Service Level Agreement (SLA)

Umbraic B.V.

Last updated: 16/03/2026
Governing law: The Netherlands

This Service Level Agreement ("SLA") describes the service performance commitments provided by Umbraic B.V. ("Provider") for its Compliance AI platform ("Service"). This SLA applies to all Customers with an active subscription, unless otherwise agreed in writing.

1. Service Availability

Provider shall maintain a minimum 99.5% Service Availability per calendar month, excluding Scheduled Maintenance. Scheduled Maintenance shall be announced at least 48 hours in advance and conducted outside business hours whenever reasonably possible.

2. Support Response Times

Support requests are classified by severity. Response and resolution targets are as follows:

P1 – Critical (complete Service unavailability or data integrity risk): Initial response within 1 hour; resolution or workaround within 4 hours. Initial Customer notification within 1 hour of detection.

P2 – High (significant degradation of core functionality): Initial response within 4 hours; resolution or workaround within 8 business hours. Customer notification within 4 hours of detection.

P3 – Medium (partial or intermittent degradation): Initial response within 8 business hours; resolution within 3 business days.

P4 – Low (general enquiries, non-urgent requests): Initial response within 2 business days; resolution within 10 business days.

For P1 and P2 incidents, Provider shall issue status updates at minimum every 2 hours until resolution. A written post-incident report shall be provided to the Customer within 5 business days of resolution, documenting root cause, impact, and corrective actions taken.

3. Security & Data Protection

Provider shall implement industry-standard security measures. Provider processes personal data in accordance with GDPR and its Privacy Policy.

4. Maintenance & Updates

The Provider may deploy updates, improvements, and security patches on a rolling basis.

4.1 Recovery Objectives. Provider commits to the following recovery targets in the event of a service disruption:

(a) Recovery Time Objective (RTO): Service shall be restored within 4 hours of a P1 incident being declared;

(b) Recovery Point Objective (RPO): Customer data shall be recoverable to a state no older than 1 hour prior to the incident.

4.2 Business Continuity and Disaster Recovery. Provider maintains a documented Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). These plans are tested at minimum annually. Upon written request, Provider shall supply to the Customer a summary of BCP/DRP scope, most recent test date, and test outcomes, subject to confidentiality obligations.

5. Service Exclusions

This SLA does not apply to interruptions caused by:

- Customer systems or integrations
- Third-party services or outages
- Internet or network instability outside Provider's control
- Misuse of the Service
- Force Majeure events

6. Service Credits

If monthly Availability falls below the committed 99.5%, the Customer is entitled to a credit toward the next subscription invoice:

- 98.0%–99.49%: 5% credit
- 95.0%–97.99%: 10% credit
- Below 95.0%: 20% credit

Claims must be submitted by email within 30 days of the affected month.

7. Change Management

7.1 Provider shall give at least thirty (30) days' prior written notice of any material change to the Service, including changes to features, architecture, data processing locations, or third-party sub-processors that may affect Customers' ICT risk profiles. For Customers that are regulated financial entities under DORA, this notice period shall be no less than sixty (60) days where the change affects services supporting critical or important functions.

7.2 Sub-processor and Subcontractor Register. Provider maintains a register of material sub-processors and subcontractors involved in the delivery of the Service. This register is available to Customers upon written request. Provider shall notify Customers of any intended changes to material sub-processors or subcontractors no less than thirty (30) days in advance, providing sufficient information for Customers to assess ICT concentration and third-party risk.

Urgent security updates may be deployed without prior notice.

8. Updates to This SLA

Umbraic may update this SLA from time to time. Significant changes that materially impact service levels will be communicated to the Customer with prior notice. The current version will always be available at: umbraic.com/Service_Level_Agreement.pdf

9. Audit Rights

9.1 Customer Audit Rights. Customer, or a qualified third-party auditor appointed by Customer, shall have the right to audit Provider's information security controls, operational resilience measures, and compliance with this SLA, upon at least thirty (30) days' prior written notice. Audits shall be conducted during normal business hours, no more than once per calendar year (unless a security incident has occurred), and shall not unreasonably disrupt Provider's operations. Costs of such audits shall be borne by the Customer unless material non-compliance is identified.

9.2 Regulatory Access. Where Customer is a regulated financial entity subject to supervisory oversight, the relevant national competent authority or European Supervisory Authority (ESA) shall have the right, upon lawful request, to conduct inspections, access Provider's premises, and request information from Provider to the extent required by applicable law, including Regulation (EU) 2022/2554 (DORA). Provider shall cooperate fully with any such regulatory inspection.

10. Data Portability and Exit Assistance

10.1 Upon termination or expiry of the Agreement, or upon Customer's written request during the Agreement term, Provider shall make Customer data available for export in a commonly used, machine-readable format (e.g. JSON, CSV, XML) within thirty (30) calendar days. Provider shall provide reasonable transition assistance for a period of up to ninety (90) days post-termination to support migration to an alternative provider, at Provider's standard time-and-materials rates unless otherwise agreed.

10.2 Provider maintains a documented exit plan setting out the steps to be taken in the event of termination, including data transfer procedures, service wind-down timelines, and key contacts for transition coordination. This exit plan is available to Customers upon written request.

11. DORA Compliance and Digital Operational Resilience

11.1 Provider acknowledges that Customers may be regulated financial entities subject to Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). Provider commits to supporting Customers' compliance with their DORA obligations, including by:

(a) providing information necessary for Customers to conduct ICT third-party risk assessments;

(b) participating in resilience testing exercises as reasonably requested; and

(c) maintaining the documentation, controls, and capabilities described in this SLA.

11.2 Threat-Led Penetration Testing (TLPT). Where Provider is designated as a critical ICT third-party service provider under DORA, or where a Customer's competent authority requires inclusion of Provider's systems in a Threat-Led Penetration Test (TLPT) pursuant to Article 26 of DORA, Provider shall cooperate fully with such testing and shall facilitate access to the relevant systems and infrastructure, subject to reasonable advance notice and agreed scope.

11.3 Critical TPSP Designation. If Provider is designated as a critical ICT third-party service provider under Article 31 of DORA, Provider shall:

(a) comply with all requirements imposed by the Lead Overseer appointed by the European Supervisory Authorities;

(b) notify affected Customers promptly of such designation and any resulting changes to obligations; and

(c) cooperate with the Lead Overseer's oversight activities, including information requests, general investigations, and on-site inspections, as required by law.