HASORIX

Data Processing Agreement

Template for client projects, with the EU Standard Contractual Clauses built in for transfers to India.

Version	Date	Contact	Online
1.0	30 October 2026	hello@hasorix.com	hasorix.com/trust/dpa/

How to use this template

- This agreement applies when HASORIX processes personal data on your behalf while delivering a project, for example when it builds or runs an AI agent that handles your customers' data.
- Complete the highlighted fields in [square brackets], the details of processing in Annex I and, if the project uses any, the sub-processors in Annex III.
- HASORIX works from India, which has no EU adequacy decision. Clause 12 therefore incorporates the European Commission's Standard Contractual Clauses and, for UK data, the UK International Data Transfer Addendum.
- The template is a starting point, not legal advice. Have it reviewed by your own adviser. Changes are welcome: send a marked-up copy to hello@hasorix.com.

Parties

This Data Processing Agreement ("DPA") is made between:

(1) [Customer legal name], a company registered in [country] under number [registration number], whose registered office is at [address] ("**Customer**"); and

(2) HASORIX, [legal form and registration details], Gandhinagar, Gujarat, India ("**HASORIX**"),

each a "party" and together "the parties".

Background

Customer and HASORIX have agreed [name and date of the services agreement or statement of work] (the "**Main Agreement**"). To deliver it, HASORIX may process personal data on Customer's behalf. This DPA sets the terms for that processing, as Article 28 of the GDPR requires.

1 Definitions

1.1 "**Data Protection Law**" means Regulation (EU) 2016/679 (the "**GDPR**"), the UK GDPR and the UK Data Protection Act 2018, the Swiss Federal Act on Data Protection (the "**FADP**"), and any other data protection law that applies to the processing, each as amended or replaced.

1.2 "**Customer Personal Data**" means the personal data that HASORIX processes on Customer's behalf under the Main Agreement, as described in Annex I.

1.3 "**SCCs**" means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

1.4 "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 (version B1.0, in force from 21 March 2022).

1.5 "**Sub-processor**" means another processor that HASORIX engages to process Customer Personal Data.

1.6 "Controller", "processor", "data subject", "personal data", "personal data breach", "processing" and "supervisory authority" have the meanings given in the GDPR.

2 Roles and scope

2.1 Customer is the controller of Customer Personal Data, or, where Customer processes it on behalf of its own client, a processor. HASORIX is Customer's processor or, in the second case, sub-processor.

2.2 Annex I sets out the subject matter and duration of the processing, its nature and purpose, the types of personal data and the categories of data subjects.

2.3 This DPA applies for as long as HASORIX processes Customer Personal Data.

3 Customer's instructions

3.1 HASORIX processes Customer Personal Data only on Customer's documented instructions, including with regard to transfers to a third country, unless the law to which HASORIX is subject requires otherwise. In that case HASORIX informs Customer of that legal requirement before processing, unless that law prohibits this on important grounds of public interest.

3.2 Customer's documented instructions are the Main Agreement, this DPA and any further written instructions Customer gives during the project. Email is enough.

3.3 HASORIX informs Customer immediately if, in its opinion, an instruction infringes Data Protection Law.

3.4 Customer is responsible for the lawfulness of its instructions, for having a lawful basis for the processing and for giving data subjects the information the law requires.

4 Confidentiality

4.1 HASORIX ensures that every person authorised to process Customer Personal Data is bound by an obligation of confidentiality.

4.2 HASORIX is a one-engineer studio. Only the engineer delivering the project has access to Customer Personal Data, unless Customer agrees otherwise in writing.

5 Security

5.1 HASORIX implements the technical and organisational measures in Annex II. They take into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing and the risks to the rights and freedoms of data subjects, as Article 32 of the GDPR requires.

5.2 HASORIX may update Annex II, provided the overall level of security does not decrease.

6 AI models

6.1 HASORIX does not use Customer Personal Data to train, fine-tune or otherwise improve any AI model, except a model built for Customer at Customer's documented instruction.

6.2 Where a project sends Customer Personal Data to a hosted AI model, HASORIX uses only providers listed in Annex III or used through Customer's own accounts, and turns off the provider's data retention and model training where the provider offers that setting.

7 Sub-processors

7.1 Customer gives HASORIX general written authorisation to engage the Sub-processors listed in Annex III.

7.2 HASORIX informs Customer in writing at least [30] days before it adds or replaces a Sub-processor. Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, Customer may end the affected services without penalty.

7.3 HASORIX imposes on each Sub-processor, by written contract, data protection obligations that give at least the protection of this DPA. HASORIX remains fully liable to Customer for each Sub-processor's performance of those obligations.

7.4 Where HASORIX works inside Customer's own accounts, such as Customer's cloud account, AI model provider account or code repository, the providers of those accounts are Customer's own processors under Customer's contracts with them, and not Sub-processors of HASORIX.

8 Data subject requests

8.1 Taking into account the nature of the processing, HASORIX assists Customer by appropriate technical and organisational measures, as far as possible, to respond to requests from data subjects exercising their rights under Chapter III of the GDPR.

8.2 If HASORIX receives such a request directly, it forwards it to Customer without undue delay and does not respond itself unless Customer instructs it to.

9 Personal data breaches

9.1 HASORIX notifies Customer without undue delay, and in any event within [48] hours, after becoming aware of a personal data breach affecting Customer Personal Data.

9.2 The notice describes, as far as then known: the nature of the breach, including the categories and approximate number of data subjects and records concerned; a contact point for more information; the likely consequences; and the measures taken or proposed to address the breach and reduce its possible adverse effects. Where not all of this is known at once, HASORIX provides it in phases without undue further delay.

9.3 HASORIX takes reasonable steps to contain the breach and reduce its effects, and assists Customer in meeting its obligations under Articles 33 and 34 of the GDPR.

10 Further assistance

10.1 Taking into account the nature of the processing and the information available to it, HASORIX assists Customer in meeting its obligations under Articles 32 to 36 of the GDPR, including data protection impact assessments and prior consultation with a supervisory authority.

11 Information and audits

11.1 HASORIX makes available to Customer all information necessary to demonstrate compliance with Article 28 of the GDPR and this DPA.

11.2 HASORIX allows for and contributes to audits, including inspections, by Customer or an auditor Customer mandates. Customer gives at least [30] days' written notice, and audits take place no more than once a year, unless a supervisory authority requires otherwise, a personal data breach has occurred or there are indications of non-compliance.

11.3 An audit starts with a written questionnaire and documents. An inspection follows only if those are not enough. Audits are carried out during business hours, without undue disruption, and under a duty of confidentiality. Each party bears its own costs.

12 International transfers

12.1 HASORIX is established in India, which has no adequacy decision under Article 45 of the GDPR. Transfers of Customer Personal Data to HASORIX are governed by the SCCs, which are incorporated into this DPA by reference and completed as follows:

(a) Module Two (controller to processor) applies where Customer is a controller, and Module Three (processor to processor) where Customer is a processor;

(b) Clause 7 (docking clause) applies;

(c) in Clause 9(a), Option 2 (general written authorisation) applies, with the notice period in clause 7.2 of this DPA;

(d) in Clause 11(a), the optional language does not apply;

(e) in Clause 13(a), the competent supervisory authority is the one identified in Annex I, section C;

(f) in Clause 17, Option 1 applies and the governing law is the law of [Ireland];

(g) in Clause 18(b), disputes are resolved by the courts of [Ireland]; and

(h) Annexes I, II and III of the SCCs are completed by Annexes I, II and III of this DPA.

12.2 For transfers subject to the UK GDPR, the UK Addendum applies and is completed as follows: Table 1 by the parties' details in this DPA and Annex I; Table 2 by the SCC modules and options in clause 12.1; Table 3 by Annexes I, II and III; and in Table 4, neither party may end the UK Addendum under its Section 19.

12.3 For transfers subject to the FADP, the SCCs apply with these changes: references to the GDPR are read as references to the FADP where the transfer is subject to it; the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority for those transfers; and the term "Member State" in Clause 18(c) does not prevent data subjects in Switzerland from bringing claims where they habitually reside.

12.4 HASORIX gives Customer the information it reasonably needs to assess the laws and practices of India for the purposes of Clause 14 of the SCCs.

12.5 HASORIX transfers Customer Personal Data onward to a Sub-processor outside the European Economic Area, the UK or Switzerland only under appropriate safeguards that meet Chapter V of the GDPR.

12.6 If the SCCs or the UK Addendum are replaced, amended or no longer valid, the parties will cooperate in good faith to put in place a valid transfer mechanism.

13 Return and deletion

13.1 When the services end, or earlier at Customer's request, HASORIX returns or deletes all Customer Personal Data, at Customer's choice, and deletes existing copies within [30] days, unless Union or Member State law requires HASORIX to keep it.

13.2 HASORIX's access to Customer's accounts and systems is removed at handover. Copies held in backups are deleted when those backups expire and stay protected under this DPA until then. On request, HASORIX confirms the deletion in writing.

14 Records

14.1 HASORIX keeps a record of the processing it carries out on Customer's behalf, as Article 30(2) of the GDPR requires.

15 Liability and precedence

15.1 Each party's liability under this DPA is subject to the limits in the Main Agreement, except where the SCCs or Data Protection Law do not allow such a limit.

15.2 If there is a conflict on data protection, the SCCs and the UK Addendum take precedence over this DPA, and this DPA takes precedence over the Main Agreement.

16 Term and general

16.1 This DPA takes effect on the date of the last signature below and continues for as long as HASORIX processes Customer Personal Data.

16.2 Apart from the SCCs, which are governed as set out in clause 12, this DPA is governed by the law that governs the Main Agreement, and disputes are resolved as the Main Agreement provides.

16.3 Changes to this DPA must be in writing and signed by both parties. If Data Protection Law changes, the parties will agree the changes needed to keep the processing lawful.

16.4 Notices under this DPA go to the contacts in Annex I. HASORIX's contact for data protection is hello@hasorix.com.

Signed for and on behalf of the parties

Customer

Name _____

Title _____

Date _____

Signature _____

HASORIX

Name _____

Title _____

Date _____

Signature _____

Annex I. Details of processing

A. List of parties

Data exporter	Customer: [legal name], [address]. Contact for data protection: [name, position, email]. Role: [controller or processor]. Activities relevant to the transfer: receiving the services under the Main Agreement.
Data importer	HASORIX, Gandhinagar, Gujarat, India. Contact for data protection: hello@hasorix.com. Role: processor (or sub-processor). Activities relevant to the transfer: software and AI engineering services under the Main Agreement.

B. Description of the processing and transfer

Project and duration	[Short description of the project], from [start date] until the services end.
Categories of data subjects	[For example: Customer's customers or end users; Customer's employees and contractors; people who contact Customer.]
Categories of personal data	[For example: names and contact details; account identifiers; messages, documents and files people submit; case or claim details; usage and audit logs.]
Special categories of data and criminal data	[None. Or describe the data and the extra safeguards that apply, such as stricter access, pseudonymisation or extra logging.]
Frequency of the transfer	[Continuous for the duration of the project, or one-off.]
Nature of the processing	Designing, building, testing, deploying and supporting software and AI systems for Customer, including access to Customer's systems and data as needed for those tasks.
Purpose of the processing	To deliver the services in the Main Agreement: [describe].

Retention	For the duration of the services, then returned or deleted under clause 13.
Transfers to Sub-processors	As listed in Annex III, for the same nature, purpose and duration.

C. Competent supervisory authority

[The supervisory authority of the EU Member State where Customer is established or, where Customer has appointed a representative under Article 27 of the GDPR, of the Member State where the representative is established.]

Annex II. Technical and organisational measures

HASORIX applies the following measures to Customer Personal Data.

Access

- Multi-factor authentication on every account used for the project.
- Least-privilege access, granted per project, and removed at handover.
- Only the engineer delivering the project has access to Customer Personal Data.

Secrets and devices

- Secrets are kept in managed vaults, never in code or chat.
- Work is done on an encrypted laptop with automatic screen lock.

Location and minimisation

- Work takes place inside Customer's own cloud accounts and EU regions where possible.
- Only the personal data a task needs is used. Development and testing use synthetic or anonymised data where possible.
- Where the use case allows, personal data is removed or masked before it reaches an AI model.

AI models

- Customer Personal Data is never used to train models (clause 6).
- Provider data retention and model training are turned off where the provider offers that setting.

Transmission and storage

- Connections to Customer's systems and to providers are encrypted in transit.
- Data at rest is encrypted using the encryption of the hosting platform.

Incidents

- Suspected breaches are contained, assessed and reported to Customer under clause 9, then remediated.

Code and changes

- Code lives in Customer's repositories. Changes are versioned and reviewable by Customer.

Annex III. Sub-processors

Sub-processors HASORIX uses for this project. Providers used inside Customer's own accounts are Customer's processors and are not listed here (clause 7.4).

Provider	Service	Processing	Location	Transfer safeguard
Google	Google Workspace (email and documents)	Project communication, which may include personal data Customer sends by email	USA and other countries	Google's data processing terms (Standard Contractual Clauses)
[Provider]	[Service]	[What it processes]	[Country]	[Safeguard]
[Provider]	[Service]	[What it processes]	[Country]	[Safeguard]