



LEGAL — TEMPLATE

Data Processing Addendum

Between AdaptivMapr (Processor) and Customer (Controller)

Customer-fillable template — version 2026-06-05.

Complete the signature block on the last page, then sign and return to dpo@adaptivmapr.com to formalize.

This Data Processing Addendum ("DPA") supplements the AdaptivMapr Terms of Service (the "Agreement") entered into between you ("Customer") and AdaptivMapr ("Processor"). It governs the processing of Personal Data carried out by AdaptivMapr on behalf of Customer in the course of providing the Services. In the event of any conflict, this DPA prevails over the Agreement with respect to data protection matters.

Article 1 — Definitions

Unless otherwise defined below, capitalised terms have the meanings given to them in Article 4 of the EU General Data Protection Regulation 2016/679 ("GDPR") and, where applicable, the Swiss Federal Act on Data Protection 2020 ("nFADP").

- Personal Data — any information relating to an identified or identifiable natural person, processed by AdaptivMapr on behalf of Customer in connection with the Services.
- Data Subject — the identified or identifiable natural person to whom Personal Data relates.
- Processing — any operation performed on Personal Data, whether or not by automated means.
- Controller — the natural or legal person that determines the purposes and means of the Processing.
- Processor — the natural or legal person that processes Personal Data on behalf of the Controller.
- Subprocessor — any Processor engaged by AdaptivMapr to assist in fulfilling its obligations under the Agreement.
- Personal Data Breach — a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.
- SCCs — the Standard Contractual Clauses adopted by the European Commission in Decision (EU) 2021/914 of 4 June 2021.

Article 2 — Subject matter and duration

AdaptivMapr processes Personal Data on behalf of Customer for the sole purpose of providing the Services as described in the Agreement. Processing begins on the effective date of the Agreement and continues for the term of the Agreement, plus any additional period during which AdaptivMapr is required to retain Personal Data for the return-or-deletion process in Article 13.

Article 3 — Nature and purpose of Processing

AdaptivMapr processes Personal Data to:

- Receive column headers and (in schema-only mode) up to three sample row values per column, with each cell truncated to 80 characters, from Customer's tabular inputs.
- Run the deterministic, heuristic, and (where invoked) LLM layers of the mapping cascade to recommend a target field for each column.
- Return the mapping recommendations, validation results, and transformed rows to Customer.
- Authenticate API calls, enforce rate limits, meter usage, and generate audit log records.

Schema-only mode (default). Full row content remains in the Customer's tenant and never leaves it. Only the clamped sample described above (header text plus up to 3 rows of up to 80 characters per cell) is persisted by AdaptivMapr as `parsed_sample` for the duration of the active session, and is cleared on commit or by the retention sweep in Article 13. The clamp is enforced at the HTTP edge (`clampForSchemaOnly()`) and re-applied defensively at the LLM call boundary; there is no code path that lets full-row content into a schema-only workspace.

Full-data mode. When Customer has executed the phi-cloud BAA addendum and explicitly elects full-data mode for a given request, full row content is forwarded to phi-cloud under that BAA. AdaptivMapr itself does not invoke the full-data LLM call.

Article 4 — Categories of Personal Data

The categories of Personal Data Processed depend on Customer's configuration but typically include:

- Identifiers and contact data (name, email, phone) where these appear as column headers or sample values in Customer's inputs.
- Employer / customer / patient identifiers where Customer uses a vertical pack (e.g. healthcare templates) under the appropriate BAA / DPA executed with phi-cloud.
- Account contact data of Customer personnel (workspace owners, admins, billing contacts).
- Technical data — IP address, user-agent, API key identifier, request metadata.

AdaptivMapr does not knowingly process special categories of personal data (GDPR Art. 9) unless the Customer has executed the phi-cloud BAA addendum and the data flows through that integration.

Article 5 — Categories of Data Subjects

- Customer's personnel (workspace users, admins).
- Customer's end users, members, customers, patients, or counterparties whose data appears in the records Customer submits to AdaptivMapr.

Article 6 — Customer's responsibilities

- Customer is the Controller of Personal Data submitted to the Services and is responsible for the lawful collection, use, and transfer of that data.
- Customer warrants that it has all necessary consents, notices, or other lawful bases to enable AdaptivMapr to process Personal Data for the purposes set out in Article 3.
- Customer is responsible for configuring schema-only mode where the mode is appropriate to its compliance posture, and for obtaining the phi-cloud BAA / DPA before invoking full-data mode.
- Customer is responsible for the security of its API keys.

Article 7 — AdaptivMapr's responsibilities

AdaptivMapr will:

- Process Personal Data only on documented instructions from Customer (the Agreement, this DPA, and any written instructions Customer provides through the dashboard or API).
- Ensure that personnel authorised to process Personal Data are bound by appropriate confidentiality obligations.
- Implement technical and organisational measures consistent with Article 32 GDPR. A current description of those measures is maintained at adaptivmapr.com/legal/security and is incorporated here by reference.
- Assist Customer in fulfilling its obligations under Articles 32–36 GDPR, including responding to data subject requests and notifying breaches.
- Make available all information necessary to demonstrate compliance with this DPA, subject to reasonable confidentiality protections.

Article 8 — Subprocessors

Customer grants general authorisation to AdaptivMapr to engage the Subprocessors listed below. AdaptivMapr enters into written agreements with each Subprocessor that impose data protection obligations no less protective than this DPA.

- Cloudflare Inc. — Workers compute (API + dashboard), KV (rate-limit counters, statistics cache), R2 (asset storage), DNS, DDoS protection, edge cache. Location: US / global PoPs.
- Supabase Inc. — Postgres database (EU instance): authentication, sessions, rate-limit ledger, audit log, upload metadata (parsed_sample clamped to <=3 rows x <=80 chars/cell; parsed_rows null in schema-only mode and cleared per Article 13 retention sweep). Location: Ireland.
-

Stripe Payments Europe Ltd. — Billing, payments, invoicing, customer-portal sessions. Location: Ireland (with US affiliate).

- SMTP relay (operator-configured) — Transactional email delivery (magic links, billing receipts, dunning notices). Current vendor listed at adaptivmapr.com/legal/security §6. Location: per operator deployment.
- phi-cloud — Full-data mode delegation only (invoked when Customer explicitly opts in and a BAA is in place). AdaptivMapr does not invoke the full-data LLM call itself. Location: EU / CH.
- OpenAI Ireland Ltd. / Anthropic PBC / Mistral AI SAS — LLM cascade layer in schema-only mode; clamp at `clampForSchemaOnly()` re-applied at the LLM call boundary; only header text + ≤ 3 sample values $\times \leq 80$ chars/cell transmitted. Location: Ireland / US / France.

AdaptivMapr will notify Customer at least 30 days before adding or replacing a Subprocessor. Customer may object to the change for reasonable data protection grounds; if the parties cannot resolve the objection in good faith, Customer may terminate the affected portion of the Services without penalty and receive a pro-rata refund of any prepaid fees.

Article 9 — International transfers

Where AdaptivMapr transfers Personal Data outside the EEA, the UK, or Switzerland to a country that has not been recognised as providing an adequate level of protection, the transfer is governed by the SCCs (Modules 2 or 3, as applicable), incorporated into this DPA by reference. For UK transfers the SCCs are read together with the UK ICO International Data Transfer Addendum. For Swiss transfers the SCCs are read together with the FDPIC implementation guidance (reference to FADP, the FDPIC, and the Swiss courts where applicable).

Article 10 — Data subject rights

AdaptivMapr will, taking into account the nature of the Processing, assist Customer through appropriate technical and organisational measures, insofar as possible, in responding to requests from Data Subjects to exercise their rights under Articles 12–22 GDPR. Customer is responsible for primary handling of Data Subject requests, including verifying identity and tracking timelines.

Article 11 — Data breach notification

AdaptivMapr will notify Customer without undue delay, and in any event within 72 hours, after becoming aware of a Personal Data Breach affecting Customer's data. The notification will, to the extent known at the time:

- describe the nature of the breach and the data affected;
- state the likely consequences;
- describe the measures taken or proposed to address it;
- provide a contact point for further information.

AdaptivMapr will cooperate with Customer's reasonable requests for further information and assistance, including for the purposes of Customer's notifications to its own supervisory authority and Data Subjects.

Article 12 — Audits

AdaptivMapr will make available to Customer, on reasonable request, the information necessary to demonstrate compliance with this DPA, including:

- The most recent SOC 2 Type II report (once published) or equivalent independent assurance.
- A summary of penetration test findings (executive summary, not raw findings).
- The current Subprocessor list and the security measures described at adaptivmapr.com/legal/security.

Customer may, no more than once per calendar year and on at least 30 days' written notice, audit AdaptivMapr's compliance with this DPA, at Customer's expense, subject to reasonable confidentiality and access restrictions. The right is satisfied by AdaptivMapr's provision of the documents above unless an audit is required by a supervisory authority or by applicable law.



Article 13 — Return or deletion

Upload-scoped Personal Data is retained for no more than 24 hours after upload. A scheduled sweep runs every 15 minutes and nulls parsed_rows (full-data mode) and clears the cached parsed_sample for any upload whose expires_at has elapsed. A successful /commit also deletes the upload from local storage immediately, ahead of the 24-hour window.

On termination of the Agreement, AdaptivMapr will, at Customer's election, return or delete all Personal Data Processed on Customer's behalf, except where retention is required by law (notably billing records). Schema-only mode mapping fingerprints (header text + chosen target field, no row values) are deleted on workspace deletion or on opt-out.

Article 14 — Liability

Each party's liability arising out of or in connection with this DPA is subject to the limitations set out in the Agreement. Nothing in this DPA limits liability that cannot be limited under applicable law.

Article 15 — Governing law

This DPA is governed by the laws of Switzerland; the courts of Zurich have exclusive jurisdiction, except where the SCCs require a different forum, in which case the SCCs prevail.

Article 16 — Contact

Data protection contact: dpo@adaptivmapr.com. Customers on Pro and Enterprise plans may request a signed counter-party version of this DPA by contacting hello@adaptivmapr.com.

Signature block

Complete the fields below, sign, and return to dpo@adaptivmapr.com. AdaptivMapr will counter-sign and return a fully-executed copy.

CUSTOMER LEGAL NAME

CUSTOMER DATA PROTECTION OFFICER (NAME)

SIGNING AUTHORITY (NAME + TITLE)

PLACE

DATE (YYYY-MM-DD)

CUSTOMER SIGNATURE



AdaptivMapr will counter-sign below on receipt. Do not complete this field.
