Privacy Policy

Umbraic B.V.

Last updated: 31/07/2026
This version is effective immediately for new clients. For existing clients, it takes effect on 30/08/2026, in accordance with clause 20 of the Standard Terms and Conditions.
Our role: Umbraic acts as Controller for personal data of website visitors, business contacts, and the account and contact details of Clients' authorised users, and as Processor for personal data contained in Client-uploaded documentation and in platform activity generated through a Client's use of the Services, in each case as described in Section 2.
Registered Address: Prof. Tulpstraat 13, 1018GZ Amsterdam, The Netherlands
KVK: 98648640
Contact: jochem@umbra-ai.com

1. Introduction

Umbraic B.V. ("Umbraic", "we", "our", or "us") provides an AI-native compliance platform that helps organisations automate compliance documentation and align outputs with regulator requirements.

This Privacy Policy explains how we collect, use, share, and protect personal data when you interact with our website, use our software and related services ("Services"; for the purposes of this Policy, "Services" means the Software and the Services together, as those terms are defined in clause 1.1 of the Standard Terms and Conditions), or otherwise engage with us.

We are committed to protecting your privacy and processing personal data in compliance with the **General Data Protection Regulation (EU) 2016/679 (GDPR)** and other applicable laws.

2. How We Collect and Use Personal Data

We collect and process data in the following ways:

a. Client and User Information
When a business (our Client) uses the Umbraic platform, we may process personal data of the Client's authorised users, such as:

- Name, email address, and contact details
- Role and organisation
- Login credentials and account security logs

We use this data to provide and secure the Services, authenticate access, deliver support, and communicate with Clients. Platform activity generated through a Client's use of the Services is processed by Umbraic as Processor, as described in section 2(b). Umbraic acts as an independent Controller in respect of the security and system logs it generates in order to secure and operate the Services and to comply with its own legal obligations.

b. Compliance Documentation and Internal Policies

Clients may upload their own internal compliance documentation, such as policies, procedures, manuals, and other materials used to manage regulatory obligations.

- These documents remain the sole property of the Client.
- Clients have full control and can upload, manage, and delete these materials at any time.
- When deleted, documents are removed from Umbraic's active systems immediately and are permanently expunged from encrypted backups within ninety (90) days, in accordance with our backup rotation schedule. Where content has been transmitted to an AI provider that applies its own limited abuse-monitoring retention period, deletion within that provider's systems occurs in accordance with that period.
- Umbraic does not access, share, or disclose Clients' internal documentation to third parties except as set out in Section 5 (How We Share Data), including trusted service providers who support our services and are bound by strict confidentiality and data-protection obligations.
- These materials are never used to train or fine-tune AI models, whether Umbraic's own or those of our AI providers. Our AI providers are contractually prohibited from using Client content for model training. Where an AI provider requires it, Client content may be retained by that provider for a limited period solely for abuse monitoring and security purposes; the providers concerned and the applicable retention periods are recorded in the register described in §7.2 of our Service Level Agreement.

Umbraic only processes these documents as a **Processor**, under the Client's direction and in accordance with a **Data Processing Agreement (DPA)**.

c. Website Visitors and Communication

When you visit our website or contact us, we may collect information such as:

- Contact details submitted via forms or email
- Log data and cookies (see Section 4)

3. Legal Basis for Processing

We process personal data based on one or more of the following legal grounds:

- **Contractual necessity:** to provide our Services and fulfil our obligations under the Agreement with the Client.
- **Legitimate interests:** to ensure platform security, improve functionality, and communicate with Clients.
- **Legal obligations:** to comply with applicable laws or regulatory requirements.
- **Consent:** for optional communications such as newsletters or event invitations (you can withdraw consent at any time).

4. Cookies

Umbraic uses cookies and similar technologies to ensure proper website functionality.

- **Necessary cookies:** enable core functionality such as login and session security.

5. How We Share Data

We only share personal data where necessary and in accordance with GDPR:

- **Service providers and AI providers:** We use a limited number of vetted providers to deliver the Service. We maintain a current register of them and bind each of them to obligations materially equivalent to our own. The full mechanism, including the Client's right to object, is set out in §7.2 of our Service Level Agreement.
- **Affiliates:** Within the Umbraic group, for internal administration and service delivery.
- **Legal or Regulatory:** Where required to comply with law or respond to lawful requests.
- **Business Transactions:** In case of a merger or acquisition, provided appropriate safeguards are in place.

Umbraic does **not** sell, rent, or use Clients' uploaded documentation or data for any purpose beyond delivering the contracted Services.

6. Data Security and Retention

Umbraic implements and maintains **technical and organisational measures** to protect data, including:

- Encryption in transit and at rest
- Access controls and activity logging
- Hosting and storage of Client data within the European Economic Area (EEA), with any onward processing outside the EEA subject to the safeguards described in Section 7.
- **Security framework:** Umbraic's security programme is aligned with recognised frameworks including ISO/IEC 27001. We work towards obtaining formal third-party certification and will make available to Clients, upon request, relevant audit reports or certifications as they become available.

ICT Incident Management. Umbraic maintains an ICT incident management process to detect, classify, and respond to security and operational incidents. In the event of an ICT incident that materially affects the availability, authenticity, integrity, or confidentiality of data processed on behalf of a Client, Umbraic will notify the affected Client within the timeframes set out in the Service Level Agreement. Where Umbraic processes personal data as a Processor on behalf of a Client who is subject to Regulation (EU) 2022/2554 (DORA), Umbraic will provide the Client with sufficient information to enable the Client to fulfil its own incident reporting obligations to competent authorities under DORA and GDPR.

We retain personal data only as long as necessary to provide the Services or meet legal obligations.

Specifically: account and business contact data is retained for the duration of the Agreement and for twenty-four (24) months thereafter; security and system logs for which Umbraic acts as Controller are retained for twelve (12) months; platform activity processed on behalf of a Client is retained in accordance with that Client's instructions and the applicable Data Processing Agreement, and in the absence of other instructions for twelve (12) months or until deleted following termination or expiry in accordance with §10.3 of the

Service Level Agreement, whichever occurs first; and Client-uploaded documents are retained until deleted by the Client or, following termination or expiry of the Agreement, until expiry of the export and transition assistance periods set out in §10 of the Service Level Agreement, after which they are deleted from active systems within thirty (30) days and permanently expunged from encrypted backups within ninety (90) days.

Client-uploaded compliance documents can be deleted by the Client at any time. Deleted documents are removed from active systems immediately and are permanently expunged from encrypted backups within ninety (90) days. Only aggregated, anonymised usage data may be retained for analytics.

7. International Data Transfers

If data is transferred outside the EEA, Umbraic ensures an adequate level of protection through **EU Standard Contractual Clauses (SCCs)** or equivalent safeguards.

8. Your Rights

Under GDPR, individuals have the following rights:

- **Access** – Obtain a copy of your personal data.
- **Rectification** – Correct inaccurate or incomplete data.
- **Erasure** – Request deletion of your personal data (subject to legal requirements).
- **Restriction** – Limit processing under certain conditions.
- **Portability** – Receive your data in a portable format.
- **Objection** – Object to processing based on legitimate interests.
- **Withdraw consent** – Withdraw consent where processing is based on it.

- **Automated decision-making.** The Service generates draft documentation and analysis for review by the Client's own personnel. Umbraic does not use personal data to make decisions producing legal or similarly significant effects on individuals based solely on automated processing within the meaning of Article 22 GDPR.

To exercise your rights, email **jochem@umbra-ai.com**. We may verify your identity before fulfilling requests. Where Umbraic processes personal data as a Processor on behalf of a Client. That is, personal data contained in Client-uploaded documentation or in platform activity, the Client is the Controller and you should direct your request to that Client. If you contact us in relation to such data, we will refer your request to the relevant Client without undue delay and assist them in responding.

9. Digital Operational Resilience and Regulatory Access (summary: clauses 23.3 and 25 of the Standard Terms and Conditions govern)

Where Umbraic provides ICT services to Clients that are regulated financial entities subject to Regulation (EU) 2022/2554 (DORA), Umbraic acknowledges its role as an ICT third-party service provider within the meaning of DORA and commits to the following:

- **ICT risk assessment support:** We will provide Clients with information reasonably necessary to conduct ICT third-party risk assessments required under Article 28 of DORA, including documentation of our security controls, sub-processor arrangements, and resilience capabilities.

- **Regulatory and supervisory access:** National competent authorities, the European Banking Authority (EBA), ESMA, EIOPA, the ECB, and other relevant supervisory bodies shall have the right, upon lawful request, to inspect Umbraic's premises, access systems and data, and request information from Umbraic to the extent required by applicable law, including DORA. Umbraic will cooperate fully with all such lawful regulatory requests.
- **Critical TPSP designation:** Umbraic does not currently meet the criteria for designation as a critical ICT third-party service provider under Article 31 of DORA. If Umbraic is designated as critical by a Lead Overseer, Umbraic will notify affected Clients promptly and will cooperate with the Lead Overseer appointed by the European Supervisory Authorities in the conduct of its oversight activities as required by applicable law.

10. Children's Privacy

Our Services are intended for business use only and are **not directed at minors**. We do not knowingly collect data from individuals under 18.

11. Updates to This Policy

We may update this Privacy Policy from time to time. The latest version is always available on our website, and we will notify Clients of material changes. Where this Privacy Policy forms part of a Client's Agreement, changes to it are made in accordance with clause 20 of the Standard Terms and Conditions.

12. Contact

For questions, concerns, or to exercise your rights:

Privacy Contact
Umbraic B.V.
Prof. Tulpstraat 13
1018GZ Amsterdam, The Netherlands
Email: jochem@umbra-ai.com

If you are unsatisfied with our response, you may contact the **Dutch Data Protection Authority (Autoriteit Persoonsgegevens)**.