AQRate POPIA Compliance Disclosure

Purpose of this document:

This document serves to explain AQRate's policies and procedures in relation to compliance with the Protection of Personal Information act in terms of South African law.

It also serves to explain AQRate's policies and procedures in terms of maintaining high levels of customer confidentiality.

The information is broken down into the 8 conditions inherent in the legislation. Text in grey or black provides background information, while text in blue indicates AQRate's response.

- Principle 1: Accountability

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

  - Responsibility for data governance lies with the appointed information officer at AQRate. This responsibility, unless otherwise defined, lies with the CEO.
  - In some cases, information is categorized by type, and a suitable manager is appointed to act as the deputy information officer for that sphere of responsibility.
  - Systems used for monitoring compliance are configured to notify the appropriate information officer of any non-compliance events for investigation.

- Principle 2: Processing Limitation

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

  - In accordance with the act, AQRate does not process information for any other purposes, other than the commercial engagement contracted, the continued servicing of the client and the legislative and regulatory requirements.

- Principle 3: Purpose Specification

  The principle of Purpose Specification helps to determine the scope within which personal information may be processed by an organisation.

  - AQRate provides a variety of disclosures to the client, as to:
    - The information collected
    - The purpose of its collection
    - The processing that will be carried out on it.
  - The most extensive of these client engagements are the information sessions that occur prior to the majority of the information collection.

- Principle 4: Further Processing Limitation

  Once an organisation has identified and obtained consent for specific, legitimate and explicitly defined purposes, the processing of such personal information may only occur insofar as it is necessary for the fulfilment of those purposes.

  - AQRate only processes information in so far as is required to complete and record the verification as per the BEE legislation and other applicable laws within the Republic of South Africa, including regulations imposed to maintain accreditation with the accreditation body, SANAS (South African National Accreditation System)
  - Limited processing of non-verification information is conducted for continued servicing of the client.

- Principle 5: Information Quality

  Clause 16 of the Bill sets out, in general terms, the responsibility of organisations to ensure and maintain the quality of the personal information that they process.

  - AQRate's service is core to the maintenance of the quality of information.
  - The processes governing collection, processing and evaluation of information are audit trailed against all business systems to ensure that integrity and quality of information are maintained.

- Principle 6: Openness

  The sixth principle of "Openness" is linked directly to an organisation's duty to process information in a fair and transparent manner.

  - During contracting and client information sessions, all data collection and processing activities are shared with the client.
  - It is made clear through those processes which information would be collected and the manner of collection.

- Principle 7: Security Safeguards

  The underlying theme of Principle 7 is that all personal information should be kept secure against the risk of loss, unauthorised access, interference, modification, destruction or disclosure

  - AQRate employs a multitude of measures, in line with established best practice. Including but not limited to:
    - All AQRate staff, contractors and service provider access are identified with unique credentials for accessing AQRate systems
    - All activity, so far as possible within the scope of each system, is audit trailed against the unique credentials.
    - Monitoring and notification rules are configured, to notify suitable parties to respond to high-risk activities, for example:
      - Removal of data from company systems
      - Improper use of user credentials
      - Data loss prevention (DLP) analytics changes
    - Active and passive security measures to monitor and mitigate against external threats to AQRate systems and data.

- Data at rest and in internal transfer are protected with end-to-end encryption, utilizing Microsoft's Office 365 infrastructure.
- AQRate recommends clients submit sensitive data via Sharepoint folders, in order to avoid the security weaknesses inherent in email communications.
- AQRate certificates are issued through a tightly controlled and audit-trailed system, allowing AQRate to certify the authenticity of any issued documents, as well as the users involved in its issuing.
- AQRate systems infrastructure is independently reviewed on a regular basis, including schedule-based checks, as well as event-based triggers. For example
  - Employee take-on and maintenance
  - Equipment decommissioning
  - Server provider changes
  - Data monitoring events or security alerts
  - Annual configuration review
  - AQRate staff with privileged access to confidential information are monitored with activity and data loss prevention software, to secure against insider threats.

- Principle 8: Data Subject Participation

  Principle 8 empowers individuals to access and/or request the correction or deletion of any personal information held about them that may be inaccurate, misleading or outdated.

  - As per the POPIA requirements, clients may request an inventory of information held by AQRate, as well as request removal or correction of information, in so far it does not contradict with any other legal or regulatory requirements for data governance. This would include regulations imposed by the accreditation body which govern the maintenance of AQRate's accreditation as a B-BBEE Ratings Agency. SANAS, under R47 requires B-BBEE Ratings Agencies to retain all records as required by the relevant Accreditation Standard at least for the duration of the current Accreditation Cycle plus the previous full Accreditation Cycle. A single Accreditation Cycle is 4 years, which results in the requirement to retain records used for the audit and verification process of all verified Measured Entities for a period of up to 8 years in order to maintain accreditation as a B-BBEE Ratings Agency. As a regulatory requirement, this supersedes the right of the data subject to request the deletion of personal information, however measures are in place to ensure the protection of such information, as required by POPIA.