DATA PROCESSING AGREEMENT

This Data Processing Agreement including its appendices ("**DPA**") forms an integral part of EULA between CO FSM and the Client. The DPA applies solely to the extent that CO FSM processes Personal Data (defined below) in connection with CO FSM's Services. All capitalized terms not defined in this DPA shall have the same meaning as defined in the EULA.

1. **Definitions:**

"**Applicable Privacy Law"** means all data protection and privacy laws and regulations applicable to the respective party in its role in the processing of Personal Data under the Agreement, including General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016. ("**GDPR"**).

"**Personal Data"** means any data related to or associated with an identified or identifiable natural person, including, but not limited to, any Client employee information, or Client customer information contained within Client Data. A natural person is identifiable if, with means reasonably likely to be used, the individual could be identified from the data or a grouping of data.

"**Services"** means the Software Solution as defined in the EULA and/or any other services provided directly by CO FSM to the Client under the Agreement.

"**Sub-processor"** means any third party engaged by CO FSM to process Personal Data in connection with the Services pursuant to the EULA.
Terms such as "**controller", "processor", "data subject"** and other terms shall have the meaning given under Applicable Privacy Law.

In addition to this DPA, in case of international data transfers, the European Commission's standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council according to the Commission's implementing decision 2021/914 of 4 June 2021 shall apply ("**Standard Contractual Clauses**" or "**SCC"**).

2. **Processing of Personal Data**

- **Scope and roles of the Parties.** This DPA applies when the Personal Data is processed by CO FSM as a processor ("**Processor**") in its provision of the Services to the Client, who will act as either controller or processor of Personal Data ("**Controller**").
- **Client obligations.** The Client will comply with its obligations under Applicable Privacy Law in its processing of the Personal Data. The Client is responsible for the lawfulness of

Personal Data processing under or in connection with this DPA. The Controller warrants that it has provided all notices and obtained all consents, permissions, and rights necessary under Applicable Privacy Law for CO FSM to lawfully process Clients Personal Data. The Client shall ensure that its processing instructions comply with Applicable Privacy Law and that processing of Clients Personal Data by CO FSM in accordance with its instructions will not cause CO FSM to be in breach of Applicable Privacy Law.

- **CO FSM obligations.** CO FSM will comply with its obligations under Applicable Privacy Law in its capacity as a processor. CO FSM will process Personal Data only to perform its obligations under the Agreement and only on documented instructions from the Client unless required to do so by Applicable Privacy Law to which the Processor is subject. If the Processor deems that an instruction violates Applicable Privacy Law, the Processor shall promptly inform the Controller. However, this shall not apply if the law in question prohibits such notification for reasons of substantial public interest. The Processor shall then be entitled to suspend the execution of the instruction by written notice to the Controller until both Parties confirm the instruction. Processor shall not I) retain, access, use, sell, share, or otherwise process any Personal Data for any purpose other than the provisions under EULA and only to the extent necessary to provide Services; II) combine Personal Data which CO FSM receives from or on behalf of the Client, with Personal Data which it receives from or on behalf of another person or persons.

- **Details of processing.** The Client is responsible for submitting Personal Data to the Software Solution. This data may include, but it is not limited to Personal Data relating to the following categories of data subject: customers, business partners, employees or contract persons. Details of the processing of Personal Data are given in the Annex 1 to the DPA.

3. Subprocessing

- **Authorization.** The Processor is authorized to enter into agreements with another data processor, e.g. a Sub-Processor, regarding the processing of Personal Data. The Controller should be informed about currently engaged Sub-Processors and the Processor is obligated to inform the Controller about any additional change of engaged Sub-Processors in the future. The Client may object to CO FSM's appointment of a new Sub-Processor on reasonable grounds relating to data protection by notifying CO FSM in writing at privacy@closeout.cloud. In such an event, CO FSM and Client will discuss those objections in good faith with a view to achieving resolution. If the Parties are not able to achieve resolution, the Client, may terminate the Services with respect to only those aspects which cannot be provided by CO FSM without the use of the new Sub-processor (if possible).

- **Subprocessors obligation.** The Processor shall draw up a written sub-processing agreement with another Sub-Processor. In its agreement with Subprocessor, the Processor shall ensure that the Subprocessor as a minimum accepts the same data protection obligations as those undertaken by the Processor in this DPA. The Processor shall guarantee the lawfulness of Subprocessor's processing of Personal Data. If Subprocessor fails to fulfill its data protection obligations, the Processor shall remain fully liable to the Controller for the fulfillment of such Subprocessors obligations. The fact that the Controller has consented to the Processor entering into an agreement with Subprocessor shall be of no consequence to the Processor's obligation to comply with the DPA. When an agreement with Subprocessor regarding the processing of Personal Data comprised by the DPA terminates, the Processor shall notify the Controller thereof.

The Controller agrees that the Processor may engage the following Sub-processors:

- Amazon Web Services EMEA SARL, ("AWS Europe")
- Pty Ltd Level 6, 341 George Street, Sydney NSW 2000

CO FSM group sub-processor:

- CloseOut Cloud Inc. 200 Continental Drive, Suite 401, Newark, Delaware 19713

4. Tranasfer of Personal Data

- **Transfer mechanism.** The Processor guarantees that any transfer of Personal Data processed on behalf of the Client will be carried out only if appropriate security measures and safeguards are applied in accordance with the Applicable Privacy Law. All transfers of Personal Data to provide Services are subject to the terms of Standard Contractual Clauses implemented by CO FSM.
- **Personal data location.** For the purposes of providing appropriate support, the Processor process Personal Data within its premises. In any other case, Personal Data is stored and processed on an available public cloud provider's infrastructure (AWS) in Europe or USA (depending on Clients choise) or Client's private cloud infrastructure. Processor does not and cannot control or limit the regions from which Client may access its Personal Data.

5. Security

- **Security measures.** The Processor will implement appropriate technical and organizational measures so that the processing of Personal Data will meet the requirements of Applicable Privacy Laws. Protective measures include using state-of-the-art software, computers, and encryption methods as well as the use of adequate access controls, password procedures, automatic blocking, case-specific authorization concepts,

logging and documentation of processes, and the implementation of a data security concept in accordance with ISO 27001 standard and GDPR principles. The measures taken shall be adequate for the protection of Personal Data against accidental or unlawful destruction, loss, or alteration and against unauthorized disclosure, abuse, or other processing in breach of the Applicable Privacy Law at any time.

- CO FSM shall ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- **Modification of security measureas.** CO FSM may update and/or modify security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services provided to the Client. Detail list of technical and organizational measures are given in Annex II.
- **Controller's obligation.**The Controller is responsible for its secure use of the Services including securing its Access credentials, and appropriate steps to securely encrypt or backup any Personal Data in connection with the Services. CO FSM shall, taking into account the nature of processing and the information available to CO FSM, assist the Client in ensuring compliance with the obligations on data protection impact assessments and prior consultations in accordance with Applicable Privacy Law.
- **Personal Data breach.** Upon becoming aware of the security breach, the Processor shall without undue delay, but no later than 72 hours after becoming aware of the security breach notify the Controller and shall provide all information relating to the security breach. CO FSM shall investigate the cause of the security breach and take all reasonably necessary actions to mitigate the impact of the security breach. If necessary, CO FSM shall assist the Controller with notifying the competent supervisory authority regarding a Personal Data security breach.

6. Assistance

- **Assistance to the Controller.** In cases where the Controller becomes subject to any inspections, investigations, and/or administrative measures conducted by a supervisory, legal or regulatory authority, an administrative offense, criminal procedure, a claim by a data subject or by a third party or any other claim relating to this DPA, the Processor shall take all steps required to support the Controller.
- **Data Subject requests.** The Processor will inform the Controller as soon as possible about any complaints, inquiries, requests or other communications received from data subjects, data protection authorities or third parties relating to the processing of Personal Data by the Processor and/or the Controller and where, in accordance with Applicable Privacy

Laws, Controller is obliged to answer a data subject's complaints, inquiries, requests or other communication relating to the processing of such data subject's Personal Data, Processor shall support Controller in providing the required information. Processor shall not directly respond to any complaints, inquiries, requests, or other communications of data subjects and shall refer such data subjects to the Controller.

7. Audit

CO FSM shall make available to the Client all information necessary to demonstrate compliance with the obligations laid down in Applicable Privacy Law. The Client shall be entitled to audit whether the Processor fulfills its obligations in accordance with this DPA, during usual business hours where the Controller gives reasonable (but in any event no less than 30 days) prior written notice to the Processor. The Controller shall bear all costs resulting from the audit and compensate the Processor for all costs incurred as a result of the audit. Nothing herein shall be construed to require CO FSM to provide any proprietary information, trade secrets, or any other information that would violate CO FSM's confidentiality obligations.

8. Return and deletion

At all times during the Term of EULA, the Client shall have the ability to access, change or delete Personal Data. At the end of the provision of the Services, all Client Data and Personal Data shall be destroyed in accordance with article 10 of EULA, unless Applicable Privacy Law requires longer storage of Personal Data.

9. California Consumer Privacy Act of 2018 ("CCPA")

CO FSM shall not process, retain, use or disclose Personal Data for any purpose other than for the purposes set out in the Agreement and is permitted under the CCPA. CO FSM shall not sell any of Personal Data.

10. General

- The DPA shall remain in force for as long as the Processor processes Personal Data on behalf of the Controller in accordance with the EULA.
- **Governing Law.** Any dispute or claim arising out or in connection with this DPA shall be finally settled by arbitration administered by the SCC.
- If any of this DPA is held unenforceable, the validity of all remaining parts will not be affected.
- **Modifications of DPA.** CO FSM may update this DPA from time to time, with such updated version posted on this site, provided, however, that no such update shall materially diminish the privacy or security of Personal Data.

- Each Party's liability arising out of or realated to this DPA, shall remain subject to the limitation of liability section of the EULA.

In addition to the DPA, where the transfer of Personal Data to CO FSM in accordance with the Applicable Data Protection Laws require that appropriate safeguards are put in place, such transfer will be governed by the SCC, which shall be deemed incorporated into and form part of the DPA as follows:

APPENDIX

STANDARD CONTRACTUAL CLAUSES

I. Modul Two terms shall apply **(**where Client is the controller of Personal Data) and the Module Three terms shall apply (where the Client is the processor of Personal Data). In each case CO FSM is a processor to the Client.

II. Clause 7 Docking clause, the optional docking clause shall apply.

III. Clause 9 Use of Sub-processors, option 2 ("general authorization") is selected, and the process and time period for prior notice of Sub-processor changes shall be 30 days in advance

IV. Clause 11 Redress, the optional language shall not apply

V. Clause 17 Governing law, option 1, the SCC will be governed by the laws of Austria.

VI. Clause 18 Choice of forum and jurisdiction, All disputes will be resolved before the courts of Austria.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter	**Data importer**
Name: The party identified as the Client in the Agreement.	Name: CloseOut FSM d.o.o.
Contact person's name, position, and contact details: as set out in the Proposal.	Contact person's name, position, and contact details: as set out in the Proposal. privacy@closeout.cloud.

Activities relevant to the transfer: Defined in Annex 1(B)	Activities relevant to the transfer: Defined in Annex 1(B)
Role: Controller	Role: Processor

B. DESCRIPTION OF TRANSFER

tegories of data subjects whose personal data is transferred.	Data subjects include individuals who use Services (Authorized Third Persons), including Client's employees, contractors and customers.
Categories of personal data transferred.	Access credentials and other contact data (such as name, contact details, phone number, email address), company, location, job title, certificates, photos, and device IDs. Any other personal data depending on the Clients use of the Service.
Sensitive data transferred	N/A
The frequency of the transfer	Depends on the Client's use of the Services.
Nature of the processing	The Services and the Support Services as set out in the Agreement
Purpose(s) of the data transfer and further processing	CO FSM will process the Personal Data to manage its business relationship with the Client, to provide agreed Services, to improve and enhance its Services, to provide Support Services, for security purposes, and to comply with legal obligations.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	CO FSM shall process Personal Data for the Term of the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.	The subject matter, nature, and duration of Processing for Sub-processors are dependent upon the Services subscribed by the Client. In particular: - For Cloud Services, CO FSM Sub-processors provide infrastructure, security and alert monitoring, and reporting services, and process Client Personal Data that the Client uploads for the duration of the Services under the Agreement. - For Support Services, Sub-processors process Client Personal Data in order to provide the Support Services pursuant to the Agreement and for the duration of the Agreement Term. - For Reseller/Distributor Services, Sub-processors process Client Personal Data to provide Services pursuant to the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority will be determined in accordance with Applicable Privacy Law.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. **Measures of pseudonymization and encryption of personal data**

- Encryption in transit is implemented as all communication between WEB front-end servers and Mobile App towards CO FSM back-end servers, is secured via HTTPS mechanism with servers' SSL certificate. Secure communication ensures that data transmitted between the Client and the backend application is encrypted and protected from eavesdropping and tampering.

- For the rest of the encryption, CO FSM is using SSE-S3 with one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt all Personal Data.
- Each user is authenticated with unique user ID/password parameters. Users' access to the Hosted Services is password protected. CO FSM follows the strong password principle, which involves enforcing password policies that require users to create strong and complex passwords to protect their accounts. Strong passwords include a combination of uppercase and lowercase letters, numbers, and special characters. All passwords on the platform are stored in encrypted form and are fully protected in terms of security.

2. **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.**

- **Confidentiality Obligations.** CO FSM personnel are required to agree to confidentiality obligations before undertaking work for CO FSM or accessing any CO FSM facilities and/or systems.
- **Password Policy.** CO FSM password management enforces password policy requirements, such as password complexity which includes a combination of uppercase and lowercase letters, numbers, and special characters.
- **Operational Security & Vulnerability Response.** CO FSM monitors a variety of communication channels for operational and capacity management, and security vulnerabilities, and CO FSM's operations and security team will react promptly to known operational issues and/or security vulnerabilities.
- **Server Operating System.** CO FSM uses a hardened operating system implementation customized for the CO FSM Services.
- The Cloud Services are incrementally backed up and virtually replicated.

3. **Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing.**

- **Software Development Lifecycle.** The Cloud Services are developed using a standardized and reviewed Secure Software Development Lifecycle (SDL) to reduce the risk of introducing security vulnerabilities into the production of Cloud Services.
- **Penetration Testing & Vulnerability Scans.** External penetration tests are performed by an independent third party on an annual basis and incorporated as a requirement of the CO FSM product compliance programs. Vulnerabilities identified are routinely documented, tracked, and resolved by the respective service team.

4. **Measures for user identification and authorization.**

- **User Roles.** Client has primary control over the creation, deletion, and suspension of user roles within the Client's environment of the Software Solution.

5. **Measures for ensuring physical security of locations at which personal data are processed.**

- **Hosting Infrastructure and Data Center Security.** CO FSM currently uses infrastructure provided by Amazon Web Services, for the infrastructure of its Cloud Services.

6. **Measures for ensuring events logging.**

- **Events Logging.** CO FSM maintains logs of every user action and is making these logs available to system administrators for search and overview. Logs are used to detect and investigate security incidents, track user actions, and ensure compliance with security policies and regulations.

7. **Measures for ensuring system configuration, including default configuration.**

- **Code Review Process.** CO FSM's change management includes a code review process within an established review process and in accordance with a defined policy.

8. **Measures for internal IT and IT security governance and management.**

- **Information Risk Governance.** CO FSM reviews, maintains, and ensures adherence to formal IT security and data handling policies.

- **Information Security Roles & Responsibilities**. All information security responsibilities are defined and allocated.

9. **Measures for ensuring data minimization.**

- **Software Development Lifecycle.** Privacy checks are performed during the Software Development Process when new product features are developed.

- **Access Restrictions.** Restrict access to Personal Data to the parties involved in the processing in accordance with the "need to know" principle and according to the function behind the creation of differentiated access profiles.

10. **Measures for ensuring data quality.**

- **Secure Development Environment**. Development environments are protected from malicious or accidental development and update of code that may compromise the confidentiality, integrity, and availability of the platform.

11. **Measures for ensuring limited data retention.**

- At the end of the provision of the Services, all Personal Data shall be destroyed by CO FSM as a processor (including copies) in its possession or control in accordance with the Agreement.

12. Sub-processors technical and organizational measures can be found at the following link:

- https://d1.awsstatic.com/legal/awsgdpr/AWS_GDPR_DPA.pdf
- Data Processing Addendum | Atlassian

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Amazon Web Services EMEA SARL, ("AWS Europe"), contact: AWS Compliance Reports Support – Amazon Web Services For Cloud Services, AWS provides infrastructure, security and alert monitoring, and reporting services.
2. Pty Ltd Level 6, 341 George Street, Sydney NSW 2000, contact: dpasubmission@atlassian.com. For Support Services, Atlassian Process Client Personal Data if provided by the Client in order to provide the Support Services pursuant to the Agreement and for the duration of the Services Term.

CO FSM group sub-processor:

3. CloseOut Cloud Inc. 200 Continental Drive, Suite 401, Newark, Delaware 19713. CloseOut Cloud Inc. as a reseller and affiliated legal person with CO FSM, may Process Client Personal Data to provide technical and operational assistance.