



Service Level Agreement (SLA)

Umbraic B.V.

Last updated: 07/05/2026

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 2 business hours; resolution or workaround within 1 business day. Initial Customer notification within 2 business hours of detection.

P2 – High (significant degradation of core functionality): Initial response within 4 business hours; resolution or workaround within 2 business days. Customer notification within 4 business hours of detection.

P3 – Medium (partial or intermittent degradation): Initial response within 1 business day; resolution within 5 business days.

P4 – Low (general enquiries, non-urgent requests): Initial response within 2 business days; resolution within 15 business days.

Business hours are defined as 08:00–19:00 CET, Monday–Friday, excluding Dutch public holidays. Resolution and response clocks begin at the start of the next business day where an incident is reported outside of business hours.

For P1 and P2 incidents, the Provider shall issue regular status updates until resolution. A written post-incident report shall be provided to the Customer within 10 business days of resolution, documenting root cause, impact, and corrective actions taken.

3. Security, Data Protection & Disclaimers

3.1 Provider shall implement and maintain the following minimum security measures in connection with the delivery of the Service:

(a) **Encryption.** Customer data shall be encrypted in transit using TLS 1.2 or higher, and encrypted at rest using AES-256 or equivalent.



(b) **Access controls.** Access to production systems and Customer data shall be restricted to authorised personnel on a least-privilege basis. Access rights shall be reviewed at least annually and revoked promptly upon a change in role or departure.

(c) **Vulnerability management.** Security vulnerabilities identified in the Service or supporting infrastructure shall be triaged and remediated in accordance with their severity, with critical vulnerabilities addressed within 14 days of identification.

(d) **Incident response.** Provider maintains an incident response procedure. In the event of a confirmed or suspected security incident affecting Customer data, Provider shall notify affected Customers without undue delay and in any event within 72 hours of becoming aware, in accordance with applicable GDPR obligations.

(e) **Personal data.** Provider processes personal data in accordance with GDPR and its Privacy Policy, and as further detailed in the applicable Data Processing Agreement.

4. Maintenance & Updates

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

Provider commits to the following recovery targets in the event of a service disruption:

- (a) Service shall be restored within 24 hours of a P1 incident being declared;
- (b) Customer data shall be recoverable to a state no older than 24 hours prior to the incident.

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 (as defined in the Standard Terms and Conditions)

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.

Service credits under this section are Customer's exclusive financial remedy for failure to meet the availability commitment in §1. For other material breaches of this SLA, Customer's rights under the Agreement (including damages claims subject to clause 12 of the Standard Terms and Conditions) are not limited by this clause. In addition, in the event of three or more P1 incidents within any six-month period, Customer may terminate the Agreement on written notice with a pro-rata refund of prepaid fees for the unused term.



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 thirty (30) days where the change affects services supporting critical or important functions.

7.2 Provider shall maintain and make available to Customer a current register of all subprocessors and AI providers engaged in the delivery of the Service, including relevant details on their identity, location, and processing activities.

Provider shall provide Customer with at least thirty (30) days' prior written notice of any intended addition or replacement of a subprocessor or AI provider, including sufficient information to enable Customer to assess data protection, regulatory, information security, and ICT concentration risks.

Customer shall have the right to object to any proposed new subprocessor or AI provider on reasonable grounds. If such objection cannot be resolved within fifteen (15) business days, Customer may terminate the affected Service without penalty.

7.3 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: umbra-ai.com/Service_Level_Agreement.pdf

9. Audit Rights

9.1 Customer Audit Rights. The Customer, or a qualified third-party auditor appointed by the 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, or twice per calendar year in the event that a confirmed security incident has occurred during that year. Audits 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 the 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 will provide up to sixteen (16) hours of transition assistance at no additional cost during the 60 days following termination, in addition to the data export described in §10.1. Transition assistance beyond this allowance shall be billed at €150 per consultant-hour, subject to a written estimate agreed in advance.

11. DORA Compliance and Digital Operational Resilience

11.1 General Support. Provider acknowledges that Customers may be regulated financial entities subject to Regulation (EU) 2022/2554 (DORA). Where applicable, Provider will reasonably support Customers in meeting their ICT third-party risk management obligations, including by:

- (a) providing information reasonably available for Customers to conduct ICT third-party risk assessments, such as details of Provider's security practices, sub-processors, and incident response procedures;
- (b) maintaining the resilience, security, and availability commitments set out in this SLA; and
- (c) notifying Customers of ICT-related incidents that materially affect service availability or the security of Customer data within the timeframes set out in section 2.

The sub-processor and subcontractor register maintained under clause 7.2 is intended to support Customers' documentation obligations under Article 30 of DORA, and Provider will keep this register sufficiently detailed for Customers to meet their own Article 30 obligations.

11.2 Resilience Testing. Provider will cooperate in good faith with resilience testing exercises reasonably requested by a Customer, subject to: (a) reasonable advance notice of no less than 30 days; (b) prior agreement on scope to ensure testing does not disrupt other customers or production systems; and (c) such testing occurring no more than once per calendar year per Customer. Costs of any material testing effort are borne by the requesting Customer. Provider is not obligated to participate in Threat-Led Penetration Testing (TLPT) under Article 26 of DORA unless Provider is expressly included in scope by the Customer's competent authority and the conditions in this clause are met.

11.3 Critical TPSP Designation. The Provider does not currently meet the criteria for designation as a critical ICT third-party service provider under Article 31 of DORA and does not accept obligations associated with that designation as a baseline contractual commitment. In the unlikely event that Provider is formally designated as critical by a Lead Overseer, Provider will: (a) notify affected Customers promptly; (b) cooperate with the Lead Overseer as required by applicable law; and (c) engage with affected Customers in good faith to agree any necessary adjustments to service terms.

12. Liability

Liability arising under or in connection with this SLA is governed by clause 12 of the Standard Terms and Conditions, which forms part of the Agreement. For the avoidance of doubt, the cap and exclusions in those Terms apply to all claims arising from the Service, including SLA failures, and service credits under clause 6 are the sole financial remedy for failure to meet the availability commitment in clause 1.