Data Processing Agreement

The processor terms that apply when your workspace holds personal data. Available as a template to sign.

October 29, 2026 · Asynchrone Space · asynchrone.space/legal/dpa

Parties and scope

This data processing agreement (the “DPA”) is a template for customers of Asynchrone Space. It is entered into between the customer named in the signature block (the “Customer”, acting as controller) and Preskater, which operates Asynchrone Space (the “Processor”). Bracketed fields are completed when it is signed.

It applies to the personal data that Customer and its users submit to the service described in the agreement between the parties (the “Agreement”). If Customer has accepted this DPA in an order form or in a signed copy, that copy prevails over this page. If a term here conflicts with the Agreement on data protection, this DPA prevails; otherwise the Agreement prevails.

Roles and instructions

Customer determines the purposes and means of the processing and is responsible for its lawfulness, including having a legal basis for the personal data of its users, clients and candidates that it puts into the service. The Processor processes that data only as a processor and only on Customer's documented instructions: the Agreement, this DPA, the configuration Customer chooses in the product, and Customer's use of its features. The Processor does not sell personal data, does not use it for advertising, and does not use it to train models for other customers.

Processor obligations

The Processor will:

- Process personal data only on documented instructions, including for transfers to a third country, unless required by EU or Member State law — in which case it informs Customer before processing, unless the law forbids it.
- Ensure that personnel authorised to process personal data are bound by confidentiality and reach it only where their role requires it.
- Implement and maintain the measures described in section 4.
- Assist Customer in responding to data subject requests and in meeting its obligations under Articles 32 to 36 of the GDPR, taking into account the nature of the processing.
- Notify Customer of a personal data breach within the time set out in section 7.
- Make available the information needed to demonstrate compliance and allow the audits in section 9.
- Return or delete personal data at the end of the provision of services, as set out in section 10.

Security measures

The Processor implements the measures below, describes them in the same terms on the security page, and reviews them as the service changes:

- TLS for all traffic between browsers, the applications and the database.
- AES-256-GCM encryption of repository and integration tokens before they are stored; scrypt hashing of passwords.
- Role-based access control inside every workspace (owner, admin, member, viewer) plus per-file permissions.
- Per-IP rate limiting on authentication endpoints, shared across replicas through the database.
- Platform staff access only through a separate internal application protected by password and TOTP, with every action written to a platform audit trail; support impersonation is a single-use handoff valid for one minute that opens a one-hour session the workspace can see and end.
- Least-privilege access to production systems, with credentials held in Kubernetes Secrets rather than in the repository.
- Application and dependency updates on every change to the main branch, checked by CI before release.

Sub-processors

Customer authorises the Processor to engage the sub-processors listed at asynchrone.space/legal/subprocessors: hosting and PostgreSQL, transactional email, the AI assistant, repository sync, payment processing, and a sign-up captcha. That page states each provider's purpose, location and transfer mechanism and is incorporated into this DPA.

The Processor notifies Customer at least 30 days before a new sub-processor starts processing personal data, by email to the workspace billing contact and by updating that page. Customer may object within those 30 days on reasonable data-protection grounds. If the objection cannot be resolved, Customer may terminate the affected part of the service and receive a pro-rata refund of prepaid fees.

The Processor imposes data-protection obligations on each sub-processor that are no less protective than this DPA, remains liable to Customer for their performance, and discloses the identity and location of each one.

International transfers

Personal data is hosted in the European Union, on OVHcloud infrastructure in Gravelines, France. Where a sub-processor processes personal data outside the EEA, the transfer relies on the Standard Contractual Clauses of Commission Decision 2021/914 (module two, controller to processor) and, where the provider is certified under the EU-US Data Privacy Framework, on that framework. The Processor completes any additional documentation Customer reasonably needs to evidence the transfer.

Security incidents

The Processor notifies Customer of a personal data breach without undue delay and in any event within 24 hours of becoming aware of it, by email to the workspace owners and to the security contact Customer has registered. The notification states, to the extent known at the time:

- what happened, with the date, time and duration (or an estimate);
- the categories and approximate number of data subjects and records concerned;
- the likely consequences;
- the measures taken or proposed to address the breach and mitigate its effects;
- a contact point for follow-up.

Where the information is not all available at once, it is delivered in phases without further delay. The Processor supports Customer's own notification duties, but Customer remains responsible for notifying supervisory authorities and data subjects. A notification is not an admission of fault.

Data subject requests and assistance

The product lets users access and correct their own profile data, lets workspace owners restrict or revoke access, and exports CRM and HR records as CSV. A complete export of all workspace data is not self-service today: Customer may request one from privacy@asynchrone.space and receives it within 30 days, in a structured, commonly used format. Deletion is scheduled by a workspace owner and completes automatically 30 days later.

If a data subject contacts the Processor directly, it redirects them to Customer unless the law requires it to respond itself. For data protection impact assessments and prior consultations with a supervisory authority, the Processor provides the information in this DPA and on the security page free of charge; where a request needs substantial additional work, it agrees the scope and cost with Customer in advance.

Audit rights

The Processor makes available to Customer:

- this DPA, the security page and the current sub-processor list;
- on request, and at most once a year, a completed security questionnaire;
- on request, a summary of the most recent penetration test or security assessment, with findings that concern other customers removed.

Customer may audit the Processor's processing facilities only where a supervisory authority requires it or after a confirmed personal data breach attributable to the Processor, with at least 30 days' written notice, during business hours, under confidentiality, and without access to other customers' data. Customer bears the cost, unless the audit reveals material non-compliance, in which case the Processor reimburses the reasonable cost of the audit.

Return and deletion on termination

While the Agreement is in force, Customer can export records from the modules that support export at any time. On termination, Customer may request a complete export within 30 days, and the Processor provides it in a structured, commonly used format.

After that window, the Processor deletes the personal data — including uploaded file bytes, which are stored as PostgreSQL large objects — within 30 days, unless EU or Member State law requires it to be retained. Retained records are limited to platform audit events and trial claim records, both disclosed in the privacy policy. On written request, the Processor confirms the deletion in writing.

Liability

Each party's liability under this DPA is subject to the limitations and exclusions in the Agreement. Nothing in this DPA limits the rights of data subjects under the GDPR.

Term, changes and governing law

This DPA takes effect when it is signed, or when Customer accepts it in an order form, and remains in force for as long as the Processor processes personal data for Customer. It is governed by the law and jurisdiction stated in the Agreement.

The Processor may update this DPA to reflect a change in the service, a change of sub-processor under section 5, or a change in law. Updates are published on this page with a new date and do not reduce the protections in force when Customer signed.

Signing

To execute this DPA, complete the block below, sign it and return it to privacy@asynchrone.space. We countersign and return a copy, usually within five business days.

Customer

Legal name: [legal name]

Registered address: [address]

Name and role: [name, role]

Signature: _____

Date: [date]

Asynchrone Space (Preskater)

Name and role: [name, role]

Signature: _____

Date: [date]