LEGAL · DATA PROTECTION

# Privacy Policy

SFER LABS LLC · Version 1.0 · Effective August 11, 2026

This Privacy Policy explains how SFER LABS LLC, 1201 N. Orange Street, Suite 7691, Wilmington, Delaware 19801-1186, USA ("Company," "we," "us") handles personal data in connection with Idelio, https://idelio.pro, our applications, support, research, sales and marketing activities (the "Service").

It applies to website visitors, prospects, account users, customers, research participants and people whose business contact information we lawfully obtain from other sources. When a business customer submits personal data to the Service and determines why and how it is processed, that customer is normally the controller and we act as its processor under our Data Processing Addendum at https://idelio.pro/legal/dpa.

## 1. Contact and representatives

Controller: SFER LABS LLC, 1201 N. Orange Street, Suite 7691, Wilmington, Delaware 19801-1186, USA. Privacy and data-protection contact: privacy@idelio.pro.

EEA representative: […]. UK representative: […].

## 2. Data we collect

Depending on your interaction, we may collect:

a) Account and identity data: name, username, email, organization, role, country, language, avatar, authentication identifiers and age/eligibility confirmations.

b) Transaction data: plan, credits, purchases, invoices, tax location, payment status, renewal, cancellation, refund and chargeback information. Our payment provider receives full payment credentials; we normally receive only limited transaction information.

c) Inputs, Outputs and project data: prompts, names, instructions, uploaded files and images, generated assets, edits, project settings, export history and associated metadata.

d) Usage and device data: IP address, approximate location derived from IP, browser, device, operating system, timestamps, page and feature events, session and account identifiers, referrer, UTM parameters, API calls, latency, error and performance information.

e) Security and trust data: login and access logs, fraud signals, moderation results, safety classifications, policy reports, investigation records and evidence associated with suspected abuse.

f) Communications and research data: support tickets, email, call notes or recordings where notified, feedback, survey answers, interview recordings/transcripts, waitlist responses, product requests and consent records.

g) Marketing and prospect data: business contact details, employer, role, professional profile, interests, campaign engagement, source and enrichment attributes.

h) Preference and rights data: cookie choices, marketing preferences, Global Privacy Control signal, opt-outs, suppression entries and privacy-request records.

Please do not submit sensitive or regulated data unless a feature is expressly approved for it. If Input contains another person's personal data, you are responsible for having an appropriate lawful basis and giving required notices.

## 3. Sources

We obtain data:

a) directly from you, your device and your use of the Service;
b) from an organization that provides your account;
c) from payment, authentication, support, analytics, security and AI providers;
d) from referrals, partners, event organizers or lead providers;
e) from public professional sources such as company websites, business directories and professional profiles; and
f) from lawfully licensed enrichment or marketing datasets.

Where EEA/UK personal data is obtained indirectly, we provide the information required by applicable law, normally in our first communication and within the applicable statutory period. We do not use unlawfully scraped private data or bypass access controls.

## 4. Why we use data and EEA/UK legal bases

| Purpose | Typical data | EEA/UK basis |
|---|---|---|
| Create and administer accounts; provide requested features; save and export projects | account, Input, Output, usage, transaction | contract; steps at your request before contract |
| Process payments, renewals, credits, refunds and tax records | account, transaction, location | contract; legal obligation; legitimate interests in accounting and fraud prevention |
| Route requests to AI providers and generate Output | Input, Output, technical metadata | contract; explicit consent only where required for sensitive data and expressly supported |
| Secure the Service, prevent fraud and enforce policies | account, content where necessary, device, security | legitimate interests in security, rights protection and service integrity; legal obligation where applicable |
| Support, debug and quality assurance | account, communications, relevant content, logs | contract; legitimate interests in reliable service and resolving issues |
| Account-linked product analytics, feature measurement, POC evaluation and product research | usage, account, survey, limited content samples where necessary | legitimate interests in understanding and improving the Service; consent where required by tracking law or for a study |
| Train or fine-tune a general/shared AI model on identifiable customer Input or Output | selected content and feedback | separate opt-in consent, or a separate written B2B arrangement with an appropriate lawful basis; never required for ordinary use |
| Deidentify data and create aggregate metrics, benchmarks and statistics | usage, performance, content-derived metrics | legitimate interests; data is no longer personal once irreversibly deidentified |
| Respond to legal requests, disputes and rights requests | relevant records | legal obligation; establishment, exercise or defense of legal claims |
| Send service and transactional communications | account, transaction | contract; legal obligation |
| Promote our products by email or professional messaging | prospect, account, engagement | consent where required; otherwise legitimate interests subject to direct-marketing and ePrivacy rules |

| Purpose | Typical data | EEA/UK basis |
|---|---|---|
| Retargeting, audience matching and cross-context behavioral advertising | identifiers, device, engagement, inferred interests | consent in EEA/UK and other opt-in regions; opt-out and other bases only where law permits |
| Telephone or SMS marketing | phone, consent and campaign records | prior consent where required; never based solely on acceptance of the Terms |
| Lead generation, enrichment and market segmentation | business contact, employer, public/licensed data, interests | legitimate interests where the balancing test supports it; consent where required; right to object |

Our legitimate interests include providing a useful and secure product, measuring demand, prioritizing features, finding business customers, preventing abuse and defending rights. We consider necessity, reasonable expectations, sensitivity and safeguards. You may object as described below.

Where processing is based on consent, you may withdraw it at any time without affecting earlier lawful processing. We do not condition ordinary Service access on optional marketing, advertising or model-training consent.

## 5. AI processing and human review

The Service may send Input, Output and technical data to the AI providers in our Technology & Vendor Register. Providers may use automated safety systems and, in limited cases, authorized human review for abuse detection, incident response, support or legal compliance. Flagged material may be kept longer than ordinary requests.

We seek commercial configurations that do not use API customer content to train shared models, but practices vary by provider, endpoint, feature and plan. We do not promise zero-data-retention unless a specific feature is expressly identified as such. Do not submit secrets or sensitive personal data based solely on an assumption that an AI provider stores nothing.

We may review a minimized sample of interactions for QA, safety, debugging or product research under access controls. Training or fine-tuning shared/general models on identifiable customer content requires a separate voluntary opt-in or written B2B terms. We may use properly deidentified statistics and performance measurements to improve products and evaluate models.

## 6. Analytics, cookies and advertising

We use cookies, local storage, pixels, SDKs and similar technology as described in the Cookie & Tracking Policy. In regions requiring prior consent, non-essential analytics, personalization, session replay and advertising remain disabled until consent. You can change your choices at any time through the Cookie Settings control available from the website footer.

Where applicable, you can opt out of sale, sharing or processing for targeted advertising through the Your Privacy Choices control available through the website or account, or by contacting privacy@idelio.pro. We treat a valid Global Privacy Control signal as an opt-out for the browser/device and profile we can reasonably associate with it, where required.

## 7. Marketing choices

You can unsubscribe from marketing email through the link in each message. You can withdraw SMS consent by using the stated keyword and telephone consent through the method provided in the call or at privacy@idelio.pro. We maintain a limited suppression record so we can respect your choice.

Service, security, billing and legal messages are not marketing opt-ins, although their content must remain limited to the relevant operational purpose.

We do not use purchased or enriched contact data unless the source, permitted uses, provenance and required notices have been reviewed. We do not use sensitive data to infer marketing audiences without valid permission.

## 8. When we disclose data

The Technology & Vendor Register at https://idelio.pro/legal/technology-vendor-register identifies current technologies, subprocessors and other recipients, including their roles, purposes and available retention/transfer information. Provider additions, removals or substitutions within purposes and data categories already disclosed here may be recorded in that Register without republishing this Policy. We update this Policy and, where required, obtain a new choice before a materially new purpose, data category or more intrusive practice begins.

We may disclose data to:

a) infrastructure, hosting, database, storage, security, communications, support, authentication, analytics and AI providers acting for us;

b) Paddle and financial, tax and fraud partners for transactions;

c) advertising, attribution, audience and campaign providers, only subject to required consent or opt-out rights;

d) professional advisers, auditors and insurers under confidentiality duties;

e) a buyer, investor or successor in a corporate transaction, subject to appropriate safeguards;

f) authorities or other parties when reasonably necessary to comply with law, protect rights or address fraud, security or safety; and

g) other parties at your direction or with your consent.

Current subprocessors are listed at https://idelio.pro/legal/technology-vendor-register. We do not disclose Input or Output to data brokers for their independent marketing. Certain advertising disclosures may be considered "sale," "sharing" or targeted advertising under U.S. state law even when no money changes hands; applicable choices are described above and in the U.S. State Privacy Notice.

## 9. International transfers

We are established in the United States and providers may process data in the United States and other countries. Where EEA, UK or Swiss law restricts transfers, we use an available adequacy decision, the applicable Standard Contractual Clauses, the UK Addendum/IDTA, or another lawful mechanism. We assess transfer risks and use supplementary measures where appropriate. Contact privacy@idelio.pro for information or an available copy of relevant safeguards, subject to necessary redactions.

## 10. Retention

We keep personal data only as long as reasonably necessary for the stated purpose, then delete or deidentify it. Default maximum periods are:

| Record | Default period |
|---|---|
| Account profile | account life plus 30 days |
| Projects, Inputs and Outputs | until user deletion or account closure, then up to 30 days in active systems |
| Backups | rolling maximum of 90 days; deleted during normal secure rotation |
| Provider-held AI request data | shortest supported vendor period shown in the Technology & Vendor Register; longer for flagged abuse or legal holds |
| Account-linked product telemetry | 24 months |

| Record | Default period |
|---|---|
| Security/access logs | 12 months; longer for an active incident or claim |
| Trust and safety cases | 3 years after closure or longer when needed for law or claims |
| Support correspondence | 3 years after closure |
| Billing, tax and accounting | 7 years or the locally required period |
| Prospect and campaign records | 24 months after the last meaningful interaction |
| Consent and suppression evidence | 6 years after withdrawal or last communication |
| Research interview/survey raw data | 24 months or the shorter period stated for the study |
| Irreversibly deidentified aggregates | may be retained indefinitely |

We may retain a limited record longer when required by law, to resolve a dispute, enforce agreements or maintain a suppression list. Deletion from backup does not require restoring and altering an isolated backup; if restored, the deletion rule is reapplied.

## 11. Your rights

Depending on where you live, you may have rights to access, correct, delete, restrict or object to processing, receive portable data, withdraw consent, opt out of targeted advertising/sale/sharing/profiling, limit certain sensitive-data uses, and appeal a denied request. EEA/UK users may object at any time to direct marketing, and may object to processing based on legitimate interests.

Submit a request through the Your Privacy Choices control available through the website or account, or email privacy@idelio.pro. We will verify it proportionately and respond within the applicable period. Authorized agents may act where permitted, subject to verification of authority. We will not discriminate against you for exercising a privacy right.

You may complain to your local supervisory authority. EEA authority contacts are available through the European Data Protection Board; UK users may contact the ICO. We invite you to contact us first, but this is not required.

## 12. Automated decisions

We may use automated systems for fraud, security, moderation, routing and product personalization. We do not use the Service to make solely automated decisions about individuals that produce legal or similarly significant effects unless we provide a specific notice, lawful basis and required safeguards. Customers are prohibited from using the Service for unapproved high-impact decisions.

## 13. Security

We use administrative, organizational and technical measures designed for the nature and risk of the data, including access controls, encryption in transit, logging, vulnerability management, backup controls and incident procedures. No system is completely secure. If law requires notice of a breach, we will provide it to affected parties and authorities within applicable deadlines.

## 14. Children

The Service is not directed to anyone under 18 and we do not knowingly collect their personal data. If you believe a child submitted data, contact privacy@idelio.pro. We will investigate and delete it where required.

## 15. Changes

We may update this Policy to reflect legal, technical or business changes. We will post the effective date and give additional notice for material changes. A new incompatible purpose will receive an appropriate notice and lawful basis; an updated policy alone does not create consent.

## 16. Contact

SFER LABS LLC 1201 N. Orange Street, Suite 7691, Wilmington, Delaware 19801-1186, USA Privacy: privacy@idelio.pro