Service Level Agreement (SLA)

Umbraic B.V.

Last updated: 31/07/2026
These terms are effective immediately for new clients. For existing clients, these terms will take effect on 30/08/2026, in accordance with the notice provisions of the prior agreement.
Governing law: The Netherlands

This Service Level Agreement ("SLA") describes the service performance commitments provided by Umbraic B.V. ("Provider") for its AI-native compliance platform ("Service"). This SLA applies to all Customers with an active subscription, unless otherwise agreed in writing. Capitalised terms used but not defined in this SLA have the meanings given in the Standard Terms and Conditions, and references in this SLA to Customer data mean Customer Data as defined in clause 1.1 of those Terms, save that for the purposes of §2 (Support Response Times), §3 (Security, Data Protection & Disclaimers) and §12 (Security Awareness and Resilience Training), references to Customer data shall additionally include the account and contact details of Customer's authorised users and business contacts and the security and system logs generated by Provider, notwithstanding their exclusion from that definition.

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.

For the purposes of this SLA, "Service Availability" means the percentage of minutes in a calendar month during which the Service is available for use by Customer, calculated as: (Total Minutes − Excluded Minutes − Unavailable Minutes) ÷ (Total Minutes − Excluded Minutes) × 100.

The Service is "Unavailable" where it fails to respond to valid requests, as measured by Provider's external monitoring at intervals of no more than five (5) minutes. A period of unavailability begins at the first failed check that is confirmed by a second consecutive failed check, and ends at the first subsequent successful check. "Excluded Minutes" means Scheduled Maintenance under this clause and any period excluded under §5. Provider shall make its availability measurements for a given month available to Customer on request.

2. Support Response Times

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

P1 – Critical (complete unavailability of the Service for all Customer users, or confirmed loss, corruption or unauthorised disclosure of Customer data): Initial response within two (2) hours. Provider shall thereafter apply continuous commercially reasonable efforts toward resolution, with a

target of resolution or workaround within twenty-four (24) hours. Initial Customer notification within two (2) hours of detection. Where the incident involves confirmed or suspected loss, corruption or unauthorised disclosure of Customer data, that initial notification may be preliminary, and Provider shall in addition provide the notification described in §3.1(d) within the period specified in that clause.

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 Central European Time (CET or CEST, as applicable in the Netherlands), 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.

Notwithstanding the foregoing, Provider maintains an on-call capability for P1 incidents on a twenty-four hours a day, seven days a week basis, and the response, notification and resolution clocks for P1 incidents run continuously from Provider's detection of, or notification by Customer of, the incident. The next-business-day rule above applies to P2, P3 and P4 incidents only.

For P1 and P2 incidents, the Provider shall issue regular status updates until resolution. For P1 incidents, 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. For P2 incidents, a written summary of root cause and corrective action shall be provided on Customer request.

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.** Provider maintains a vulnerability management process covering the Service and supporting infrastructure under its control. Vulnerabilities shall be triaged and

remediated in accordance with their severity, with vulnerabilities rated Critical (CVSS 9.0 or higher) remediated within fourteen (14) days of a vendor fix becoming available, and vulnerabilities rated High (CVSS 7.0–8.9) within thirty (30) days. Where remediation is not technically feasible within these periods, Provider shall apply compensating controls and inform Customer on request. Vulnerabilities in third-party infrastructure not under Provider's control shall be escalated to the relevant provider.

(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 twenty-four (24) hours of becoming aware. The notification shall include the information then reasonably available to Provider that Customer requires in order to assess the incident and to meet its own notification obligations under Article 33 GDPR and, where applicable, Articles 17 to 19 of DORA. Provider shall provide further updates as additional information becomes available.

(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.

(f) **Data location.** The Service is provided from, and Customer data is stored within, the European Economic Area. Where processing necessarily involves a transfer outside the EEA, including processing by an AI provider or subprocessor identified in the register maintained under §7.2, such transfer shall be subject to EU Standard Contractual Clauses or another transfer mechanism valid under Chapter V of the GDPR, and the relevant subprocessor and its processing location shall be identified in that register. Provider shall give Customer at least thirty (30) days' prior written notice, or sixty (60) days' prior written notice where §7.1 requires a longer period, of any change to the countries in which the Service is provided or Customer data is processed.

3.2 Regulatory Output Deficiencies

3.2.1 If Provider becomes aware of a material deficiency in the Service that results in materially incorrect regulatory output, Provider shall, without undue delay after becoming aware:

(i) notify Customer;
(ii) provide reasonable information regarding the affected output and its potential impact; and
(iii) take reasonable steps to correct the issue and prevent recurrence.

3.2.2 This obligation:

(i) is a knowledge-based duty and does not include any duty to monitor or detect;
(ii) does not constitute an admission of liability or a warranty of regulatory correctness; and
(iii) is subject to the liability cap in clause 12 of the Standard Terms and Conditions.

3.2.3 For the purposes of this clause, “materially incorrect output” means output that is materially inconsistent with the documented functionality of the Service or attributable to a deficiency in the Service, and excludes output that merely reflects a differing regulatory interpretation.

3.2.4 Without limiting clause 11.5 of the Standard Terms and Conditions, Provider warrants that the Service will perform materially in accordance with Provider's documentation and will be provided and maintained with reasonable skill and care.

4. Maintenance, Updates and Business Continuity

4.1 Provider will update the Service within a commercially reasonable timeframe in response to material changes to the supported regulatory frameworks identified in the Agreement, provided that (i) the relevant changes are publicly available; (ii) the necessary regulatory data or sources are reasonably accessible; and (iii) such updates are technically feasible. Updates may be rolled out incrementally. This obligation relates to the maintenance of the Service and does not constitute a warranty of complete or immediate alignment with all regulatory changes. The Provider may deploy updates, improvements, and security patches on a rolling basis.

4.2 Business Continuity and Disaster Recovery. Provider maintains a documented business continuity and disaster recovery plan covering the Service, and commits to the following recovery targets in the event of a service disruption:

(a) **Recovery Time Objective:** Provider shall target restoration of the Service within 24 hours of invocation of the business continuity and disaster recovery plan referred to in this clause 4.2, in respect of disruptions within Provider's control. This recovery time objective is a recovery target only and does not vary the Service Availability commitment in §1 or Customer's entitlement to service credits under §6; periods of unavailability count towards the calculation in §1 whether or not restoration is achieved within this objective. Where the disruption originates in underlying cloud infrastructure, Provider's recovery time is dependent on that provider's restoration and Provider shall apply commercially reasonable efforts to restore the Service as soon as practicable thereafter;

(b) **Recovery Point Objective:** Customer data shall be recoverable to a state no older than 24 hours prior to the incident.

5. Service Exclusions

The Service Availability commitment in §1 and the service credits in §6 do not apply to interruptions caused by:

- Customer systems or integrations
- Failure or degradation of third-party services or infrastructure outside Provider's reasonable control, save that this exclusion shall not apply to the acts or omissions of subprocessors, AI providers or hosting infrastructure providers engaged by Provider in the delivery of the

Service, for which Provider remains responsible in accordance with clause 24.2 of the Standard Terms and Conditions, except to the extent that such failure or degradation is itself attributable to a Force Majeure event as defined in clause 13.1 of the Standard Terms and Conditions
- Internet or network instability outside Provider's control
- Misuse of the Service
- Force Majeure events (as defined in the Standard Terms and Conditions)

- Suspension of the Service by Provider in accordance with clause 4.4 or 5.3 of the Standard Terms and Conditions

For the avoidance of doubt, the exclusions in this §5 do not relieve Provider of its obligations under §4.2 (Business Continuity and Disaster Recovery), which continue to apply to the extent restoration is within Provider's control, as provided in clause 13.1 of the Standard Terms and Conditions. Nor do they limit Provider's other obligations under this SLA, including those under §2 and §3.

6. Service Credits

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

- Availability ≥98.0% and <99.5%: credit of 5% of the monthly subscription fee for the affected month
- Availability ≥95.0% and <98.0%: credit of 10% of the monthly subscription fee for the affected month
- Availability <95.0%: credit of 20% of the monthly subscription fee for the affected month

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 each exceeding twenty-four (24) hours in duration within any six-month period, Customer may terminate the Agreement on thirty (30) days' written notice with a pro-rata refund of prepaid fees for the unused term, provided that Customer gives such notice within thirty (30) days of the third such incident.

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 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, and any period for which they retain Customer Data for abuse monitoring or security purposes.

Provider shall provide Customer with at least thirty (30) days' prior written notice, or sixty (60) days' prior written notice where §7.1 requires a longer period, 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.

Where a subprocessor or AI provider must be replaced with less notice because of (i) discontinuation, deprecation or material degradation of that provider's service; (ii) a security, availability or legal risk arising from continued use; or (iii) that provider's insolvency or termination of its agreement with Provider, Provider may effect the replacement on such notice as is reasonably practicable, and shall notify Customer without undue delay and in any event within five (5) business days, providing the information described above. Any replacement provider shall be bound by obligations materially equivalent to those applying to the provider replaced, and the replacement shall not result in Customer data being processed outside the EEA except in accordance with §3.1(f).

Customer shall have the right to object to any proposed new subprocessor or AI provider on reasonable grounds relating to data protection, information security or regulatory compliance. The Parties shall discuss the objection in good faith. If such objection cannot be resolved within fifteen (15) business days, Customer may terminate the affected Service without penalty, with a pro-rata refund of prepaid, unused fees.

7.3 Urgent security updates may be deployed without prior notice.

8. Updates to This SLA

This SLA forms part of the Agreement. Amendments are made in accordance with clause 20 of the Standard Terms and Conditions. The current version will always be available at: https://www.umbra-ai.com/Service_Level_Agreement.pdf

9. Audit Rights

9.1 **Customer Audit Rights.** Customer's rights to audit Provider's information security controls, operational resilience measures and compliance with this SLA are as set out in clause 23.2 of the Standard Terms and Conditions.

9.2 Regulatory Access. Regulatory and supervisory access rights, including the rights of national competent authorities and the European Supervisory Authorities under Regulation (EU) 2022/2554 (DORA), are as set out in clause 23.3 of the Standard Terms and Conditions and apply to the Service provided under this SLA.

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, subject to the free allowance and the rates set out in §10.2.

10.2 Provider will provide up to eight (8) hours of transition assistance at no additional cost during the ninety (90) 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. Provider's obligation to provide transition assistance is conditional on Customer having paid all undisputed amounts due.

10.3 Following expiry of the export period in §10.1 and the transition assistance period in §10.2, Provider shall delete Customer data from its active systems within thirty (30) days and shall ensure that such data is permanently expunged from encrypted backups within ninety (90) days, save to the extent retention is required by applicable law. Provider shall confirm such deletion to Customer in writing on request.

11. DORA Compliance and Digital Operational Resilience

11.1 DORA Commitments. Provider's commitments in relation to DORA: general support for Customers' ICT third-party risk management obligations, resilience testing and threat-led penetration testing, and critical ICT third-party service provider designation under Article 31, are as set out in clause 25 of the Standard Terms and Conditions and apply to the Service provided under this SLA.

The sub-processor and subcontractor register maintained under clause 7.2 of this SLA 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.

12. Security Awareness and Resilience Training

Provider shall ensure that personnel with access to Customer data complete information security awareness training on induction and at least annually thereafter, and shall confirm completion to Customer on request. Provider shall maintain records of completion of such training and make them available to Customer on request. Where Customer is a regulated financial entity, Provider shall on reasonable request permit relevant personnel to participate in Customer's ICT security awareness programmes and digital operational resilience training, to the extent reasonably necessary for Customer to meet its obligations under Article 30(2)(i) of DORA, at Customer's cost.

13. 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.