SHADOW AI DISCOVERY · KANGO LABS LLC

Service Terms & Data Governance

Umbravi · Kango Labs LLC · umbravi.io

Version 2.0 · May 2026

PURPOSE OF THIS DOCUMENT

This document details how Umbravi works, what we do with your data, and what your rights are. If anything is unclear, email us at hello@umbravi.io.

NOT LEGAL ADVICE

Umbravi's Shadow AI Risk Reports provide technical and operational risk-observational guidance only. They do not constitute legal advice, formal certification, compliance determinations, or regulatory approval. Consult qualified legal counsel for formal compliance positions.

SERVICE LIMITATION

This service is not currently available to Government, Defense, or ITAR / FedRAMP-regulated organizations. Contact hello@umbravi.io to discuss your requirements.

1. What Umbravi does

Umbravi is a Shadow AI Discovery service. We analyze your organization's software (i.e., SaaS) spend data to identify AI tools in use, map their regulatory risk exposure, and deliver a branded Shadow AI Risk Report within 1–2 business days of receiving your data.

How the service works

The following steps describe exactly what happens from the moment you submit your intake to the moment your report is delivered:

1. **You complete the intake form.**
   You provide your name, work email, company name, company size, role, and preferred delivery platform (Microsoft OneDrive or Google Drive). This information is used solely to personalize your report and deliver it to the correct location.

2. **You upload your software (i.e., SaaS) spend export.**
   You upload a CSV, XLSX, or XLS export from your accounting, expense, or IT management tool. This file contains vendor names, amounts, and dates. We do not require login credentials, API access, or write permissions to any of your systems. Required fields: Vendor Name, Amount, and Transaction Date (the date each charge was processed). Department and Description are helpful but not required.

3. **You pay securely via Stripe.**
   Payment of $749 USD is processed by Stripe, a PCI-DSS Level 1 certified payment processor. Kango Labs LLC does not store your card information. Your payment confirmation is sent directly by Stripe.

4. **We analyze your data.**
   Umbravi's AI Auditor analyzes your spend export against our proprietary AI Tool Risk Database and the Umbravi AI Regulatory Reference. We identify AI-enabled tools, classify their risk level, and map regulatory exposure across applicable frameworks.

5. **We deliver your report.**
   Your completed Shadow AI Risk Report is uploaded to your chosen platform — Microsoft OneDrive or Google Drive — and shared with you via a secure, time-limited link with download permissions. We do not email your report as an attachment.

6. **Your data is purged.**
   All raw data — your spend export, intake form responses, and report files — is permanently deleted from our active systems 14 days after delivery. You retain your downloaded copy of the report.

2. What your report includes

Every Umbravi Shadow AI Risk Report includes three core deliverables:

AI tool inventory

A complete table of every AI-enabled tool identified in your software (i.e., SaaS) spend data, including tool name, risk classification (High / Medium / Low / Approved), applicable regulatory frameworks, and a risk score.

Regulatory Exposure Score

A composite score from 0 to 100 indicating where your organization's AI exposure surface sits based on the tools identified. A risk observation, not a compliance determination. Scored as: Low Exposure (80–100), Moderate (60–79), Elevated (40–59), or High Exposure (0–39).

Priority Action Plan

A tiered remediation plan with Immediate, 30-Day, and 60-Day actions your team can execute without a consultant. Actions are specific to the tools and frameworks identified in your report.

> **IMPORTANT LIMITATION**
>
> Reports generated from software (i.e., SaaS) spend data alone reflect probable risk exposure based on known tool behaviors — not your actual configuration or usage. Actual regulatory exposure depends on how tools are configured, what data they access, and your organization's specific regulatory profile. This report is a risk observation, not a compliance audit or legal opinion.

3. Data governance

We take the security and privacy of your data seriously. The following principles govern how we handle every piece of data you provide to Umbravi.

What data we collect

- **Contact information:** first name, last name, work email address.
- **Organization information:** company name, company size, your role.
- **Delivery preference:** your chosen platform (OneDrive or Google Drive).
- **Software spend export:** the file you upload (CSV, XLSX, or XLS).
- **Payment information:** processed entirely by Stripe — we never see your card details.
- **Optional context:** any additional information you choose to provide in the intake form.

What we do not collect

- Login credentials or passwords to any of your systems.
- API keys or programmatic access to your financial or IT systems.
- Write access to any platform or account.

- Any data beyond what you explicitly provide in the intake form.
- Behavioral data, cookies, or tracking identifiers from our web pages beyond minimal analytics.

How we process your data

The following principles govern how we handle every piece of data you provide.

PRINCIPLE	WHAT IT MEANS
Minimal-retention processing	Your raw software (i.e., SaaS) spend data is used solely to generate your report and is deleted from our active systems within 14 days of delivery. We do not use your data to train AI models, sell it to third parties, or retain it for any secondary purpose. All data is encrypted in transit (TLS 1.2+) and at rest (AES-256) throughout the engagement.
Platform-native delivery	Your report is delivered to your Microsoft OneDrive or Google Drive, where it remains under your control and your organization's existing security policies. We do not host your report on third-party infrastructure.
No model training	Umbravi's AI analysis pipeline operates under contractual zero-retention terms with our language model provider. Your data is not used to train, fine-tune, or improve any AI model.
Read-only access	We never request write access, admin access, or credentials to any of your systems or platforms.
Automatic purge	All raw data, processed files, and report delivery links are permanently deleted from our active systems 14 days after your report is delivered.
GDPR-aligned practices	Umbravi applies GDPR-aligned principles including data minimization, purpose limitation, and defined retention periods. A Data Processing Agreement is available upon request for organizations with EU data obligations. Contact hello@umbravi.io to discuss your requirements.
No third-party selling	We do not sell, license, or share your data with any third party for commercial purposes.
Tally (form processing)	Intake form submissions and file uploads are processed via Tally.so, a GDPR-compliant form platform. Files are stored in the Tally dashboard and accessed only by authorized Umbravi personnel. Raw files are deleted from Tally within 24 hours of download.
Stripe (payment processing)	Payments are processed by Stripe, Inc., a PCI-DSS Level 1 certified payment processor. Stripe's privacy policy governs the handling of your payment data.

4. Service terms

Payment and refunds

The service fee is **$749 USD**, charged at the time of intake submission via Stripe. If Umbravi does not identify at least one at-risk AI tool in your software (i.e., SaaS) spend data, your report is provided free of charge and a full refund is issued within 5 business days. All other sales are final. If you have a concern about your report, contact hello@umbravi.io within 14 days of delivery.

Delivery timeline

Umbravi commits to delivering your Shadow AI Risk Report within 1–2 business days of receiving your complete intake form submission and payment confirmation. Delivery times may vary during periods of high demand. If delivery will exceed 2 business days, we will notify you by email.

Acceptable use

You certify that you have the authority to submit the software (i.e., SaaS) spend data provided. You agree not to submit data belonging to another organization without authorization. You agree not to use the Umbravi service for any unlawful purpose.

Service limitations

Umbravi is not available to organizations operating under Government, Defense, ITAR, or FedRAMP regulatory frameworks. Submitting data from such an organization is a violation of these terms and may result in cancellation of service without refund.

Disclaimer of warranties

The Umbravi Shadow AI Risk Report is provided "as is" for informational, risk-observational, and operational guidance purposes only. It does not constitute a legal opinion, compliance determination, or certification. Kango Labs LLC makes no warranties, express or implied, regarding the completeness, accuracy, or fitness for a particular purpose of any report. Tool risk classifications are based on publicly available vendor information as of the date of report generation and are subject to change.

Limitation of liability

To the maximum extent permitted by law, Kango Labs LLC's total liability for any claim arising from the use of the Umbravi service shall not exceed the amount paid for the specific report giving rise to the claim. Kango Labs LLC is not liable for any indirect, incidental, consequential, or punitive damages.

Governing law

These terms are governed by the laws of the State of Georgia, United States, without regard to conflict of law principles. Any disputes shall be resolved in the courts of Fulton County, Georgia.

Changes to these terms

Kango Labs LLC reserves the right to update these terms at any time. Updated terms will be posted at umbravi.io. Continued use of the service after changes constitutes acceptance of the updated terms.

5. Your rights

Regardless of where you are located, Kango Labs LLC honors the following rights with respect to your personal data. To exercise any of these rights, email **hello@umbravi.io** with your request. We will respond within 1–2 business days.

Right to access

You may request a copy of the personal data Kango Labs LLC holds about you.

Right to correction

You may request correction of any inaccurate personal data we hold.

Right to deletion

You may request deletion of your personal data at any time. We will permanently delete all data associated with your intake within 5 business days of your request. Note: data is automatically purged 14 days after report delivery regardless of a deletion request.

Right to data portability

You may request a copy of your intake data in a machine-readable format.

Right to object

You may object to the processing of your personal data at any time. If you object prior to report delivery, we will cancel your intake and issue a full refund.

Right to withdraw consent

Where processing is based on consent, you may withdraw consent at any time without affecting the lawfulness of prior processing.

Right to lodge a complaint

If you are located in the EU or UK, you have the right to lodge a complaint with your local data protection authority.

6. Contact

For questions about these terms, your data, or the Umbravi service:

COMPANY

Kango Labs LLC

PRODUCT

Umbravi — Shadow AI Discovery

EMAIL

hello@umbravi.io

WEBSITE

umbravi.io

This document constitutes the complete Service Terms and Data Governance policy for the Umbravi Shadow AI Discovery service offered by Kango Labs LLC. It supersedes all prior representations, warranties, or agreements. Last updated: May 2026.