

DATA PROTECTION COMPLIANCE FRAMEWORK

AquaSee Networks Limited - Internal Compliance Document

Policy ID: AQUA-DP-001 | Version: 1.0 | Effective: 15 January 2026

Status: INTERNAL COMPLIANCE DOCUMENT. Prepared by: CEO. This Framework is binding on all personnel and systems that process personal data on behalf of AquaSee Networks Limited.

1. PURPOSE, SCOPE & GOVERNANCE INTEGRATION

This Data Protection Compliance Framework ("the Framework") formalizes AquaSee Networks Limited's commitment to the highest standards of data privacy and security. It operationalizes our obligations under Kenya's Data Protection Act, 2019 ("DPA") and aligns with the EU General Data Protection Regulation ("GDPR") for international operations and investor assurance purposes.

This Framework integrates with the following existing AquaSee governance documents:

Related Policy	Integration Point
Trade Secret Protection Policy (AQUA-TSP-001)	Data security controls align with and reinforce IP protection obligations.
Terms of Service & Privacy Policy (external)	This Framework internally enforces the external-facing commitments made to Platform users.
Employment Agreement (AQUA-KEA)	Individual accountability for data handling is embedded in employment contracts.
NDA (AQUA-NDA-001)	Confidentiality of personal data processed by contractors is governed jointly by this Framework and the NDA.

Scope: This Framework applies to all processing of personal data by AquaSee Networks Limited, whether as a Data Controller (determining purpose and means) or Data Processor (acting on client instructions) across all operational territories.

2. KENYA DATA PROTECTION ACT (DPA) 2019 COMPLIANCE

2.1 Core Obligations & ODPC Registration

AquaSee is obligated to register with the Office of the Data Protection Commissioner (ODPC) based on our processing activities, specifically, the systematic monitoring of environmental data correlated with commercial farm operations. The Compliance Officer (CEO, pending dedicated appointment) is responsible for completing registration via the ODPC electronic portal.

Our data processing activities are anchored in the DPA's eight core principles:

DPA Principle	AquaSee Implementation
Lawfulness, Fairness & Transparency	All processing has a documented lawful basis. Privacy Policy is publicly available on the Platform.
Purpose Limitation	Data collected only for specified, explicit, and legitimate purposes. Not processed incompatibly with stated purpose.
Data Minimization	Only data strictly necessary for the agricultural monitoring function is collected. No biometric or sensitive personal data.
Accuracy	Sensor data is timestamped and traceable. User account data correction mechanism is available.
Storage Limitation	Retention schedules are defined per category. Customer data deleted or anonymized upon contract termination.
Integrity & Confidentiality	AES-128 encryption in transit and at rest. Role-based access controls. Annual penetration testing.
Accountability	This Framework, training records, DPIA logs, and breach register constitute the accountability documentation.

2.2 Data Subject Rights Management

Data Subject Right (DPA 2019)	AquaSee Response Process & Timeline
Right to be Informed	Fulfilled via publicly available Privacy Policy and in-Platform notices at point of data collection.
Right of Access (SAR)	Subject Access Request procedure. Response within 7 days of request verification. SAR form available on Platform.
Right to Rectification	Process to correct inaccurate data. Action within 14 days of verified request.
Right to Erasure	Deletion upon withdrawal of consent where no overriding legitimate interest exists. Confirmed in writing to data subject.
Right to Restrict Processing	Temporary processing halt under dispute. Customer notified within 3 business days.
Right to Data Portability	Structured, machine-readable export of customer data upon request. Available via Platform export function.
Right to Object	Objection to processing for direct marketing: immediate effect. Other objections assessed within 14 days.

3. DATA CATEGORIES & CLASSIFICATION

Data Category	Examples	Classification & Controls
Environmental Sensor Data	Temperature, pH, turbidity, dissolved oxygen readings	BUSINESS DATA: encrypted in transit and at rest; not personal data per se; aggregated for anonymization.
Customer Account Data	Name, email, organization, contact number	PERSONAL DATA: DPA compliant; lawful basis: contract; retention: life of contract + 3 years.
Platform Usage Data	Login timestamps, feature interactions, API calls	PERSONAL DATA: anonymized after 12 months; used only for service improvement.
Payment Data	Billing name, organization, payment reference	FINANCIAL DATA: processed via PCI-DSS compliant third-party payment gateway; not stored on AquaSee servers.
Employee HR Data	Names, IDs, salaries, health information	SENSITIVE PERSONAL DATA: restricted access; CEO only; encrypted storage.

4. TECHNICAL & ORGANISATIONAL SECURITY MEASURES

4.1 Technical Controls

- Encryption: AES-128 minimum for all data in transit (TLS 1.3) and at rest on cloud infrastructure.
- Access Control: Role-based access control (RBAC) with principle of least privilege. Multi-factor authentication (MFA) mandatory for all administrative accounts.
- Penetration Testing: Annual third-party penetration test of the Platform. Critical findings must be remediated within 30 days.
- Vulnerability Management: Monthly automated vulnerability scanning. Patch management policy aligned with CVE severity levels.
- Data Backup: Daily automated backups with 30-day retention. Offsite backup maintained. Recovery time objective (RTO): 4 hours. Recovery point objective (RPO): 24 hours.

4.2 Organisational Controls

- Data Protection Training: Mandatory for all employees upon onboarding and annually thereafter.
- Data Protection Impact Assessment (DPIA): Required before implementing any new feature, product, or processing activity involving personal data.
- Data Breach Register: All incidents; actual and near-miss, to be logged within 24 hours of discovery.
- Breach Notification: Data subjects notified within 72 hours of confirmed breach where likely to result in high risk (DPA Sec 43). ODPC notified as required.

5. CROSS-BORDER DATA TRANSFERS

AquaSee operates cloud infrastructure hosted on cloud servers which may involve cross-border data transfers. All transfers are governed by:

- Standard Contractual Clauses (SCCs) incorporated into cloud provider Data Processing Agreements.
- Adequacy assessments for any transfers outside Kenya and the EU, documented in the Transfer Impact Assessment register.
- Transfers to third-country processors only permitted where: (a) adequacy decision exists; (b) appropriate safeguards (SCCs) are in place; or (c) specific derogations under DPA Sec 48 apply.

6. GOVERNANCE & ACCOUNTABILITY

Role	Responsibilities
Compliance Officer (current: CEO)	ODPC registration; DPIA oversight; breach response; policy review; staff training.
Technical Lead / CTO	Implementation of technical security controls; encryption; access management; incident detection.
All Employees	Report actual or suspected data breaches within 24 hours; comply with this Framework; complete mandatory training.

This Framework is reviewed annually and upon any material change in law, technology, or business structure. Next scheduled review: January 2027.

SIGNATURES

Odero Otieno
JahBungu

Digitally signed by Odero Otieno JahBungu
DN: cn=Odero Otieno JahBungu, c=KE,
o=AquaSee Networks Ltd, ou=Founder,
email=aquaseeafrica@gmail.com
Reason: I am the author of this document
Location: Kisumu Kenya
Date: 2025.03.26 19:52:01 +03'00'

Policy Approved by (CEO)

Odero Otieno JahBungu

Founder & CEO — AquaSee Networks Limited

Date: