimality, and collection

10.1 Lawful basis under section 11

The Company shall process personal information only where a lawful basis exists for doing so, including consent, contract necessity, legal obligation, legitimate interest of the data subject, public-law duty where relevant, or legitimate interests of the responsible party or a third party. The Company acknowledges that the responsible party bears the burden of proof for consent, and that consent may be withdrawn at any time.

10.2 Minimality

The Company shall collect and use only information that is adequate, relevant, and not excessive for the stated purpose. Campaign fields, dialler imports, and CRM screens shall therefore be designed so that staff do not collect "nice to have" data without a documented need.

10.3 Direct collection and exceptions

Personal information must generally be collected directly from the data subject, unless a lawful exception applies, such as public-record sourcing, consent to third-party sourcing, no prejudice to legitimate interests, legal necessity, or impracticability in defined circumstances. For purchased lists and data-broker leads, the Company shall document which section 12 exception is relied on and why it applies.

10.4 Collection notices

At or before collection of the personal information, or as soon as reasonably practicable, the Company must provide the information required by section 18, including what is collected, source (if not from the data subject themselves), Company identity and address, purpose, whether supply is voluntary or mandatory, consequences of failure, legal authority where relevant, intended cross-border transfer, recipients, categories of information, and rights of access and rectification.

11. Direct marketing policy for telemarketing and electronic communications

11.1 Core rule

The Company acknowledges that POPIA section 69 prohibits processing personal information for direct marketing by electronic communication unless the data subject consents or is, subject to section 69(3), an existing customer of the responsible party. The Information Regulator's guidance states that telephone calls are electronic communication. The Company therefore designs its outbound telemarketing on the basis that routine sales calls fall within section 69.

11.2 One-time consent request rule

Where the data subject is not a customer, the Company shall approach the person only once to request consent, and only if the person has not previously withheld consent. That first communication must be a consent request only, not an attempt to obtain their business.

11.3 Prescribed consent process

The data subject's consent must be requested in the prescribed manner and form. Pursuant to the Information Regulator's guidance, which states that the responsible party should use Form 4 or a substantially similar form ("the form"), free of charge and readily accessible, and that the form should identify the goods or services and permit the data subject to choose the communication method, the Company will make the form available online. Where consent is requested by telephone, the Company employee making the call will read out the contents of Form 4 and the call shall be recorded.

11.4 Existing-customer exception

The Company will market by electronic communication to an existing customer only if all of the following apply:

• the Company obtained the customer's contact details in the context of a sale of a product or service;

• marketing relates to the Company's own similar products or services; and

• the customer had a reasonable opportunity to object, free of charge and without unnecessary formality, both at collection and on each marketing communication if they did not initially refuse. The Company affirms that silence on the subject is not consent.

11.5 Mandatory content in every direct-marketing communication

The Company shall ensure that all of its direct-marketing communication will contain:

• the identity of the sender or the person on whose behalf the message is sent; and

• an address or contact detail enabling the recipient to request that communications cease.

Operational rule: all outbound calls, SMS, email, and messaging scripts must clearly identify BYC Aqua, identify the client principal if relevant, and offer an immediate no-cost opt-out.

11.6 Caller identification, scripts, and call conduct

Because section 69(4) requires identity and a cease-contact channel, and because call centres rely on script control to evidence compliance, the Company shall ensure that every outbound call script includes:

1. caller and company identity;
2. client identity where acting for a client;
3. source explanation where appropriate;
4. purpose of the call;
5. consent or customer-basis wording;
6. free opt-out wording;
7. suppression coding outcome; and
8. record-keeping of result and timestamp.

11.7 Suppression and do-not-contact lists

Pursuant to the Regulator's guidance, the Company shall compile and maintain a database of persons who have withheld consent and those who have objected, and shall not contact those objecting persons again through the relevant channel. The Company shall maintain a central suppression register across all campaign systems and ensure client-supplied lists are screened against it before loading.

11.8 Consumer Protection Act pre-emptive block

The Company acknowledges that the Regulator's guidance makes clear that even where a person has not registered a pre-emptive block, POPIA section 69 still applies and a responsible party cannot rely on the absence of a block as permission to send unsolicited electronic direct marketing. The Company shall put processes in place to ensure compliance with this directive.

12. Lead generation, list acquisition, and campaign data sourcing

12.1 Lead generation

The Company acknowledges that the Information Regulator's guidance states that lead generation is a direct-marketing practice involving collection of personal information and that sharing contact details with other responsible parties, or selling/renting lists, is treated as further processing that must comply with section 15 and also with section 18 notice obligations.

12.2 Purchased lists and data brokers

The Company shall not purchase, rent, import, or use a prospect list unless the campaign owner and Information Officer approve a written intake record confirming:

• source identity and chain of custody;

• whether the Company will act as responsible party or operator;

• section 12 collection basis for non-direct collection;

• section 11 lawful basis;

• section 15 further-processing compatibility;

• section 18 notice plan;

• section 69 consent status for telemarketing/electronic contact;

• suppression screening;

• cross-border hosting or transfer implications; and

• client contractual indemnities and audit rights.

12.3 Client-supplied campaign lists

Where a client supplies a campaign list, the Company shall ensure that:

• the contract allocates whether the client is the responsible party and the Company the operator, or whether the Company is a separate responsible party for any independent use;

• the client must warrant lawful collection, notice, and section 69 compliance for the intended channel;

• the Company must still apply its own suppression, security, and rights-handling controls; and

• the Company may reject or quarantine a list that appears unlawful, unclear, stale, or incompatible with the stated purpose. These are governance controls inferred from POPIA's allocation of accountability, operator duties, and section 21 contract requirements.

13. Responsible party / operator allocation and contractual controls

13.1 Allocation principles

The Company acknowledges that a party that determines the purpose and means of processing is the responsible party. A service provider processing for another under instruction is an operator. Under POPIA's framework, in outsourced call-centre arrangements, the Company acknowledges that the allocation should be documented per campaign because the Company may be an operator for client data but a responsible party for its own HR, telephony, QA, security, and internal analytics activities.

13.2 Mandatory operator contract terms

Where the Company appoints or acts through an operator, the written agreement shall address at least:

• processing only on documented instructions;

• confidentiality;

• security measures aligned to section 19;

• immediate breach notification to the responsible party;

• subcontracting restrictions;

• return or deletion at end of service;

• audit and evidence rights;

• data-subject request cooperation;

• cross-border restrictions; and

• incident escalation. POPIA requires a written contract to ensure the operator establishes and maintains section 19 security measures and requires operators to notify the responsible party immediately if unauthorised access or acquisition is reasonably suspected.

14. Call recording, monitoring, QA, voice biometrics, and surveillance

14.1 Call recording

The Company may record calls for lawful purposes including quality assurance, training, complaint handling, contract evidence, fraud prevention, security, and consent evidence. Where a telephone call is used to obtain section 69 consent, the Company acknowledges that the Regulator's guidance states that the call must be recorded. For all other recordings, the Company will provide an appropriate notice at the start of the call or through an equivalent prior notice mechanism, consistent with section 18 openness duties.

14.2 Monitoring and QA

The Company acknowledges that under the applicable rules and legal guidance, monitoring and QA must be proportionate, role-based, and tied to defined business purposes. The Company agrees that access to recordings, transcripts, and scorecards must be limited to authorised personnel, retained in line with the retention schedule, and logged in order to implement POPIA's security and minimality requirements.

14.3 Voice biometrics

The Company acknowledges that under POPIA, the use of voice biometrics should be treated as processing of biometric information, which POPIA classifies as **"**special personal information"**.** Accordingly, the Company will not deploy voice-biometric authentication, fraud-scoring, or matching unless there is a documented lawful basis, necessity analysis, transparency notice, strict access control, retention limit, and legal review of whether authorisation or further safeguards are required.

14.4 CCTV and physical surveillance

Where Company premises use CCTV, visitor access controls, or audio surveillance, the Company shall display clear notices and include the processing in its records of processing and retention schedule, with access restricted to authorised security, compliance, or management personnel.

14.5 Inbound calls

Inbound customer-service calls often involve identity verification, complaint handling, contract performance, and call recording. The Company shall ensure that inbound scripts include privacy and recording notices where applicable, and that staff do not use inbound interactions as a backdoor for unrelated direct marketing unless a lawful basis and, where section 69 applies, the required consent/customer basis exists.

15. Special personal information and children's information

15.1 Special personal information

The Company acknowledges that POPIA prohibits processing of special personal information, including information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life, and biometric information, unless an exception or authorisation applies. The Company's default rule is that the Company does not collect or use special personal information for telemarketing or routine call-centre operations unless specifically approved by the Information Officer and legally justified.

15.2 Children's information

The Company acknowledges that POPIA prohibits processing personal information concerning a child, subject to section 35. The Information Regulator's children's guidance explains that authorisation may be granted if processing is in the public interest and appropriate safeguards exist. The Company will always avoid intentionally marketing to children and shall escalate any child-data processing for legal and compliance review before collection or use.

16. Employee and applicant data

The Company processes employee and applicant data for recruitment, contract administration, payroll, benefits, performance, security, disciplinary management, scheduling, and statutory compliance. The Company acknowledges that under the applicable rules, HR processing must still comply with the section 11 lawful-basis framework, section 18 notice requirements, section 19 security safeguards, and rights-handling rules. Where health information is processed, the Company acknowledges that the 6 March 2026 health-information regulations reinforce confidentiality, disposal controls, and cross-border restrictions for covered responsible parties and operators; while those regulations are sector-specific, they are also a useful benchmark for employer-side health-data handling.

17. Data-subject rights and request procedures

17.1 Access

A data subject may request confirmation, free of charge, whether the Company holds personal information about them, and may request the record or a description of that information, including identities or categories of third parties who have had access, within a reasonable time, in a reasonable format, and generally understandable form.

17.2 Correction, deletion, and destruction

A data subject may request correction or deletion of inaccurate, irrelevant, excessive, outdated, incomplete, misleading, or unlawfully obtained personal information, or destruction/deletion of records the Company is no longer authorised to retain. The Company shall respond as soon as reasonably practicable and either correct, delete, provide credible evidence, or annotate the disputed record where agreement is not reached and the data subject requests annotation. The prescribed request route under which such a request can be made is POPIA Form 2. Any other forms or formats of such a request shall be reviewed and assessed by Compliance for further direction.

17.3 Objection

A data subject may object at any time to direct marketing other than unsolicited electronic communications under section 11(3), and processing must stop after objection. The prescribed route is POPIA Form 1 or a substantially similar accessible process. For electronic direct marketing under section 69, the Company shall implement objections and withdrawals of consent immediately through suppression controls.

17.4 Complaint handling

Complaints about alleged POPIA interference may be escalated to the Information Regulator using the prescribed complaint form. In the event that the Company receives POPIA Form 5 or PAIA Form 5 complaint forms, the Company shall immediately direct those to the Chief Compliance Officer for further handling.

18. Automated decision-making, profiling, and analytics

The Company acknowledges that the Regulator’s direct-marketing guidance warns that lead generation and profiling can involve automated processes and must comply with POPIA and that POPIA provides that a data subject may not be subject to a decision with legal consequences, or one affecting the person to a substantial degree, if that decision is based solely on automated processing intended to profile the person, subject to limited exceptions and safeguards. The Company shall ensure that where automated decision-making is used, if at all, appropriate measures will be in place to ensure that the Company can provide sufficient information about the underlying logic upon request.

Company rule: do not use fully automated scoring, suppression, vulnerability ranking, or campaign eligibility logic that materially affects a person without:

• legal review;

• documented purpose and lawful basis;

• human oversight where required;

• explainability notes;

• challenge/escalation route; and

• retention and testing controls.

19. Information quality, retention, and deletion

The Company shall take reasonably practicable steps to ensure information is complete, accurate, not misleading, and updated where necessary, having regard to purpose. Retention shall be linked to purpose and legal requirements, and records must be destroyed or de-identified when no longer authorised to be retained, subject to litigation holds, statutory periods, and contractual obligations.

19.1 Retention schedule framework

Record type	Indicative rule	Owner
Consent records / Form 4 evidence	retain while relied on and for dispute limitation period thereafter	**Compliance / Campaign Ops**
Suppression records	retain as long as needed to honour objection/withdrawal	**Compliance**
Routine call recordings	retain per published schedule and purpose	**Operations / IT**
Complaints and escalations	retain through resolution plus legal hold period	**Customer Care / Legal**
HR records	retain per labour, tax, and employment requirements	**HR**
Client campaign files	retain per contract, legal need, and dispute period	**Account Management**

The Company shall maintain the detailed retention matrix separately and review it periodically.

20. Security safeguards and incident response

20.1 Security baseline

The Company shall secure the integrity and confidentiality of personal information by taking appropriate, reasonable technical and organisational measures to prevent loss, damage, unauthorised destruction, unlawful access, or unlawful processing. The Company will identify reasonably foreseeable risks, establish safeguards, verify implementation, and update safeguards as risks change.

20.2 Minimum controls

The Company shall maintain operation measures to implement Section 19 controls including:

- role-based access and MFA where appropriate;
- least-privilege permissions;
- endpoint protection;
- encryption in transit and at rest where appropriate;
- dialler/CRM segregation;
- audit logging;
- vendor due diligence;
- secure disposal;
- clean-desk and remote-work controls;
- backup and recovery testing; and
- periodic access recertification.

20.3 Security compromises

Where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, the Company must notify the Information Regulator and, subject to POPIA, the affected data subject, as soon as reasonably possible. Operators must notify the responsible party immediately where they reasonably suspect unauthorised access or acquisition and, with the assistance of Compliance and Legal, shall review and issue the section 22 security-compromise notification for such instances.

20.4 Incident response workflow

1. detect and contain;

2. preserve evidence;

3. classify data and affected population;

4. determine responsible party/operator roles;

5. assess whether notification thresholds are met;

6. notify Regulator and data subjects where required;

7. remediate;

8. record lessons learned/remediation;

9. update controls and training.

21. Cross-border transfers

The Company acknowledges that a responsible party in South Africa may not transfer personal information to a foreign recipient unless one of section 72's grounds applies, including adequate protection under law, binding corporate rules, or binding agreement; the data subject's consent; contractual necessity; or benefit-of-data-subject circumstances. The Company shall therefore map all cloud telephony, CRM, analytics, QA, AI transcription, and support tools that store or access personal information outside South Africa.

Operational rule: no new foreign-hosted call-centre or martech platform may be onboarded without a documented cross-border assessment and contract review.

22. Training, monitoring, and assurance

The Company shall run a compliance programme including:

• induction training for all staff;

• enhanced training for agents, QA, team leaders, sales managers, HR, IT, and procurement;

• annual refresher training;

• script approvals and spot checks;

• list-intake approvals;

• suppression testing;

• DSAR and PAIA drills;

• breach tabletop exercises; and

• quarterly compliance reporting to management. The Company acknowledges that these controls give practical effect to POPIA accountability, security, documentation, and rights-participation duties.

23. Internal registers and mandatory records

The Information Officer shall maintain at least the following registers:

Register	Required content
PAIA request register	date received, requester, record sought, fee status, outcome, timelines
POPIA rights register	access, objection, correction, deletion, complaint requests
Consent register	source, method, wording version, timestamp, channel, evidence location
Suppression register	objection/withdrawal date, channel, source, client restrictions
Processing inventory	all processing activities and legal bases
Operator register	vendors, role, contract, location, due diligence
Cross-border register	recipient country, legal basis, contract safeguard
Incident register	event facts, impacted systems, notices, remediation
Training register	attendees, modules, test scores, remediation
Record retention register	classes, retention periods, disposal actions

These registers support PAIA section 51 content and POPIA documentation, notice, security, and participation obligations.

24. Standard operating rules for telemarketing campaigns

Before any campaign goes live, the Centre Manager and Information Officer must confirm that:

• campaign purpose is documented;

• responsible party/operator role is allocated;

• list source is known;

• lawful basis is documented;

• section 69 analysis is completed for phone/SMS/email/auto-dial use;

• Form 4 process is configured if non-customer consent is required;

• scripts include identity and cease-contact details;

• suppression screening is complete;

• recording and notice requirements are configured;

• cross-border tools are assessed;

• retention and deletion rules are assigned; and

• complaints and escalation routes are operational.

25. Adoption statement

This manual is adopted by **BYC AQUA** with effect from **[Effective Date]**. All directors, employees, agents, contractors, and relevant operators shall comply with it. Non-compliance may result in disciplinary action, contractual remedies, access restrictions, or legal escalation.

Approved by: [Name / Title] Date: [Approval Date] Version: [Version]