Data Processing Agreement — template

DPA template v1.0 · 2026-06-10 · Permia SAS · permia.eu/documents

This is the template version, published before any conversation so your lawyer or your own client can read it first. The signed version is executed at contract, with the parties and annexes completed.

§ 1 · Parties and roles

This Data Processing Agreement (“DPA”) is entered into between the Customer (the controller, or a processor acting for its own controllers) and Permia SAS, a société par actions simplifiée under French law (the processor). It forms part of the service agreement and is governed by Regulation (EU) 2016/679 (GDPR), in particular Article 28.

§ 2 · Subject matter and nature of processing

Permia hosts persistent development environments for the Customer: the server, the persistent terminal session, the storage and the network path to them, operated in a datacenter in France. Permia supplies no access to any AI model, resells no model API, and holds no credential to any model account. Any model the Customer’s agents call is reached with the Customer’s own keys, under the Customer’s own contract with the model provider: that provider is not Permia’s sub-processor, and its GDPR role toward the Customer (processor or independent controller) is defined by that contract, not by this DPA.

§ 3 · Location of processing

All processing under this DPA is performed in France. Permia transfers no Customer data outside the European Union and is subject to no non-EU parent company.

§ 4 · Sub-processors

The authorised sub-processors at the date of this version are published at permia.eu/documents/sub-processors: OVHcloud SAS, datacenter operator, France. Permia gives the Customer thirty days’ written notice before adding or replacing a sub-processor; the Customer may object on reasonable data-protection grounds.

§ 5 · Security and operational access

Permia implements the technical and organisational measures described in § 5 of the Acceptable Use Policy: isolation per environment on a dedicated instance, restrictive permissions on secrets files, TLS in transit, least-privilege administrative access, and, from the micro-VM tier, at-rest encryption with a key not held by the operator. Operational access for provisioning, backup and incident response is logged, and the log is retained for twelve months. Permia does not read Customer code in the course of operations and does not use the Customer’s model keys, a prohibition stated in § 3 of the Acceptable Use Policy and enforced through the access controls above; on the early-access tier this is an organisational commitment, and technical impossibility of reading data at rest applies from the micro-VM tier.

§ 6 · Assistance, audits and breach notice

Permia assists the Customer with data-subject requests and with Articles 32 to 36 GDPR, makes available the information necessary to demonstrate compliance, allows audits, and notifies the Customer of a personal data breach without undue delay and at the latest within 48 hours of becoming aware of it.

§ 7 · Deletion and return

At the end of the contract, Permia returns the contents of the Customer’s environments on request and deletes all copies within thirty days, except where French law requires longer retention of billing records.

§ 8 · Governing law

This DPA is governed by French law. The competent courts are those of Paris, France.

```
Annex A (processing details) and Annex B (signatures) are completed at contract; the
exit runbook is delivered with them. The deletion-and-return commitment is § 7 above.
```