

Data Processing Agreement

Updated 19 October 2026 · version 1.2

AI Generation Oy · Business ID 3365357-7 · VAT ID FI33653577

This data processing agreement ("DPA") forms part of the Aigen PackTrack terms and meets the requirements of Article 28 of the EU General Data Protection Regulation. It takes effect when the customer accepts the terms and remains in force as long as we process personal data on the customer's behalf.

1. Parties

- Controller: the customer company ("customer").
- Processor: AI Generation Oy, Business ID 3365357-7, Selkämerenkatu 12 B 34, 00180 Helsinki ("processor").

2. Subject, nature and purpose

The processor prepares the customer's packaging data for its report to the producer organisation while the service is used. Processing comprises storing, organising, classifying, calculating, presenting to the customer's users, exporting and deleting data.

3. Data subjects and categories

- Data subjects: the customer's users and supplier and other contacts to the extent the customer brings them into the service.
- Data: names and contact details in uploaded material, user and membership identifiers, and the audit log.
- The service is not intended for special categories of personal data, and the customer must not upload them.

4. Instructions

The processor processes personal data only on the customer's documented instructions: the terms, this agreement and the customer's choices in the service. They include transfers of personal data to third countries on the transfer bases stated on the subprocessors page. The processor tells the customer if it considers an instruction unlawful.

5. Confidentiality

Only those of the processor's personnel whose duties require it, and who are bound by confidentiality, process personal data.

6. Security (Article 32)

- Encryption in transit (HTTPS/TLS).
- Authentication by email and password (verified email; the password is stored only as a hash); HttpOnly, SameSite session cookies; a bot check on sign-up and password reset; origin checks and rate limits on state-changing requests.

- Access control by company and role; companies' data is separated.
- Actions recorded in an audit log.
- Payment event notifications are verified by signature.
- Database operated by the hosting provider, with the provider's backups.

7. Subprocessors

The customer gives general prior authorisation to use the subprocessors listed on the subprocessors page (<https://packtrack.aigen.fi/subprocessors?lang=en>). The processor binds them to data protection obligations at least equivalent to this agreement and remains responsible for them. New or changed subprocessors are announced at least 30 days in advance. If the customer objects on reasonable grounds, it may terminate the plan and receive a refund for unused time.

8. Transfers outside the EU/EEA

If a subprocessor is outside the EU or can access data from there, the transfer is protected by the Commission's standard contractual clauses (Implementing Decision (EU) 2021/914) or an adequacy decision (EU-US Data Privacy Framework, Implementing Decision (EU) 2023/1795). Each subprocessor's transfer basis is on the subprocessors page.

9. Assistance and personal data breaches

The processor reasonably assists the customer with data subject requests, breach notification, impact assessments and prior consultation. It notifies the customer of a personal data breach without undue delay, including the Article 33(3) information available to it.

10. Return and deletion

The owner can download the data in a machine-readable format and delete the company and its data in the service. When the service to the customer ends (the agreement ends or the company is deleted), the processor returns or deletes the personal data at the customer's choice and deletes existing copies. Otherwise the processor deletes the customer's personal data on request and provides it in a machine-readable format before deletion if asked.

Deletion does not cover data the law requires us to keep. After a user's account is deleted, the processor keeps, as its own controller processing, only a minimal proof of acceptance of the terms and this agreement for 3 years, as set out in the privacy notice. Unused accounts: if nobody has signed in to or used a user's account for 24 months, the processor sends a warning by email and deletes the account 30 days later unless someone signs in before then. If the user is the company's only owner, the company's data is deleted too; however, the only owner's account is not deleted while the company has a running subscription. The deletion works like a user's own account deletion (privacy notice). Data is removed from backups as the backups rotate.

11. Audits

The processor provides the information needed to demonstrate compliance with this agreement. The customer may carry out or commission an audit with reasonable notice and at its own

cost, at most once a year, unless a breach or an authority requires otherwise.

12. Liability and precedence

Liability is subject to the limitation in the terms to the extent permitted by Article 82 GDPR. For personal data processing, this agreement prevails over the terms.