Upsun Data Processing Agreement

1. Introduction

This Data Processing Agreement, including its Exhibits (this "**DPA**"), supplements and forms an integral part of the Upsun Terms of Services (https://upsun.com/trust-center/legal/tos/) or any other written contract in place (the '**Agreement**') between You (the '**Customer**' as defined in that Agreement) and Upsun ("**Upsun**") in connection with Services with respect to the processing of Customer Personal Data in accordance with the requirements of the Data Protection Laws. This DPA shall be effective on the effective date of the Agreement.

2. Definitions

For the purposes of this DPA**:**

"**Data Protection Laws**" means all laws, regulations, and other legal requirements in any jurisdiction that are directly applicable to Upsun's processing of Customer Personal Data under the Agreement, which may include without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. ("**CCPA**") and its implementing regulations and applicable amendments, the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"), equivalent requirements in the United Kingdom including the UK Data Protection Regulation and the Data Protection Act 2018 ("**UK Data Protection Law**"), and the Swiss Federal Act on Data Protection ("**FADP**").

"**Customer Personal Data**" means any Customer data that is Personal Data and is processed by Upsun in connection with providing the Services pursuant to the Agreement. Customer Personal Data does not include Personal Data that relates to Customer's relationship with Upsun, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information, ("**Operational Data**") or Service usage data collected by Upsun in connection with the provision of the Services, including without limitation data used to provide customer support and troubleshoot technical issues, activity logs, data used to optimize, improve and maintain performance of the Services, and to investigate and prevent system abuse ("**Service Usage Data**") as described in the Upsun Privacy Notice located at https://upsun.com/trust-center/privacy/privacy-notice/ .

Personal Data' includes "personal data," "personal information," "personally identifiable information," and similar terms, and such terms shall have the same meaning as defined by Data Protection Laws

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data transmitted, stored, or otherwise processed.

"**Services**" means, collectively, the Upsun Cloud platform-as-a-service offering, the Dispatch service, and any other product or service made available by Upsun to Customer under the Agreement.

"**Subprocessor**" means an Upsun subsidiary and/or any third party entity engaged by Upsun to Process Customer Personal Data for the provision of Services.

"Standard Contractual Clauses" or **"SCCs**" means i) the standard contractual clauses annexed to the EU Commission decision EU 2021/914 of 4 June 2021 as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (and as updated from time to time).

"Data Controller" (or ''**Controller**''), **"Data Processor"** (or ''**Processor**''), **"Data Subject"**, all have the meanings given to those terms in Data Protection Laws or their equivalent terms (and related terms such as **"process"** and **"processed"** shall have corresponding meanings);

Capitalized terms not defined herein shall have the meaning ascribed to them in the Agreement.

3. Processing Instructions

3.1 Customer shall ensure that the use of the Services and its instructions comply with Data Protection Laws applicable to the processing of Personal Data, and that will not cause Upsun to be in breach of the Data Protection Laws.

3.2 Customer acknowledges that Upsun is not responsible for determining which laws or regulations are applicable to Customer's business, nor whether Upsun's provision of the Services meets or will meet the requirements of such laws or regulations. Customer is solely responsible for the accuracy, quality, and legality of the Customer Personal Data provided to Upsun by or on behalf of Customer and the means by which Customer acquired any such Customer Personal Data.

3.3 Upsun shall process Customer Personal Data (i) for the purposes set forth in the Agreement, (ii) in accordance with the terms and conditions set forth in this DPA and any other documented instructions provided by Customer from time to time, and (iii) in compliance with the Data Protection Laws.

3.4 The parties acknowledge and agree that with regard to the processing of Customer Personal Data, Customer may act as either a Data Controller or a Data Processor and Upsun is a Data Processor. If Customer is a Data Processor, Customer represents and warrants that its instructions and actions with respect to the Customer Personal Data, including appointing Upsun as a Data Processor, have been and are authorized by the relevant Data Controller.

3.5 Upsun shall not sell or share (as those terms are defined under the CCPA) any such Customer Personal Data nor retain, use or disclose any Customer Personal Data provided by Customer pursuant to the Agreement except as necessary for performing the Services or otherwise as set forth in the Agreement or as permitted by the applicable Data Protection Laws.

3.6 The subject matter, nature, purpose and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this DPA.

3.7 Following completion of the Services, Upsun shall delete Customer Personal Data, and shall, upon Customer's written request, provide Customer with written confirmation of deletion, except as required to be retained by applicable law. The provisions of this DPA survive the termination or expiration of the Agreement for so long as Upsun processes Customer Personal Data.

4. Personnel and Subprocessors

4.1 Upsun shall ensure the reliability of its employees who access Customer Personal Data, and have signed agreements requiring them to keep Customer Personal Data confidential.

4.2 Upsun may use Subprocessors to fulfil its contractual obligations to Customer under the Agreement. Customer generally authorizes and consents to Upsun use of Subprocessors for such purposes. A current list of Upsun's Subprocessors is available in https://upsun.com/trust-center/privacy/subprocessor-list/ and can be updated by Upsun from time to time.

4.3 Upsun shall notify Customer if it adds any new Subprocessors at least fifteen (15) days prior to allowing such Subprocessor to process Customer Personal Data. Customer may object in writing to Upsun's appointment of a new Subprocessor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. If Customer objects, the parties shall discuss in good faith a reasonable resolution, and Upsun shall use commercially reasonable efforts to provide the affected Services without the use of the objected-to Subprocessor. If the parties are unable to reach a resolution within ten (10) days of Customer's objection, and Upsun is unable to provide the affected Services without the use of the objected-to Subprocessor, Upsun may proceed to use the new Subprocessor, in which case Customer's sole and exclusive remedy shall be to terminate, without penalty, the portion of the Services that cannot be provided by Upsun without the use of the objected-to Subprocessor, by providing written notice to Upsun.

4.4 Upsun shall enter into a written agreement that imposes obligations no less protective than those imposed on Upsun under this DPA on the Subprocessors.

4.5 Upsun shall be liable to Customer for the acts and omissions of its Subprocessors to the same extent that Upsun would itself be liable under the Agreement had it conducted such acts or omissions.

5. **Assistance and Audits**

5.1 Upsun shall, taking into account the nature of the processing and the information available to it and provided that Customer does not otherwise have access to the relevant information, provide Customer with reasonable cooperation and assistance, where necessary for Customer to:

i. comply with its obligations under the Data Protection Laws, including responding to Data Subject requests;

ii. conduct a data protection impact assessment;

iii. cooperate with and/or participate in prior consultation with any supervisory authority, where necessary and legally required.

Where a request for assistance under this Section 5.1 requires materially disproportionate time or resources, meaning time or resources substantially exceeding what is reasonably required for comparable requests of that type, Upsun may charge Customer for its reasonable, documented costs (including personnel time calculated at a reasonable hourly rate) directly incurred in providing such assistance, provided that Upsun first notifies Customer of the estimated cost and obtains Customer's written approval before proceeding .

5.2 Upsun, upon request shall (i) supply a summary copy of its audit report(s) to Customer, so Customer can verify Upsun's compliance with the audit standards against which it has been assessed, and to the extent applicable this DPA, and (ii) if the summary audit report(s) provided under (i) do not provide sufficient information for Customer to reasonably verify Upsun's compliance with its obligations under this DPA**,** allow Customer or its authorized representative to conduct an audit of Upsun's data processing practices to demonstrate such compliance, provided that such audit shall be communicated to Upsun 30 days in advance, shall not be unreasonably disruptive to Upsun's business, and shall occur no more than once per twelve (12) month period during the term of the Agreement, unless otherwise required by a supervisory authority or in connection with a Personal Data Breach. The Customer shall be responsible for the costs of any such audit.

6. Transfers of Personal Data

6.1 Customer acknowledges that Upsun or its Subprocessor may need to process Customer Personal Data outside the European Economic Area, the United Kingdom or Switzerland to a country that may not have the same level of protection as the applicable Data Protection Laws.

6.2 Upsun shall ensure international transfers of Customer Personal Data are conducted in compliance with all Data Protection Laws. Where Upsun engages in an onward transfer of Customer Personal Data, Upsun shall ensure that a lawful data transfer mechanism (e.g., an adequacy decision, including the EU-U.S. Data Privacy Framework, irs UK Extention and the Swiss-U.S. Data Privacy Framework, or Standard Contractual Clauses) is in place prior to transferring Customer Personal Data from one country to another.

6.3 With respect to Customer Personal Data transferred from the European Economic Area for which the GDPR governs the international nature of the transfer, to the extent legally required, Customer and Upsun are deemed to have signed the SCCs, which form part of this DPA and will be deemed completed as follows:

- Module 2 of the SCCs applies to transfers of Customer Personal Data from Customer (as a Data Controller) to Upsun (as a Data Processor) and Module 3 of the SCCs applies

to transfers of Customer Personal Data from Customer (as a Data Processor) to Upsun (as a Data Processor);

- Clause 7 of Modules 2 and 3 (the optional docking clause) shall not apply;
- Under Clause 9 of Modules 2 and 3 (Use of sub-processors), the parties select Option 2 (*General written authorization*). The initial list of sub-processors is set forth in Exhibit B of this DPA;
- Under Clause 11 of Modules 2 and 3 (*Redress*), the optional language requiring that data subjects be permitted to lodge a complaint with an independent dispute resolution body shall not be deemed to be included;
- Under Clause 17 of Modules 2 and 3 (Governing law), the parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the law of France;
- Under Clause 18 of Modules 2 and 3 (*Choice of forum and jurisdiction*), the parties select the courts of Paris, France;
- Annex I(A) and I(B) of Modules 2 and 3 (*List of Parties*) is completed as set forth in Exhibit A of this DPA;
- Under Annex I(C) of Modules 2 and 3 (Competent supervisory authority), the parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the French National Commission on Informatics and Liberty.
- Annex II of Modules 2 and 3 (Technical and organizational measures) is completed with Exhibit C of this DPA; and
- Annex III of Modules 2 and 3 (List of subprocessors) is intentionally not included as the parties have chosen general authorization under Clause 9.

6.4 With respect to Customer Personal Data transferred from the United Kingdom for which UK Data Protection Law governs the international nature of the transfer, to the extent legally required, the SCCs as implemented pursuant to Section 6.3 above shall apply, as supplemented by the UK Information Commissioner's Office's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "**UK Addendum**"), which is hereby incorporated into and forms part of this DPA. In case of any conflict or ambiguity between the UK Addendum and the SCCs, the UK Addendum shall prevail with respect to such transfers. For purposes of the UK Addendum, Table 1 is completed with the details of the parties set out in Exhibit A, Table 2 is completed by reference to the SCC options set out in Section 6.3, Table 3 is completed with the subprocessor and technical and organizational measures information set out in Exhibits B and C, and Table 4 (Ending the Addendum when the Approved Addendum changes) is completed by selecting that either party may end the UK Addendum as set out in Section 19 of that Addendum.

6.5 With respect to Customer Personal Data for which the FADP governs the international nature of the transfer, where such Customer Personal Data is transferred (directly or by onward transfer) to a country not listed in Annex 1 of the Swiss Data Protection Ordinance as providing an adequate level of protection, such transfer shall, to the extent legally required, be made (a) to a recipient certified under the Swiss-U.S. Data Privacy Framework, in reliance on that

certification, or, failing that, (b) under the SCCs as implemented pursuant to Section 6.3 above, which shall apply with the following adaptations:

(i) the Swiss Federal Data Protection and Information Commissioner ("FDPIC") shall be the competent supervisory authority under Clause 13 and Annex I(C) insofar as the transfer is governed by the FADP; where the transfer is governed by both the FADP and the GDPR, the FDPIC and the supervisory authority identified under Section 6.3 shall act in parallel, each for the law it supervises;

(ii) references to the GDPR shall be understood as references to the FADP insofar as the transfer is governed by the FADP;

(iii) the governing law and choice of forum selected in Section 6.3 shall apply.

Upsun shall ensure that each Subprocessor receiving Customer Personal Data subject to the FADP is bound by one of the mechanisms in this Section 6.5.

6.6 If Upsun receives a legally binding request from a government, law enforcement, or other public authority seeking disclosure of Customer Personal Data, Upsun shall (a) notify Customer promptly, and in any event prior to any disclosure, unless legally prohibited from doing so, in which case Upsun shall use commercially reasonable efforts to obtain a waiver of such prohibition and, where a waiver cannot be obtained, notify Customer as soon as the prohibition ceases to apply, and/or (b) where legally permitted, seek to redirect the requesting authority to seek the Customer Personal Data directly from Customer, and shall reasonably cooperate with Customer in responding to such request;

7. Security

7.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Upsun shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data, including at a minimum those outlined in Exhibit C.

8. **Security Breach Notification**.

8.1 Upsun shall notify Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach by Upsun or its Subprocessors of which Upsun becomes aware, providing Customer with sufficient information (insofar as such information is within Upsun's possession). Upsun shall make commercially reasonable efforts to assist in the investigation, mitigation and remediation of Personal Data Breach that is known to Upsun.

9. **Liability**

9.1 Each party's liability arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the limitations and exclusions of liability set forth in the Agreement. Any reference in the Agreement to the liability of a party arising under, or in connection with, the Agreement shall include liability arising under, or in connection with, this DPA.

10. Order of Precedence

10.1 This DPA relates to the Agreement. The general conditions declared applicable in the Agreement are equally applicable to this DPA. However, if the Agreement is in direct conflict with this DPA in regard to Customer Personal Data, the provisions of this DPA shall prevail. In the event of any conflict or inconsistency between the terms of this DPA and the Standard Contractual Clauses incorporated under Section 6.3 (and, where applicable, the UK Addendum incorporated under Section 6.4 or the adaptations under Section 6.5), the Standard Contractual Clauses (or the UK Addendum or such adapations, as applicable) shall prevail to the extent of such conflict or inconsistency. The provisions of this DPA apply to the processing of Customer Personal Data by Upsun in relation to the Agreement.

Exhibit A
Details of Processing

List of Parties:

Data Exporter: Customer, as identified in the Agreement.

Activities relevant to the data transferred: use of the Services as described in the Agreement.

Role: Controller or Processor, as applicable (see Section 3.4 of this DPA).

Signature and date: deemed executed as of the effective date of the Agreement, in accordance with Section 6.3 of this DPA.

Data Importer: Upsun entity as identified in the Agreement., acting as Processor.

Activities relevant to the data transferred: provision of the Upsun Cloud platform-as-a-service, Dispatch, and related Services, as described in the Agreement.

Role: Processor.

Signature and date: deemed executed as of the effective date of the Agreement, in accordance with Section 6.3 of this DPA.

Nature and Purpose of Processing: The overall purpose of Upsun's processing of Customer Personal Data is to provide the Services described in the Agreement to Customer. Processing

operations necessary to achieve the stated purposes may include data entry, hosting, storage, structuring, transmission, and deletion.

Duration of Processing: For the duration of the Agreement.

Categories of Data Subjects: The Data Subjects may include Customer's employees, customers and end-users, or any other individual whose Personal Data Customer uploads to or make available to Upsun through the Services.

Type of Personal Data: Upsun provides the project environment and stores the Customer Content within as part of its service offering. The categories of Personal Data processed by Upsun are determined solely by the Customer and are dependent on the data that the Customer uploads, transmits, or otherwise makes available on or through the Services. Upsun does not determine the nature, scope, or purpose of the data uploaded by the Customer and disclaims any responsibility for ensuring that such data falls within the categories described herein. This Exhibit A applies regardless of whether Customer accesses the Services through Upsun Cloud, Dispatch, or any other Upsun product.

***Frequency of the transfer*:** Continuous, for the duration of the Agreement.

Exhibit B

List of approved Subprocessors:

- A list of current and approved Subprocessors can be found at https://upsun.com/trust-center/privacy/subprocessor-list/ .

Exhibit C

Technical and Organizational Measures

Explanatory Note: Below is a list of technical and organizational measures applicable to our day to day operations and focusing on employees access to our systems , for a comprehensive list of all security measures implemented in the provision of our services, please read our security assurance plan (https://upsun.com/static/a9d9034d6dd5fde960a8b199784b80e7/upsun_security_assurance_plan_2026_9e7f9236d6.pdf).

Workforce Security Management

- Permanent employees, temporary employees, and sub-contractors of Upsun have signed confidentiality and non-disclosure agreements (or are individually bound by equivalent confidentiality obligations) upon employment or appointment.
- Security policies and individuals' responsibilities for good information security are communicated to all relevant personnel and agents upon start of employment and at other appropriate times (for example once a year).

- Personnel is informed of information security risks associated with travel and working from remote locations.

Workstation & Device Protection

- Personnel is not authorised to use non-company computers (i.e. computers not owned/leased and operated by Upsun), unless technical security policies implemented by Upsun protect the processing of Upsun and customer data on non-company computers.
- All laptop and desktop computers have security policies enforced, which ensure encryption, AV protection, OS updates, as well as the possibility of remotely disconnecting a device from the network, locking the device or performing a full data wipe, to ensure data integrity and combat leaking information in case of a security incident.
- Passwords granting access to computers, applications and accounts are not hard coded into any computer or file or transmitted in clear text.
- Upsun reduces password usage by enforcing Single Sign-On (SSO) wherever possible. When passwords are necessary, personnel are advised to use a password manager to generate and store strong, unique passwords.
- Hard disks in laptop and desktop computers are subject to a multiple overwrite process before disposal. Other media potentially containing data are disabled/destroyed or otherwise sufficiently formatted or overwritten to prevent unauthorised data access.
- Where a specific laptop or desktop computer is issued to personnel, data on this computer's hard drive is erased before this computer is issued to any subsequent user.
- Personnel are instructed to immediately report thefts and other losses of devices/media containing company information (including laptops). Any loss/theft of such devices/media is followed with the necessary actions to prevent unauthorised network access (e.g., by removal from the directory service) and unauthorised disclosure of information (e.g., by executing 'remote kill' commands).
- All company-managed devices run endpoint protection software with real-time threat detection and response capabilities.

Network and System Access Management

- Access to the web application is managed through Okta, our enterprise-grade identity and access management platform. All user authentication flows are directed through Okta’s secure infrastructure, ensuring that credentials are never handled directly by the application.
- This integration leverages Single Sign-On (SSO) based on industry-standard protocols, including SAML 2.0, OAuth 2.0, and OpenID Connect, to provide a seamless and secure authentication experience.
- Documented procedures and access policies are established and communicated to request, approve, administer, and review user IDs (also known as "system accounts" or "accounts") and passwords for network and applications access.

- Access requests for application/data access are approved at least by the requestor's supervisor or the application/data owner. Approved access is assigned individually to a person in accordance with that person's approved job/position responsibilities and considerations regarding segregation of duties.
- Passwords are automatically set to expire after a limited period and contain a minimum of 12 characters that are not easily guessed. Accounts granting access to networks and applications are automatically locked out after a predefined number of unsuccessful logon attempts, and such lockouts are investigated before reactivating accounts and/or resetting passwords. Additionally this requires ‘in-person’ verification with security personnel to confirm identity, before access is restored. Network and application settings are maintained to keep concurrent logon connections to a minimum. Security settings are enabled so as to prevent re-use of the last 24 passwords.
- Default user IDs and passwords are disabled or changed from their initial values to prevent abuse of default system administrator accounts and features. Workstation administrative passwords are changed at least once per year.
- Accounts granting access to the network and to applications are regularly reviewed to detect and disable/remove inactive user IDs. User IDs of terminated personnel are disabled on the day of termination. User master files for network and application access are reconciled to lists of departing/departed personnel periodically to ensure unrequired system access has been removed promptly.
- System access rights (of collaboration / document management systems as well as file servers storing information) are reviewed at least once per year in liaison with application/data owners to validate that all users' system access permissions are commensurate with approved position responsibilities

Backup and Disaster Recovery Operations

- Contingency and disaster recovery plans covering critical applications/document repositories are documented, updated, and tested/evaluated on an annual basis.
- Up-to-date anti-virus software is installed on all workstations connecting to Upsun’s network. The anti-virus software is configured to identify and remove, disable, or quarantine computer viruses automatically, and receives automatic updates to ensure this capability is maintained on an ongoing basis.

Change Management

- Formal change management procedures are documented, communicated and adhered to for the development and maintenance of custom-built computer applications, to ensure sufficient review and approval of software code and system configuration changes and to segregate the ability to modify computer programs and move these into production. Critical applications have separate environments (and appropriately configured access rights) for development/training/testing/QA and production.

Other Security Controls

- System administrator and “super-user” privileges to computers and application/system management software are limited to a small number of qualified and authorised personnel, in accordance with their approved job responsibilities.
- Log files recording critical security and system administrator activities (including creation of new users, password resets, changes of access rights, clearance of audit logs) are maintained and independently reviewed on a regular basis.
- Remote network access capabilities are provided in a controlled and secure manner to ensure that remote network access only occurs for approved business purposes and by authorised personnel only.
- Employees are informed that highly confidential data transmissions must be subject to additional data protection measures as Upsun makes available, (e.g., encryption of emails).