Revision: v4 — 18 August 2026

AQRATE POPIA COMPLIANCE DISCLOSURE

Purpose of this document

This document explains AQRate's policies and procedures for compliance with the Protection of Personal Information Act, 4 of 2013 ("POPIA"), and for maintaining client confidentiality.

The content is structured around the eight conditions for lawful processing under POPIA. Text in grey/black provides legislative background; text in blue sets out AQRate's response. Principle 7 (Security Safeguards) has been expanded to cover the full scope of sections 19 to 22, including the treatment of information processed by an operator and the notification of security compromises.

Principle 1: Accountability

This principle contemplates the assigning of responsibility by organisations for overseeing compliance with the Act.

- Responsibility for data governance lies with the appointed Information Officer at AQRate. Unless otherwise designated, this responsibility lies with the CEO.
- Where information is categorised by type, a suitable manager may be appointed as deputy Information Officer for that sphere of responsibility.
- Systems used for monitoring compliance are configured to notify the appropriate Information Officer of non-compliance events for investigation.
- The current Information Officer and deputy Information Officer(s), together with their registration status with the Information Regulator, are recorded in [internal register / PM-33].

Principle 2: Processing Limitation

This principle requires that personal information may only be processed in a fair and lawful manner.

- AQRate does not process information for any purpose other than the commercial engagement contracted, continued servicing of the client, and applicable legislative or regulatory requirements.

Principle 3: Purpose Specification

This principle determines the scope within which personal information may be processed.

- AQRate discloses to clients: the information collected, the purpose of collection, and the processing to be carried out.
- The most extensive of these disclosures occur during information sessions held prior to the majority of data collection.
- These disclosures are supplemented, for website visitors, by AQRate's website Privacy Notice, which independently satisfies sections 18 and 19 of POPIA.

Principle 4: Further Processing Limitation

Processing of personal information may only occur insofar as necessary for the purposes for which it was obtained.

- AQRate only processes information to the extent required to complete and record verification under the B-BBEE Codes of Good Practice and applicable law, including regulations imposed by SANAS to maintain accreditation.
- Limited processing of non-verification information is conducted for continued client servicing.

Principle 5: Information Quality

Organisations must take reasonable steps to ensure personal information is complete, accurate, not misleading, and updated where necessary.

- AQRate's verification service is itself a quality-control process over the information supplied.
- Collection, processing, and evaluation activities are audit-trailed against AQRate's business systems to preserve data integrity and quality.

Principle 6: Openness

This principle requires processing to occur in a fair and transparent manner, made known to the data subject.

- During contracting and client information sessions, all data collection and processing activities are shared with the client.
- It is made clear which information will be collected and by what means.
- AQRate's website Privacy Notice provides equivalent openness disclosures to website visitors and prospective clients, consistent with sections 18 and 19 of POPIA.

Principle 7: Security Safeguards

Condition 7 (sections 19 to 22 of POPIA) requires that personal information be kept secure against loss, unauthorised access, interference, modification, destruction, or disclosure. It covers the security measures a responsible party must take (s19), the treatment of information processed by an operator (s20-21), and the notification of security compromises (s22).

Security measures (section 19)

- All AQRate staff, contractors, and service providers are identified with unique credentials for accessing AQRate systems.
- Activity is audit-trailed against unique credentials, so far as each system allows.
- Monitoring and notification rules alert suitable parties to high-risk activity, including removal of data from company systems, improper use of credentials, and DLP analytics changes.
- Active and passive security measures monitor and mitigate external threats to AQRate systems and data.

- Data at rest and in internal transfer is protected with end-to-end encryption via Microsoft Office 365 infrastructure.
- Clients are directed to submit sensitive data via SharePoint folders rather than email, to reduce email-borne security risk.
- Certificates are issued through a tightly controlled, audit-trailed system, enabling AQRate to certify document authenticity and the identity of issuing users.
- Systems infrastructure is independently reviewed on a scheduled and event-triggered basis (e.g. employee take-on, equipment decommissioning, server provider changes, security alerts, annual configuration review).
- Staff with privileged access to confidential information are monitored via activity and DLP software to guard against insider threats.
- In line with section 19(2), AQRate identifies reasonably foreseeable internal and external risks to personal information in its possession or under its control, establishes and maintains safeguards against those risks, verifies that the safeguards are effectively implemented, and updates them in response to new risks or deficiencies. This process is governed by AQRate's Risk Management Policy (HR-27) and Information Security Policy (HR-25).

Information processed by an operator (sections 20 and 21)

- Where AQRate engages an operator or a person acting under its authority to process personal information, that party processes the information only with AQRate's knowledge or authorisation and is required to treat it as confidential (section 20).
- In accordance with section 21, such processing is subject to a written contract requiring the operator to establish and maintain security measures consistent with those set out above.
- AQRate's supplier due diligence and contracting processes give effect to these requirements for the third-party service providers that support its operations.

Notification of security compromises (section 22)

- Where there are reasonable grounds to believe that personal information in AQRate's possession or under its control has been accessed or acquired by an unauthorised person, AQRate will notify the Information Regulator as soon as reasonably possible after discovery of the compromise, in accordance with section 22 of POPIA.
- AQRate will similarly notify affected data subjects immediately or no later than 24 hours from the reasonable belief or discovery of the incident, unless a competent public body responsible for the prevention, detection, or investigation of offences, or the Regulator, determines that notification would impede a criminal investigation.
- Notification to data subjects will be made in one of the forms permitted by section 22, and will include sufficient information to allow the data subject to take protective measures — including a description of the possible consequences of the compromise, the measures AQRate has taken or intends to take, a

recommendation of protective steps the data subject can take, and, if known, the identity of the unauthorised party.

- This process is governed internally by AQRate's Incident Management Policy (HR-23), which sets out escalation paths, timelines, and roles for incident response, including the point at which the Information Officer is engaged for regulatory notification.

Principle 8: Data Subject Participation

This principle empowers data subjects to access, correct, or request deletion of personal information held about them.

- Clients may request an inventory of information AQRate holds about them, and request correction or removal, save where this conflicts with another legal or regulatory data-governance requirement.
- SANAS Requirement R47 obliges B-BBEE Rating Agencies to retain verification records for the current Accreditation Cycle plus the immediately preceding full cycle. As a single cycle is 4 years, this results in a retention obligation of up to 8 years for verification records.
- This regulatory retention requirement takes precedence over a data subject's right to request deletion during that period; appropriate security safeguards, as described under Principle 7, continue to apply throughout the retention period.
- Requests should be directed to the Information Officer per the contact details in [Section/Annexure reference].