



# Privacy Policy

Umbraic B.V.

**Last updated:** 07/05/2026

**Data Controller:** Umbraic B.V.

**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”), 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 platform activity

We use this data to provide and secure the Services, authenticate access, deliver support, and communicate with Clients.

### 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 **permanently removed** from Umbraic’s active systems and backups within the retention window required for system integrity.



- Umbraic does not **access, share, or disclose** Clients' internal documentation to third parties except **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**.

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 and analyse traffic.

- **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:** (a) Umbraic shall maintain and make available to Client a current list of all subprocessors and AI providers used in the provision of the Service. (b) Umbraic shall provide Client with at least thirty (30) days' prior written notice of any intended addition or replacement of a subprocessor or AI provider, including details of the entity, its location, and the processing activities involved. (c) Client shall have the right to object to any proposed new subprocessor or AI provider on reasonable grounds, including data protection, regulatory, or information security concerns. If the objection cannot be resolved within fifteen (15) business days, Client may terminate the affected Service without penalty. (d) Umbraic shall impose contractual obligations on all subprocessors and AI providers that are materially equivalent to those set out in this 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
- Secure hosting within the **European Economic Area (EEA)**
- **Security framework:** Umbraic's security programme is aligned with recognised frameworks including ISO/IEC 27001 and the principles of NIS2. 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.

Client-uploaded compliance documents can be deleted by the Client at any time. Once deleted, Umbraic ensures they are not recoverable from active storage. 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.

To exercise your rights, email [jochem@umbra-ai.com](mailto:jochem@umbra-ai.com). We may verify your identity before fulfilling requests.

## 9. Digital Operational Resilience and Regulatory Access

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:** If Umbraic is designated as a critical ICT third-party service provider under Article 31 of DORA, 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.

## 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 periodically. The latest version will always be available on our website. Continued use of our Services constitutes acceptance of any updates.

## 12. Contact

For questions, concerns, or to exercise your rights:

### **Data Protection Officer**

Umbraic B.V.

Prof. Tulpstraat 13

1018GZ Amsterdam, The Netherlands

Email: [jochem@umbra-ai.com](mailto:jochem@umbra-ai.com)



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