

DATA PROCESSING AGREEMENT

Jurisphere Legal | Template — For Legal Review Before Use

This Data Processing Agreement (this "**DPA**" or "**Agreement**") is entered into as of the date last signed below (the "**Effective Date**") between [LEGAL NAME OF CONTROLLER], a [STATE / JURISDICTION] entity (the "**Controller**"), and [LEGAL NAME OF PROCESSOR], a [STATE / JURISDICTION] entity (the "**Processor**"). This DPA is incorporated into and forms part of the services agreement between the parties (the "**Services Agreement**"). To the extent of any conflict between this DPA and the Services Agreement with respect to the Processing of Personal Data, this DPA shall control.

The parties enter into this DPA to comply with applicable data protection laws, including the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), the UK GDPR, the California Consumer Privacy Act as amended by the California Privacy Rights Act ("**CCPA/CPRA**"), and any other applicable data protection or privacy legislation (collectively, "**Data Protection Laws**").

1. DEFINITIONS

The following terms have the meanings set out below. Terms not defined here shall have the meanings given to them in applicable Data Protection Laws or the Services Agreement.

"Controller"	The entity that determines the purposes and means of Processing Personal Data. For the purposes of this DPA, Controller means the party identified above as the Controller.
"Data Protection Laws"	All applicable laws and regulations relating to the Processing of Personal Data, including the GDPR, UK GDPR, CCPA/CPRA, and any implementing or supplementary legislation, as amended from time to time.
"Data Subject"	An identified or identifiable natural person whose Personal Data is Processed under this DPA.
"Personal Data"	Any information relating to an identified or identifiable natural person, as defined under applicable Data Protection Laws. For the avoidance of doubt, this includes "personal information" as defined under the CCPA/CPRA.
"Personal Data Breach"	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

"Process" / "Processing"	Any operation or set of operations performed on Personal Data, whether by automated means or otherwise, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction.
"Processor"	The entity that Processes Personal Data on behalf of the Controller. For the purposes of this DPA, Processor means the party identified above as the Processor.
"Restricted Transfer"	A transfer of Personal Data to a country or territory outside the EEA or UK that has not been recognized as providing an adequate level of protection under applicable Data Protection Laws.
"Standard Contractual Clauses" / "SCCs"	The standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission, as updated from time to time, including the UK Addendum as applicable.
"Sub-processor"	Any third party engaged by the Processor to Process Personal Data on behalf of the Controller.
"Supervisory Authority"	A public authority responsible for monitoring compliance with Data Protection Laws, including any national data protection authority within the EEA or the UK Information Commissioner's Office.

2. SCOPE AND ROLES

2.1 Subject Matter.

The Processor shall Process Personal Data on behalf of the Controller solely in connection with the provision of services under the Services Agreement (the **"Services"**).

2.2 Nature, Purpose, and Duration.

The nature, purpose, and duration of Processing, the types of Personal Data Processed, and the categories of Data Subjects are set out in Schedule 1 to this DPA. The Processor shall Process Personal Data only for the duration of the Services Agreement, unless a longer retention period is required by applicable law.

2.3 Controller Instructions.

The Processor shall Process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data, unless required to do so by applicable law. The Processor shall promptly notify the Controller if, in its opinion, an instruction infringes applicable Data Protection Laws, unless prohibited from doing so by law.

3. PROCESSOR OBLIGATIONS

3.1 Confidentiality.

The Processor shall ensure that all persons authorized to Process Personal Data are subject to appropriate obligations of confidentiality and have committed to keep Personal Data confidential or are under a statutory obligation of confidentiality.

3.2 Security Measures.

The Processor shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk presented by the Processing, taking into account: (a) the state of the art and cost of implementation; (b) the nature, scope, context, and purposes of Processing; and (c) the likelihood and severity of risks to the rights and freedoms of Data Subjects. Such measures shall include, at minimum:

- Pseudonymization and encryption of Personal Data, where appropriate;
- The ability to ensure ongoing confidentiality, integrity, availability, and resilience of Processing systems and services;
- The ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures.

3.3 Sub-processors.

The Processor shall not engage any Sub-processor without the prior written authorization of the Controller. A list of currently authorized Sub-processors is set out in Schedule 2 to this DPA. The Processor shall notify the Controller of any proposed changes to the Sub-processor list at least thirty (30) days in advance. If the Controller objects to a new Sub-processor on reasonable data protection grounds, the parties shall work in good faith to resolve the objection. Where a Sub-processor is engaged, the Processor shall impose on it data protection obligations substantially equivalent to those set out in this DPA by way of written contract.

3.4 Data Subject Rights.

The Processor shall assist the Controller, by appropriate technical and organizational measures and to the extent reasonably practicable, in fulfilling the Controller's obligations to respond to requests from Data Subjects seeking to exercise their rights under applicable Data Protection Laws, including the rights of access, rectification, erasure, restriction, portability, and objection.

3.5 Data Protection Impact Assessments.

The Processor shall provide reasonable assistance to the Controller in conducting data protection impact assessments and, where required, prior consultations with Supervisory Authorities, to the extent that such assessments or consultations relate to the Processing of Personal Data under this DPA.

3.6 Personal Data Breach Notification.

The Processor shall notify the Controller without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a Personal Data Breach. Such notification shall include, to the extent then known: (a) a description of the nature of the breach, including the categories and approximate number of

Data Subjects and Personal Data records affected; (b) the likely consequences of the breach; and (c) the measures taken or proposed to address the breach. The Processor shall provide further information to the Controller as it becomes available.

3.7 Audit Rights.

The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with the obligations set out in this DPA and shall allow for and contribute to audits, including inspections, conducted by the Controller or a third-party auditor mandated by the Controller, subject to reasonable advance notice of at least thirty (30) days and confidentiality obligations. The Processor may satisfy audit obligations through the provision of up-to-date third-party audit certifications (e.g., ISO 27001, SOC 2 Type II) where agreed by the parties.

3.8 Deletion and Return of Personal Data.

Upon termination or expiration of the Services Agreement, or upon the Controller's written request, the Processor shall, at the Controller's election, delete or return all Personal Data to the Controller and delete all existing copies, unless applicable law requires the Processor to retain such data. The Processor shall certify in writing that deletion has been completed within sixty (60) days of the relevant request or termination date.

4. CONTROLLER OBLIGATIONS

4.1 Compliance with Data Protection Laws.

The Controller represents and warrants that: (a) it has a valid legal basis for Processing Personal Data under applicable Data Protection Laws; (b) it has provided all required notices to, and obtained all necessary consents from, Data Subjects; and (c) its instructions to the Processor comply with applicable Data Protection Laws.

4.2 Accuracy of Data.

The Controller is responsible for the accuracy, quality, and legality of the Personal Data it provides to the Processor, and for the means by which it acquired such Personal Data.

5. INTERNATIONAL DATA TRANSFERS

5.1 Restricted Transfers.

The Processor shall not make any Restricted Transfer of Personal Data without the prior written consent of the Controller, except where required by applicable law. Where a Restricted Transfer is authorized, the parties shall ensure that such transfer is subject to an appropriate transfer mechanism under applicable Data Protection Laws, including Standard Contractual Clauses, adequacy decisions, or binding corporate rules.

5.2 Standard Contractual Clauses.

Where the GDPR or UK GDPR applies and a Restricted Transfer is made, the parties agree to execute the applicable SCCs as a separate annex to this DPA. In the event of any conflict between the SCCs and this DPA, the SCCs shall prevail solely with respect to the Restricted Transfer.

6. CALIFORNIA CONSUMER PRIVACY ACT

To the extent the CCPA/CPRA applies to the Processing of Personal Data under this DPA, the Processor acknowledges and agrees that: (a) it is a “service provider” as defined under the CCPA/CPRA; (b) it shall not sell or share Personal Data, or retain, use, or disclose Personal Data outside of the direct business relationship with the Controller or for any purpose other than the specific purpose of providing the Services; (c) it shall not combine Personal Data received from the Controller with personal information received from or collected on behalf of other businesses, except as permitted under the CCPA/CPRA; and (d) it shall comply with applicable sections of the CCPA/CPRA and shall provide the same level of privacy protection as required thereunder.

7. GENERAL PROVISIONS

7.1 Liability and Indemnification.

Each party’s liability under this DPA is subject to the limitations set out in the Services Agreement. In the event of a breach of this DPA, the breaching party shall indemnify and hold harmless the other party against any fines, penalties, claims, costs, and damages arising from such breach, to the extent caused by the breaching party’s act or omission.

7.2 Duration and Survival.

This DPA shall remain in force for the duration of the Services Agreement. Obligations relating to confidentiality, security, and data deletion shall survive termination or expiration for so long as the Processor retains any Personal Data.

7.3 Governing Law.

This DPA shall be governed by the laws of **[Governing Jurisdiction]**, without regard to conflict of laws principles, subject to any mandatory requirements of applicable Data Protection Laws.

7.4 Order of Precedence.

In the event of any conflict between this DPA and the Services Agreement, this DPA shall govern with respect to the Processing of Personal Data. In the event of any conflict between this DPA and the SCCs, the SCCs shall govern with respect to the Restricted Transfer.

7.5 Amendment.

This DPA may be amended by the Controller on reasonable notice to the Processor where required to comply with applicable Data Protection Laws or guidance from a Supervisory Authority. Any other amendment requires the written agreement of both parties.

IN WITNESS WHEREOF, the parties have caused this Data Processing Agreement to be executed by their duly authorized representatives as of the date last signed below.

CONTROLLER:**[Legal Name of Controller]**

By: _____

Printed Name: _____

Title: _____

Date: _____

Address: _____

Email: _____

PROCESSOR:**[Legal Name of Processor]**

By: _____

Printed Name: _____

Title: _____

Date: _____

Address: _____

Email: _____

SCHEDULE 1 — DETAILS OF PROCESSING

Nature of Processing	[Describe the processing activities, e.g., hosting, storage, analytics, support]
Purpose of Processing	[Describe the purpose, e.g., provision of SaaS platform services]
Duration of Processing	[State the duration, or refer to the term of the Services Agreement]
Types of Personal Data	[List categories, e.g., name, email, IP address, usage data, payment data]
Categories of Data Subjects	[Describe, e.g., Controller's end users, employees, customers]

SCHEDULE 2 — AUTHORIZED SUB-PROCESSORS

Sub-processor Name	Processing Activity	Location
[ADD]	[ADD]	[ADD]