Monitor AML Compliance with Ease

InfoAML

INFO SOFT
انفو سوفت

INFOAML – BASE SERVICE LEVEL AGREEMENT (BASE SLA)

Version 1.0

Effective Date: 05/02/2026

Contents

1. Purpose

This Service Level Agreement ("SLA") describes the general service commitments applicable to the InfoAML application and related support services.

This SLA forms part of the customer's subscription agreement and does not replace applicable terms and conditions

2. No Signature Required

This Base Service Level Agreement is issued by InfoAML and does not require a signature. It becomes effective as of the effective date stated above and applies in accordance with the customer's subscription, invoice, or use of the service.

3. Scope of Services

This SLA applies to:

- Access to the InfoAML application
- Core application functionality
- Automated screening and reporting features
- Standard support services

This SLA does **not** cover:

- Regulatory outcomes or approvals
- Legal or compliance advice
- Accuracy or completeness of customer-provided data
- Third-party or platform-level services

4. Service Availability

InfoAML is designed to be available on a continuous basis, subject to the availability of the underlying platform and hosting environment.

- Target availability: **99% per calendar month**
- Availability is measured at the application level
- Planned maintenance and platform-level outages are excluded

No guarantee of uninterrupted service is provided.

5. Maintenance

Planned maintenance may be performed periodically.

- Reasonable advance notice will be provided where practicable
- Emergency maintenance may be performed without notice
- Maintenance activities may result in temporary service interruption

6. Support Services

6.1. Support Channels

- Email support
- Ticket-based support system (where applicable)

6.2. Support Hours

- Standard business hours (UAE time), excluding public holidays

7. Incident Response Targets

InfoAML applies reasonable efforts to respond to reported incidents.

Severity	Description	Target Response
Critical	Application unavailable	Same business day
High	Core function impacted	Next business day
Medium	Partial functionality issue	2-3 business days
Low	Minor or cosmetic issue	Best Effort

Response times refer to acknowledgment, not resolution.

8. Platform Dependencies

InfoAML operates within an underlying platform and hosting environment provided by third-party service providers.

Certain services, including but not limited to:

- Infrastructure availability
- Data backups
- Environment separation (e.g. staging and production)
- Core database and storage services are outside the direct operational control of InfoAML and are subject to the policies and terms of the respective platform service provider.

9. Sanctions Screening Coverage

InfoAML performs sanctions screening by comparing customer and related-party data against configured sanctions data sources.

Sanctions screening coverage includes, where applicable:

- **United Arab Emirates sanctions lists** issued by relevant authorities

- **United Nations Security Council sanctions lists**
- **Consolidated international sanctions datasets**, curated from multiple jurisdictions and publicly available authoritative sources

Sanctions data is sourced from official publications and curated third-party datasets and is subject to their scope, structure, and publication practices.

10. Sanctions-Data Update Frequency

InfoAML updates sanctions screening data on a periodic basis to reflect changes published by underlying data sources.

- Updates are **typically processed every 6 to 8 hours**, subject to source availability
- Update timing may vary depending on publication schedules and technical processing
- Real-time updates are not guaranteed

Sanctions screening reflects the data available at the time of screening.

11. Politically Exposed Persons (PEP) Screening

Where enabled, InfoAML performs screening for **Politically Exposed Persons (PEPs)** based on configured PEP data sources.

- PEP screening results are provided as **risk indicators only**
- Identification of a PEP does not constitute a sanctions designation
- PEP identification requires appropriate risk-based assessment and human review

12. Delisted Status Information

InfoAML may provide **delisted status indicators** where such information is officially published.

- Delisted status handling currently applies **only to UAE-issued sanctions lists**
- Delisted indicators are provided for reference and historical context
- Absence of a delisted indicator does not imply that an individual or entity has never been listed

13. Automated System Outputs

InfoAML provides automated screening results, risk indicators, reports, dashboards, and audit logs based on system logic and customer-provided data.

These outputs:

- Are provided for **decision-support purposes only**
- Do not constitute regulatory, legal, or compliance determinations
- Require human review, validation, and judgment

14. Data Processing and Retention Model

InfoAML performs sanctions and PEP screening by **temporarily processing customer data** provided by the customer for the sole purpose of comparison against configured sanctions and risk datasets.

- Customer data used for screening is **processed transiently** to execute screening requests
- InfoAML does **not retain or store full customer profile data** on the server side beyond what is required to perform the screening operation
- No manual review or access to customer screening data is performed by InfoAML personnel as part of standard operations

InfoAML retains **limited technical metadata** related to screening requests, such as timestamps, reference identifiers, and processing status, solely for operational monitoring, auditability, and system integrity purposes. Such metadata does **not** include full customer identity records.

15. Customer Responsibilities

The customer is responsible for ensuring that InfoAML is used appropriately and in accordance with applicable laws and internal compliance procedures.

The customer shall:

- Designate a **competent compliance officer and/or MLRO**, where required
- Ensure users have appropriate knowledge and training
- Review and validate screening results and risk indicators
- Maintain accurate and complete customer data
- Use the system in accordance with provided documentation

InfoAML may provide onboarding or training support; however, such support does not transfer regulatory responsibility.

16. Customer Security Responsibilities

The customer is responsible for maintaining the security of its system environment and user access.

In particular, the customer shall:

- Implement appropriate access controls
- Use strong and confidential authentication credentials
- Restrict system access to authorized personnel
- Promptly revoke access when no longer required
- Protect systems and devices from unauthorized access
- Notify InfoAML of any suspected security incident

InfoAML is not responsible for incidents arising from compromised credentials or customer-side security weaknesses.

17. Optional Security Controls

The system environment may support additional security controls, such as **two-factor authentication (2FA**), depending on customer configuration and platform capabilities.

- Enabling such controls is at the customer's discretion
- The customer is responsible for configuring and managing these controls
- InfoAML does not enforce or monitor customer security configurations unless expressly agree

18. Data & Security

- Customer data remains the property of the customer
- Application-level access controls and audit logs are maintained
- Reasonable technical and organizational security measures are applied

Absolute security is not guaranteed.

19. Limitations of Liability

InfoAML shall not be liable for:

- Regulatory penalties or enforcement actions
- Missed or undetected suspicious activity
- Platform or third-party service failures
- Customer configuration, access, or usage errors

Total liability, if any, is limited to the subscription fees paid for the affected service period.

20. Changes to the Service

InfoAML may update, modify, or enhance the application from time to time. Reasonable efforts will be made to minimize material disruption.

21. Governing Law

This SLA shall be governed by and construed in accordance with the laws of the **United Arab Emirates.**