1. Introduction

This Data Processing Agreement, including its Exhibits (this **“DPA**”), supplements the Upsun Terms of Services or any other written contract in place (the ‘**Agreement**’) between You (the ‘**Customer**’) and Upsun (“**Upsun”**) in connection with the Services to reflect the parties’ agreement with regard to the Processing of Personal Data.

2. Definitions

“**Data Protection Laws**” means laws and regulations relating to privacy and/or data protection, applicable to the processing of personal data under the Agreement, including without limitation, to the extent applicable, the General Data Protection Regulation (EU) 2016/679 (**"GDPR"**), the UK General Data Protection Regulation (“**UK GDPR**”), the Swiss Federal Data Protection Act and its implementing regulations (“**Swiss FADP**”) the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (“**CCPA**”), the California Privacy Rights and Enforcement Act of 2020, and/or any applicable analogous legislation in any jurisdiction.

“**Personal Data Breach**” means 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.

“**Subprocessor**” means an Upsun affiliate and/or any other third party engaged by Upsun to Process Personal Data.

“Standard Contractual Clauses” 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 (as updated from time to time).

“Data Controller” (or Controller), **“Data Processor”** (or Processor) **“Data Subject”**, **“Personal Data”**, **“Processing”**, all have the meanings given to those terms in Data Protection Laws (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 will not cause Upsun to be in breach of Data Protection Laws.

3.2 Customer is solely responsible for the accuracy, quality, and legality of (i) Personal Data provided to Upsun by or on behalf of Customer, (ii) the means by which Customer acquired the Personal Data, and (iii) the instructions it provides to Upsun.

3.3 Upsun shall Process 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 Data Protection Laws.

3.4 The parties acknowledge and agree that Upsun is a Processor of Personal Data under Data Protection Laws (or a subprocessor as may be applicable) and the Customer is a Controller or a Processor. If Customer is a Processor, Customer represents and warrants that its instructions and actions with respect to the Personal Data, including appointing Upsun as a subprocessor, have been and are authorized by the relevant Controller. Upsun shall not sell, retain, use or disclose any 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 applicable Data Protection Laws.

3.5 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.

3.6 Following completion of the Services, Upsun shall delete the Personal Data, 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 Personal Data.

4. Upsun Personnel and Subprocessors

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

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

4.3 Upsun shall notify Customer if it adds any new Subprocessor (notification may be via email, by notification on an online portal of our Services, or by other reasonable means) at least fifteen (15) days prior to allowing such Subprocessor to Process 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 substantial rational grounds relating to data protection or documented evidence of non-compliance with applicable Data Protection Laws . If the parties are unable to reach a mutually agreeable resolution to Customer objection to a new Subprocessor, as sole and exclusive remedy, Customer may terminate the specific Service or

portion of Service that cannot be provided without the objected-to Subprocessor., and Upsun will refund any prepaid, unused fees for the terminated portion of the applicable subscription term for the affected Service.

4.4 Upsun shall enter into a written agreement that imposes similar obligations on its Subprocessors as are imposed on Upsun under this DPA.

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 this DPA 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 Data Protection Laws, including responding to Data Subject requests; If Upsun receives a request from a Data Subject in relation to the Data Subject's Personal Data processed under this DPA, Upsun will notify Customer and will advise the Data Subject to submit the request to Customer;

ii. conduct a data protection impact assessment;

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

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, to the extent applicable this DPA and (ii) allow Customer or its authorized representative to conduct an audit of Upsun data processing practices to demonstrate compliance with its obligations under this DPA, 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 or Personal Data

6.1 Customer authorizes Upsun or its Subprocessor to Process Personal Data outside the European Economic Area to the extent required for the provision of Services in a country that may not have the same level of protection as the applicable Data Protection Laws.

6.2 Upsun shall take all steps necessary to comply with relevant Data Protection Laws regarding transfers of Personal Data to third countries including entering into Standard Contractual Clauses (or other approved transfer mechanism) with the importing entity.

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 B.

8. Security Breach Notification.

8.1 Upsun shall notify Customer without undue delay after becoming aware of a Personal Data Breach by Upsun or its Subprocessors, 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 such a Personal Data Breach. Customer acknowledges that Upsun providing notification of a Personal Data Breach is not an acknowledgment of fault or liability.

9. **Order of Precedence**
9.1 This DPA supplements 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, the provisions of this DPA shall prevail. The provisions of this DPA apply to any Processing of Personal Data by Upsun in relation to the Agreement.

Exhibit A

Details of Processing

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

Type of Personal Data: Upsun provides the project environment and stores the Customer Content (as defined in the Agreement) 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.

Exhibit B

Technical and Organizational Measures

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 practices are communicated to all relevant personnel and agents upon the start of employment and at other appropriate times (for example once a year).
- Personnel are informed of information security risks associated with travel and working from remote locations.

Workstation & Device Protection

- Personnel are 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 Personal 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 Active Directory) 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 e-mail).