Workshop

WORKSHOP SOFTWARE, INC.

DATA PROCESSING ADDENDUM

Last Updated: February 10, 2026

This Data Processing Addendum ("**DPA**") supplements and forms part of the Agreement between the customer entering into an Order Form or other agreement that references this DPA ("**Customer**") and Workshop Software, Inc. ("**Company**") and applies to the extent the Company processes Personal Data on behalf of the Customer in connection with the Services. This DPA governs the parties' respective obligations with respect to such processing under applicable Data Protection Laws.

This DPA is incorporated by reference into the Agreement and is effective as of the effective date of the applicable Order Form or other agreement referencing the Agreement (the "**Effective Date**"). Customer enters into this DPA on its own behalf and, where required under applicable Data Protection Laws, on behalf of its Affiliates. Capitalized terms used but not defined in this DPA have the meanings given in the Agreement.

1. Definitions

1.1. "**Affiliate**" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2. "**Controller**" means the person or entity who determines the purposes and means of the Processing of Personal Information and includes the term "Business" as similarly defined under applicable Data Protection Laws.

1.3. **"Sub-Processor**" or "**Subprocessor**" means a third-party that processes Customer's Personal Data on Company's behalf to enable Company to perform its obligations under this Addendum or the Agreement, and who is either (1) listed in Exhibit B or (2) subsequently authorized under Section 4.2 of this Addendum.

1.4. "**Customer Personal Data**" means personal data that relates to Customer's relationship with Company, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Customer Account Data also includes data Company processes to manage its contractual relationship with Customer, including account administration, billing, identity verification, and compliance with applicable laws and regulations.

1.5. "**Customer Usage Data**" means Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse. Customer Usage Data does not include the content of communications and is processed in aggregated or de-identified form where reasonably practicable.

1.6. "**Personal Information**" or "**Personal Data**" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Data Subject or household, or is otherwise regulated by applicable Data Protection Laws. Personal Information or Personal Data does not include data that has been de-identified or aggregated such that it can no longer identify a Data Subject.

1.7. "**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.8. "**Processor**" means the entity that processes Personal Data on behalf of the Customer and includes the term "Service Provider" as similarly defined under applicable Data Protection Laws.

1.9. "**Data Exporter**" means Customer.

1.10. "**Data Importer**" means Company.

1.11. "**Data Protection Laws**" means any applicable current and future laws, rules, regulations and guidance governing the privacy, security and protection of Personal Information processed under the Agreement, including but not limited to: (i) the US Data Protection Laws; (ii) the European Data Protection Laws; (iii) the Canadian Data Protection Laws; (iv) Australian Data Protection Laws; and (v) South African Data Protection Laws

1.12. **"European Data Protection Laws"** means all applicable legislation applicable to data protection and privacy regarding residents of the EU, UK or Switzerland, including but not limited to: (i) the EU General Data Protection Regulation ((EU) 2016/679) (the "EU GDPR")); (ii) Directive 2002/58/EC the Privacy and Electronic Communications Regulations 2003 as amended (iii) the EU GDPR as applicable as part of UK domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (as amended) ("UK GDPR"); (d) the Swiss Federal Act on Data Protection of 1 September 2023 and its corresponding ordinances (the "FADP"); and any applicable guidance or codes of practice issued by any applicable Supervisory Authorities from time to time.

1.13. **"Canadian Data Protection Laws**" means those Canadian federal and provincial laws, rules, regulations and guidance related to the privacy, security and protection of Personal Information processed under the Agreement, including but not limited to: (a) the Personal Information Protection and Electronic Documents Act ("PIPEDA") and/or (b) the applicable provincial privacy laws including: (i) an Act Respecting the Protection of Personal Information in the Private Sector, ("ARPPIPS") as amended by Quebec's Bill

64; (ii) Alberta's Personal Information Protection Act (iii) the Personal Information Protection Act of British Columbia and (iv) the Canadian Anti-Spam Legislation.

1.14. **"South African Data Protection Laws"** means all applicable legislation relating to data protection and privacy regarding residents of South Africa, including but not limited to the Protection of Personal Information Act, 2013 ("POPIA") and all associated regulations and any guidelines, directives, codes of conduct, or guidance notes issued by the Information Regulator (South Africa) or any other relevant regulatory authority from time to time.

1.15. "**Australian Data Protection Laws**" means all applicable legislation relating to data protection and privacy regarding residents of Australia, including but not limited to: the federal *Privacy Act 1988 (Cth)* and any applicable state or territory privacy or health records legislation; and any guidelines, directives, or codes of practice issued by the Office of the Australian Information Commissioner (OAIC) or any other relevant regulatory authority from time to time.

1.16. "**EU SCCs**" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).

1.17. "**ex-EEA Transfer**" means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the "EEA"), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.18. "**ex-UK Transfer**" means the transfer of Personal Data, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its premises) outside the United Kingdom (the "UK"), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.19. "**Services**" shall have the meaning set forth in the Agreement.

1.20. "**Standard Contractual Clauses**" means the EU SCCs.

1.21. "**UK Addendum**" means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner's Office, as amended or updated from time to time.

2. Processing of Personal Data

2.1. The parties acknowledge and agree that with regard to the processing of Personal Data, Customer is a controller of Personal Data processed in connection with the Services, and Company acts as a processor on Customer's behalf, except with respect to Customer Account Data and Customer Usage Data as defined in the Master Services Agreement, for which Company acts as an independent controller. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer's instructions will not cause Company to be in breach of the Data Protection Laws. Customer is responsible

for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data;(iii) the instructions it provides to Company regarding the processing of such Personal Data; and (iv) to determine the legal basis processing. Customer shall not provide or make available to Company any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services.

2.2. Company shall not process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with the terms and conditions set forth in this Addendum or any other documented instructions provided by Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by applicable law or a Supervisory Authority to which the Company is subject; in such a case, the Company shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, or (iii) in violation of Data Protection Laws. Customer hereby instructs Company to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Services.

2.3. 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 Addendum.

2.4. Company shall promptly notify Customer if, in Company's reasonable opinion, any instruction from Customer infringes applicable Data Protection Laws.

2.5. Upon Customer's reasonable request, Company shall provide written certification, in a form satisfactory to Customer, confirming its full compliance with this Section and with the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, the "**CCPA**"). Specifically:

(a) Company shall not sell any personal information.
(b) Company shall not share personal information, as that term is defined under the CCPA.
(c) Company shall not retain, use, or disclose any personal information provided by Customer except as necessary to perform the Services under the Agreement, as otherwise permitted by the Agreement, or as allowed under the CCPA.
(d) Company certifies that it understands and will comply with the restrictions set forth in this Section 2.5.

The terms "personal information," "service provider," "sale," and "sell" have the meanings assigned to them in Section 1798.140 of the CCPA.

3. Compliance with Data Protection Laws

The Company may only retain, use, and/or disclose Personal Information processed under this Agreement solely to fulfill the specific Business Purpose subject to this Agreement.

a. Restrictions on Use. The Company shall not:

(a) retain, use, and/or disclose Personal Information for any purpose other than fulfilling the specific Business Purposes specified in the Master Agreement and the DPA
(b) retain use, using, or disclosing the Personal Information for a Commercial Purpose other than the Business Purposes specified in the contract;
(c) "sell or share" Personal Information as defined under the Data Protection Laws,
(d) share Personal Information with any third party for targeted advertising;
(e) combine Personal Information it receives pursuant to this Master Agreement with Personal Information that it receives or collects on behalf of, another person or persons, or collects from its own interaction with the Consumer, except as permitted under applicable Data Protection Laws; or
(f) retain, use, or disclose Personal Information Processed by the Company under this Agreement outside of the direct business relationship between the parties;

b. Notification. The Company shall promptly notify the Customer after making a determination that it can no longer meet its obligations under the Data Protection Laws.
c. Certification. The Company certifies to the Customer that it understands the requirements and restrictions in the Data Protection Laws and will comply with them.

4. Workshop Personnel

4.1. Company shall take reasonable steps to ensure the reliability of any Company Personnel who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as necessary for the performance of the Services, their regular job duties, or to comply with any applicable Data Protection Laws in the context of that individual's duties to Company.

4.2. Company shall ensure that any person it authorizes to process Personal Data is subject to appropriate confidentiality obligations. Company may disclose Personal Data to its advisers, auditors, and other third parties solely to the extent reasonably necessary to perform its obligations under this Addendum or the Agreement, provided that such parties are bound by confidentiality obligations at least as protective as those set forth herein.

5. Subprocessing

5.1. Customer acknowledges and agrees that Company may (i) engage its Affiliates and the Authorized Sub-Processors on the List (defined below) to process Personal Data in connection with the Services and (ii) from time to time engage additional third parties as necessary to provide the Services. By way of this Addendum, Customer provides general written authorization to Company to engage sub-processors to perform the Services.

5.2. A list of Company's current Authorized Sub-Processors (the "**List**") is available at https://docs.useworkshop.com/article/26-subprocessors and may be updated by Company from time to time. Company will provide a mechanism to receive notifications of new Authorized Sub-Processors, which Customer may subscribe to where available. At least ten (10) days before authorizing a new sub-processor to process Personal Data, Company will add such sub-processor to the List and provide notice to subscribers.

5.3. Customer may object to the engagement of a new Authorized Sub-Processor by providing written notice to Company within ten (10) days of receiving notice, provided such objection is based on reasonable grounds relating to data protection. Customer acknowledges that certain sub-processors are essential to the provision of the Services and that objecting to the use of a sub-processor may prevent Company from providing the affected Services.

5.4. If Customer reasonably objects to the engagement of a new Authorized Sub-Processor and Company cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue use of the affected Service by providing written notice to Company, subject to the terms of the Agreement.

5.5. Company will enter into a written agreement with each Authorized Sub-Processor imposing data protection obligations no less protective than those imposed on Company under this Addendum. Company shall remain responsible for the acts and omissions of its Authorized Sub-Processors with respect to the processing of Personal Data.

5.6. Where the EU Standard Contractual Clauses apply pursuant to Section 6 (Transfers of Personal Data), the foregoing authorizations constitute Customer's prior written consent to the engagement of sub-processors where such consent is required. Upon Customer's reasonable request, Company shall provide information regarding such sub-processors, subject to the redaction of confidential or commercially sensitive information.

6. Security of Personal Data

6.1. 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 risks of varying likelihood and severity to the rights and freedoms of natural persons, Company shall maintain appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk of processing Personal Data. Exhibit C sets forth additional information regarding Company's technical and organizational security measures.

6.2. In assessing the appropriate level of security, Company shall take account in particular of the risks that are presented by its Processing, in particular from a Personal Data Breach.

7. Transfers of Personal Data

7.1. Company may process and transfer Personal Data outside the European Economic Area ("**EEA**"), the United Kingdom, and Switzerland as necessary to provide the Services. Customer acknowledges that Company's primary processing operations are located in the United States. Where such transfers are subject to Data Protection Laws and are not subject to an adequacy decision, Company will implement appropriate safeguards in accordance with applicable Data Protection Laws.

7.2. EU Transfers. To the extent Personal Data originating in the EEA is transferred to a country not subject to an adequacy decision, such transfers shall be governed by the EU Standard Contractual Clauses, which are incorporated in this Addendum by reference. The applicable modules of the EU SCCs shall apply depending on the role of the parties, as described in this Addendum.

7.2.1. Module One (Controller to Controller) of the EU SCCs apply when Company is processing Personal Data as a controller pursuant to Section 9 of this Addendum.
7.2.2. Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Company is processing Personal Data for Customer as a processor pursuant to Section 2 of this Addendum.
7.2.3. Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and Company is processing Personal Data on behalf of Customer as a sub-processor.

7.3. UK Transfers. To the extent Personal Data originating in the United Kingdom is transferred to a country not subject to an adequacy decision, the EU Standard Contractual Clauses shall apply as modified by the UK Addendum, which is incorporated by reference.

7.4. Swiss Transfers. To the extent Personal Data originating in Switzerland is transferred to a country not subject to an adequacy decision, such transfers shall be governed by the EU Standard Contractual Clauses, interpreted to include the Swiss Federal Act on Data Protection and the authority of the Swiss Federal Data Protection and Information Commissioner.

7.5. Supplementary Measures. Company shall implement reasonable technical and organizational measures designed to protect Personal Data transferred pursuant to this Section 6, including measures to limit access to Personal Data and to challenge government access requests where legally permitted. Company shall notify Customer of legally binding requests for disclosure of Personal Data unless prohibited by law.

8. Data Subject Rights

8.1. Company shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise a Data Subject's rights under applicable Data Protection Laws (such requests individually and collectively "**Data Subject Request(s)**"). If Company receives a Data Subject Request in relation to Customer's data, Company will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Company, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

8.2. Company shall, at the request of the Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request or to demonstrate such compliance, where possible, provided that (i) Customer is itself unable to respond without Company's assistance and (ii) Company is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall, to the extent legally permitted, be responsible for any reasonable costs and expenses arising from such assistance by Company.

9. Personal Data Breach

9.1. Company shall notify Customer upon Company or any Approved Subprocessor first suspecting or becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with all necessary information to allow Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under Data Protection Laws.

9.2. Company shall, at its own cost, co-operate fully with Customer (and/or its advisors as applicable) in respect of the Personal Data Breach and take all reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach, by:

(a) co-operating with Customer (and/or its advisors as applicable) and any Supervisory Authorities; providing information on the Personal Data Breach; investigating the incident and its cause; and securing and recovering the compromised Customer Personal Data to the extent Company is able to do so; and

(b) coordinating with Customer (and/or its advisors as applicable) on the management of public relations and public statements relating to the Personal Data Breach. For the avoidance of doubt, Company shall not make any public statement in relation to the Personal Data Breach.

(c) Customer shall have sole control over the timing, content, and method of providing notification to the impact individuals and Supervisory Authorities of a Personal Data Breach as it relates to impacted Customer Personal Data.

10. Data Protection Impact Assessment and Prior Consultation

10.1. Company shall, taking into account the nature of the processing and the information available to Company, provide reasonable cooperation and assistance to Customer to enable Customer to conduct a data protection impact assessment or to demonstrate compliance with applicable Data Protection Laws, provided the Customer does not otherwise have access to the relevant information. Customer shall, to the extent legally permitted, be responsible for any reasonable costs and expenses arising from such assistance.

10.2. Company shall, taking into account the nature of the processing and the information available to Company, provide reasonable cooperation and assistance with respect to Customer's cooperation and prior consultation with any Supervisory Authority where required by applicable Data Protection Laws. Customer shall, to the extent legally permitted, be responsible for any reasonable costs and expenses arising from such assistance.

10.3. Company shall, taking into account the nature of the processing and the information available to Company, provide reasonable cooperation and assistance to Customer as necessary to enable Customer to comply with its obligations under applicable Data Protection Laws with respect to notification of the relevant Supervisory Authority and affected Data Subjects.

11. Audit Rights

11.1. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality obligations, Company shall, either (i) make available copies of

certifications or reports demonstrating Company's compliance with applicable data security standards, or (ii) where such materials are insufficient under applicable Data Protection Laws, permit an audit of Company's data protection practices by Customer's independent third-party auditor, provided that any such audit: (a) is conducted upon reasonable prior written notice; (b) occurs no more than once per calendar year; (c) is conducted during normal business hours; (d) does not unreasonably interfere with Company's business; and (e) is limited to data relevant to Customer. Customer shall bear the costs of any such audit, including reasonable reimbursement for Company personnel time.

12. Response To Complaints and Requests From Supervisory Authorities

12.1. In the event that Company receives any official complaint, notice, or communication that relates to Processing of Customer Personal Data, (including from a Data Subject or Supervisory Authority) in connection with the Order Form or Agreement, to the extent legally permitted, Company shall promptly notify Customer. Company shall provide Customer with reasonable cooperation and assistance in relation to any such complaint, notice, or communication.

12.2. Company shall inform Customer without undue delay of requests, audits, subpoenas, or other inquiries from a Supervisory Authority in relation to the Customer Personal Data or Processing of the Customer Personal Data as permitted under applicable law.

12.3. Company and Company Personnel shall provide Customer with reasonable cooperation in responding or cooperating with any audit, review, investigation, or other activity undertaken by a Supervisory Authority pertaining to the Processing of Customer Personal Data under this DPA.

13. Deletion or Return of Personal Data

13.1. Following completion of the Services, at Customer's choice, Company shall return or delete Customer's Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Company shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control.

13.2. Company and any Approved Subprocessor may retain Customer Personal Data solely to the extent required by any applicable Data Protection Laws and only to the extent and for such period as required by any applicable Data Protection Laws and always provided that Company shall ensure (and procure) the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified by any applicable Data Protection Laws requiring its storage and for no other purpose.

14. General Terms

14.1. Order of Priority

(a) Nothing in this DPA shall be intended to reduce, restrict or limit Company's

obligations under the Agreement in relation to the protection of Personal Data.

(b) In the event of conflict or inconsistency between the provisions of this DPA and the Agreement, this DPA shall prevail.

(c) No provision of the Agreement shall have the effect of excluding, restricting or limiting Company's obligations or Customer's rights under this DPA.

(d) For the avoidance of doubt, each Party shall bear its own costs incurred in connection with the preparation, negotiation, execution and performance of this DPA.

14.2. Change in Data Protection Laws, etc.

14.2.1. In the event of any change in, or decision of a competent authority under, the applicable Data Protection Laws, the Parties shall mutually agree in good faith on any amendments or changes to this DPA, and the Parties shall reasonably agree in good faith on a timeline for ensuring that such amendments or changes become applicable to Approved Subprocessors.

14.3. Severance

14.3.1. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either:

(i) be amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible;

(ii) be construed in a manner as if the invalid or unenforceable part had never been contained therein.

14.4. Termination

14.4.1. This DPA shall automatically terminate if the Agreement is terminated or expires.

14.4.2. Customer may terminate the Agreement with immediate effect by giving written notice to Company if Company commits a breach of any term of this DPA.

14.5. Governing Law and Jurisdiction

14.5.1. This DPA and all non-contractual or other obligations arising out of or in connection with it shall be governed by and construed as set out in the Agreement.

Exhibit A

Details of Processing

Nature and Purpose of Processing: Company will process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this Addendum, and in accordance with Customer's documented instructions.

Duration of Processing: Company will process Customer's Personal Data for the duration of the Agreement and thereafter only as necessary to comply with applicable law or for legitimate business purposes consistent with the Agreement and Company's privacy policy. Customer Account Data and Customer Usage Data will be processed and retained in accordance with Company's privacy policy.

Categories of Data Subjects: Customer's employees, consultants, contractors, and authorized users.

Categories of Personal Data: May include identifiers (such as name, email address, username), professional information (such as job title), device and usage information (such as IP addresses and device identifiers), and any other Personal Data submitted by or on behalf of Customer in connection with use of the Services.

Sensitive Data or Special Categories of Data: The Services are not intended for the processing of special categories of personal data or sensitive personal data (as defined under applicable Data Protection Laws), including data revealing criminal history, except where expressly agreed in writing by the parties and subject to appropriate safeguards. Customer remains responsible for ensuring that any Personal Data submitted to the Services complies with applicable Data Protection Laws.

Exhibit B

EU SCC Annex I & Annex II Information

The following includes the information required by Annex I and Annex II of the EU Standard Contractual Clauses ("SCCs"), and, where applicable, the UK Addendum.

Parties

Data Exporter: Customer, as identified in the applicable Order Form or Agreement.

Role: Controller

Data Importer:

Workshop Software, Inc.

1229 Millwork Avenue, Suite 200

Omaha, NE 68102

Email: privacy@useworkshop.com

Role: Processor

Description of the Transfer	
Data Subjects	Customer's employees, consultants, contractors, and authorized users.
Categories of Personal Data	Personal Data submitted by or on behalf of Customer in connection with use of the Services, which may include identifiers (such as name and email address), professional information (such as job title), and device and usage information.
Special Category Personal Data	The Services are not intended for the processing of special categories of personal data, except where expressly agreed in writing and subject to appropriate safeguards.
Nature of the Processing	Processing of Personal Data as necessary to provide, operate, maintain, and support the Services in accordance with the Agreement and this Addendum.
Purposes of Processing	As described in the Agreement and this Addendum.

Description of the Transfer	
Duration and Retention	For the duration of the Agreement and thereafter as described in this Addendum and Company's privacy policy.
Frequency of the transfer	Continuous and/or periodic during the term of the Agreement, as initiated by Customer's use of the Services.
Recipients of Personal Data Transferred to Data Importer	Company's authorized sub-processors, as listed at: https://docs.useworkshop.com/article/26-subprocessors.

Competent Supervisory Authority

The competent supervisory authority shall be determined in accordance with Clause 13 of the EU SCCs.

Exhibit C

Description of Technical and Organizational Security Measures

The following includes the information required by Annex II of the EU Standard Contractual Clauses ("SCCs").

Technical and Organizational Security Measures	
Pseudonymization and Encryption	Company uses industry-standard encryption protocols and secure transmission mechanisms to protect Personal Data in transit and at rest. Data stored in production systems is encrypted using managed encryption services provided by Company's cloud infrastructure providers.
Confidentiality, Integrity, Availability, and Resilience	Company maintains confidentiality obligations for personnel with access to Personal Data and requires Authorized Sub-Processors to enter into written agreements imposing data protection and confidentiality obligations no less protective than those set forth in this Addendum. Company maintains administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of Personal Data.
Backup and Recovery	Company performs regular backups of production systems and tests restoration procedures in accordance with its information security and data management policies to ensure availability and resilience.
Testing and Evaluation of Security Measures	Company conducts regular risk assessments, security reviews, and independent audits, including annual SOC 2 Type II assessments, to evaluate the effectiveness of its technical and organizational security measures.
User Identification and Access Control	Access to production systems is restricted based on role and business need and protected using strong authentication mechanisms, including multi-factor authentication. Network access is restricted and monitored in accordance with industry best practices.

Technical and Organizational Security Measures	
Data Transmission Security	Company protects Personal Data transmitted over public networks using secure communication protocols and encryption.
Data Storage Security	Personal Data stored within Company systems is protected using encryption and access controls appropriate to the sensitivity of the data.
Physical Security	All production infrastructure is hosted in secure data centers operated by Company's cloud service providers, which maintain physical security controls and compliance programs consistent with industry standards.
Logging and Monitoring	Company monitors access to systems processing Personal Data and maintains logging and alerting mechanisms to detect and investigate security events.
Configuration and Change Management	Company uses formal change management processes and automated deployment mechanisms to ensure secure and consistent system configurations.
Information Security Governance	Company maintains an information security program designed around risk-based governance principles, incorporating administrative, technical, and physical safeguards.
Data Minimization and Retention	Company processes Personal Data only as necessary to provide the Services and in accordance with Customer instructions. Customer Data is deleted or returned following service termination in accordance with the Agreement, this Addendum, and applicable law.
Accountability	Company maintains policies, procedures, and assigned responsibilities for information security and data protection and conducts periodic internal and third-party assessments.

Technical and Organizational Security Measures	
Sub-Processor Security	Company requires Authorized Sub-Processors to implement appropriate technical and organizational security measures and to comply with contractual data protection obligations substantially similar to those set forth in this Addendum.