LEGAL · DATA PROTECTION

Data Processing Addendum

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

This Data Processing Addendum ("DPA") forms part of the agreement between the customer identified in an order form or account ("Customer") and SFER LABS LLC, 1201 N. Orange Street, Suite 7691, Wilmington, Delaware 19801-1186, USA ("Company") for Idelio (the "Agreement"). It applies when Company processes Customer Personal Data on Customer's behalf.

1. Definitions

"Applicable Data Protection Law" means privacy and data-protection law applicable to the processing, including where relevant the GDPR, UK GDPR, Swiss FADP and U.S. state privacy laws.

"Customer Personal Data" means personal data contained in Input or otherwise submitted by or for Customer to the Service that Company processes as processor or service provider. It excludes data Company processes as independent controller, such as Customer account administration, billing, security, direct business relationship management and Company's own legal compliance, as described in the Privacy Policy.

"Controller," "processor," "personal data," "processing," "data subject" and "personal data breach" have the meanings in Applicable Data Protection Law. "Subprocessor" means another processor engaged by Company to process Customer Personal Data.

2. Roles and instructions

Customer is the controller or a processor acting under a controller's authority. Company is Customer's processor/service provider for Customer Personal Data. Each party will comply with its obligations under Applicable Data Protection Law.

Company will process Customer Personal Data only:

a) to provide, secure and support the Service as described in the Agreement and Annex I;
b) on Customer's documented instructions through use and configuration of the Service;
c) as required by law, after informing Customer unless law prohibits notice; or
d) as otherwise agreed in writing.

Company will notify Customer if, in its reasonable opinion, an instruction infringes Applicable Data Protection Law and may suspend the affected processing while the parties resolve it.

Customer is responsible for its instructions, required notices, lawful bases, data accuracy and permissions. Customer will not submit sensitive, special-category, biometric, health, children's or other regulated data unless the parties expressly approve the data and safeguards in an order form.

Company will not sell Customer Personal Data; retain, use or disclose it outside the business purposes in the Agreement; combine it with personal data from other sources except as permitted by applicable U.S. state law to provide the Service; or use it for targeted advertising. Company certifies that it understands and will comply with these restrictions.

3. Confidentiality and personnel

Company ensures that persons authorized to process Customer Personal Data are bound by confidentiality and receive privacy and security training appropriate to their role. Access is limited to personnel who need it for authorized purposes.

4. Security

Company will maintain measures designed to protect Customer Personal Data against unauthorized or unlawful processing and accidental loss, destruction, alteration or disclosure. Current minimum measures are in Annex II. Company may update measures without materially reducing overall protection.

Customer is responsible for secure configuration of its account, credentials, access permissions, endpoints, exports and integrations.

5. Subprocessors

Customer gives general written authorization for the Subprocessors listed at https://idelio.pro/legal/technology-vendor-register. Company will:

a) impose data-protection obligations providing materially equivalent protection;
b) remain responsible for each Subprocessor's performance to the extent required by law and the Agreement;
c) maintain a current public register; and
d) provide at least 30 days' notice before a new Subprocessor begins processing Customer Personal Data, where Customer has subscribed to notices.

Customer may object during the notice period on reasonable data-protection grounds. The parties will work in good faith on a commercially reasonable alternative. If none is available, Customer may stop using the affected feature or terminate the affected Service and receive a pro-rata refund for its unused prepaid portion. This is Customer's sole remedy for a justified Subprocessor objection, except where law requires otherwise.

6. Assistance

Taking into account the nature of processing and information available, Company will reasonably assist Customer with:

a) data-subject requests;
b) security and breach obligations;
c) data-protection impact assessments and prior consultations; and
d) information needed to demonstrate compliance.

If a data subject contacts Company about Customer Personal Data, Company will refer the request to Customer unless law permits or requires a direct response. Customer is responsible for responding. Additional assistance outside standard Service functionality may be charged at reasonable rates if agreed in advance, except where caused by Company's breach.

7. Personal data breaches

Company will notify Customer without undue delay after becoming aware of a confirmed breach of Customer Personal Data and provide information reasonably available about its nature, likely consequences, affected data and mitigation. Notification is not an admission of fault. Customer is responsible for regulatory and data-subject notifications unless law assigns that duty to Company.

8. Return and deletion

During the term, Customer may access or export Customer Personal Data through available functionality. After termination or Customer's documented deletion instruction, Company will delete or return Customer Personal Data within 30 days, except for:

a) encrypted backups deleted through normal rotation within 90 days;
b) data required by law or reasonably needed for legal claims, isolated and protected; and
c) information irreversibly deidentified so it no longer constitutes personal data.

Subprocessor deletion follows its documented schedule in the register and applicable contract.

9. Audits

Company will make reasonably current third-party certifications, summaries, security materials and compliance information available under appropriate confidentiality. No more than once annually, unless required by a regulator or following a material incident, Customer may request additional written information reasonably necessary to verify compliance.

If that information is insufficient, Customer may conduct an audit through an independent qualified auditor, on reasonable notice, during business hours, without accessing other customers' data or disrupting systems. The parties will agree scope and confidentiality. Customer bears cost unless the audit identifies a material Company breach.

10. International transfers

For restricted transfers of Customer Personal Data from the EEA, the parties incorporate the European Commission Standard Contractual Clauses adopted by Decision (EU) 2021/914 ("EU SCCs") as follows:

a) Module Two applies where Customer is a controller and Company is a processor;
b) Module Three applies where both Customer and Company are processors;
c) Clause 7 (docking) applies;
d) for Clause 9, Option 2 and a 30-day notice period apply;
e) the optional language in Clause 11 does not apply unless required in the Customer's jurisdiction;
f) in Clauses 17 and 18, the eligible EEA Member State specified in Annex III applies;
g) Annexes I-III of this DPA complete the corresponding SCC annexes.

For UK restricted transfers, the UK International Data Transfer Addendum to the EU SCCs, as issued by the ICO and updated from time to time, is incorporated with the information in this DPA. For Swiss transfers, references in the EU SCCs are adapted as required by the Swiss FADP, and competent Swiss authorities retain their powers.

An applicable adequacy decision or other lawful transfer mechanism takes precedence while valid. The parties will cooperate on a replacement if a mechanism becomes invalid. Company will provide information reasonably needed for transfer assessments and use supplementary measures appropriate to risk.

11. Liability and precedence

The Agreement's liability limitations apply to this DPA to the maximum extent permitted by law. Nothing in this DPA limits data-subject rights or liability that cannot be limited under the EU SCCs or Applicable Data Protection Law.

If documents conflict on Customer Personal Data, the order is: EU SCCs/mandatory transfer terms, this DPA, signed order form, Agreement. This DPA does not change Company's independent-controller processing described in the Privacy Policy.

12.1. Annex I - Processing details

Parties: Customer as identified in the account/order form; Company as identified above. Subject and duration: provision of the Service for the Agreement term plus deletion/backup periods. Nature and purpose: hosting, routing to AI models, generation/transformation, storage, account access, export, support, security, moderation and Customer-directed integrations. Data subjects: Customer's authorized users and individuals whose data Customer lawfully includes in Input. Data categories: account identifiers; prompts, uploaded content and Output; project metadata; usage, device, security and support data related to Customer instructions. Sensitive data: not permitted unless expressly approved in an order form with additional safeguards. Frequency: continuous or as initiated by Customer. Retention: Section 8 and the Technology & Vendor Register. Competent supervisory authority: determined under Clause 13 of the EU SCCs based on the exporter and applicable law.

12.2. Annex II - Minimum technical and organizational measures

a) documented security and privacy responsibilities;
b) role-based access, least privilege, credential controls and MFA for privileged access;
c) encryption in transit using current industry-standard protocols and encryption at rest where supported by the relevant storage layer;
d) segregated production environments and tenant-access controls appropriate to architecture;
e) logging, monitoring, incident detection and response procedures;
f) vulnerability, dependency and patch management;
g) secure software-development and change-review practices;
h) backups, restoration testing and defined deletion rotation;
i) vendor due diligence and contractual security/data-protection controls;
j) personnel confidentiality and recurring security awareness;
k) business continuity, recovery and incident communication procedures;
l) processes for data-subject requests, retention, deletion and transfer assessment; and
m) periodic risk review and testing proportionate to the Service.

The measures in this Annex describe the controls maintained for the Service as of the effective date.

12.3. Annex III - Transfer selections

EEA governing Member State for SCC purposes: Poland.
Exporter contact: as stated in Customer's order form.
Importer contact: privacy@idelio.pro.
Subprocessors: https://idelio.pro/legal/technology-vendor-register.