DATA PROCESSING AGREEMENT FOR PERFORCE CUSTOMERS

This Data Processing Agreement ("**DPA**"), is dated effective as of the date of the last signature below ("**Effective Date**"), and is made by and between the organization identified below ("**Customer**") and Perforce Software, Inc., a Delaware corporation, having a principal place of business at 400 North First Avenue, Suite 400, Minneapolis, Minnesota 55401 USA, and its Affiliates ("**Perforce**"), each a "**Party**" and collectively the "**Parties**." This DPA applies where, and only to the extent that, Perforce Processes Customer Data in the course of providing Services to the Customer under the Agreement and forms a part of the Agreement.

1. **Definitions**.

a) "**Affiliate**" has its meaning as set forth in the Agreement (if defined) or means any entity (i) that is owned more than 50% by a Party, (ii) over which a Party exercises management control, (iii) that is under common control with a Party, or (iv) that owns more than 50% of a Party's voting securities or other voting interests of an entity. As to Customer, any reference to "Affiliate" herein is strictly limited to those Affiliates of Customer that qualify as a Controller and are permitted to use the Services pursuant to the Agreement.

b) "**Agreement**" means the existing agreement(s), order(s), purchase orders and statements of work, or other commercial arrangement, pursuant to which Perforce provides the Services to Customer and includes any exhibits and subsequent amendments, or orders.

c) **"Customer Data"** means that Personal Data that Perforce Processes in the course of providing the Services to Customer.

d) "**Data Protection Laws**" means all data protection, privacy and cyber security laws and regulations of any country applicable to Perforce's Processing of Customer Data under the Agreement, including (where applicable and without limitation) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"), GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"), the revised Swiss Data Protection Act ("**revDPA**"), data protection laws of the European Union ("**EU**") or European Economic Area member states ("**EEA**") or the United Kingdom (including Gibraltar) ("**UK**") that supplement GDPR or UK GDPR (respectively), and California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively referred to as the "**CCPA**") in each case as may be amended or superseded from time to time.

e) "**Data Subject**" means the individual to whom the Personal Data relates, which is Processed for the performance of the Agreement by Perforce.

f) "**ex-EEA Transfer**" means a Processing activity whereby Customer Data which is Processed in accordance with the GDPR is transferred from Customer to Perforce outside 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.

g) "**ex-Swiss Transfer**" means a Processing activity whereby Customer Data which is Processed in accordance with Swiss Data Protection Laws is transferred from Customer to Perforce outside Switzerland and such transfer is not governed by an adequacy decision made by the Federal

Data Protection and Information Commissioner of Switzerland ("**FDPIC**") in accordance with the relevant provisions of the revDPA.

h) "**ex-UK Transfer**" means a Processing activity whereby Personal Data which is Processed in accordance with the UK Data Protection Laws is transferred from Customer to Perforce outside the UK or Gibraltar, and such transfer is not governed by an adequacy decision pursuant to Section 17A of the UK Data Protection Act 2018.

(a) "**Personal Data**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household. This definition includes "Personal Data," "Personal Information," or "Personally Identifiable Information," as defined by any applicable Data Protection Laws. Personal Data does not include information or data that has been Processed in such a manner that no longer identifies, relates to, describes, or is capable of being associated or linked with a particular Data Subject.

i) "**Personal Data Breach**" means any unauthorized or unlawful breach of security leading to the unauthorized access to, disclosure of, loss of, alteration of, or acquisition of Customer Data.

j) "**Processing**" or "**Process**" means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether by automated means, 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.

k) "**Restricted Transfer**" means (i) where the GDPR applies, an ex-EEA Transfer, (ii) where the UK GDPR applies, an ex-UK Transfer, and (iii) where the revDPA applies, an ex-Swiss Transfer.

l) "**Services**" means the software, software as a service, software-related products, support and maintenance services, professional services, and such other activities to be supplied to or carried out by or on behalf of Perforce for Customer per the Agreement, or as otherwise defined in the Agreement.

m) "**Subprocessor**" means any third party (including any Perforce Affiliate) appointed by or on behalf of Perforce or any Perforce Affiliate to Process Customer Data in connection with the Services or the Agreement.

2. **Scope and Applicability.** Customer hereby instructs Perforce to Process Customer Data on Customer's behalf. In respect of such Processing, and as between Perforce and Customer, Customer will be the controller (or, where Customer is instructing Perforce on behalf of a third-party controller, a processor on behalf of that controller) and Perforce will be a processor (or, where Customer is a processor on behalf of a third-party controller, Perforce will be a subprocessor to Customer). The "Business Purpose" for Perforce's Processing of Customer Data on Customer's behalf is identified in Schedule 1. The duration of processing, the nature and purpose of the processing, the types of Customer Data, and the categories of data subjects processed under this DPA are further specified in Schedule 1.

3. **Perforce Obligations.** Perforce may Process Customer Data on behalf of Customer solely in accordance with the terms of the Agreement, this DPA, the Data Protection Laws applicable to such Processing by Perforce, and Customer's lawful instructions. Perforce shall ensure that any

person who is authorized by Perforce to Process Customer Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty), with respect to such Personal Data. Perforce shall implement and maintain throughout the term of this DPA appropriate technical and organizational measures as set forth in Schedule 2. In assessing the appropriate level of security, Perforce will take into account the risks, including those resulting from a Personal Data Breach, that are presented by the Processing at issue. Customer acknowledges that these technical and organizational measures are subject to technical progress and development and that Perforce may update or modify these technical and organizational measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by Customer.

4. **Customer Representations and Warranties.** Customer hereby represents and warrants that it: (a) will maintain appropriate notice and consent mechanisms, consistent with applicable Data Protection Laws, for the collection, use, and disclosure of Customer Data; (b) has any and all consents, authorizations, rights, and authority necessary to transfer or disclose, and permit Perforce to Process, any and all Customer Data in connection with the Agreement; and (c) will have sole responsibility for the accuracy, quality, and legality of any and all Customer Data Processed by Perforce. Customer will promptly notify Perforce if it is unable to comply with any of its obligations hereunder.

5. **Subprocessors.** Customer acknowledges and expressly agrees that Perforce may retain its Affiliates or certain third parties as Subprocessors to Process Customer Data in order for Perforce to provide the Services. Customer hereby authorizes Perforce to engage the Subprocessors set forth in Schedule 3. Customer shall have notification rights and rights to object to such Subprocessors in accordance with Schedule 3. Prior to a Subprocessor's Processing of Customer Data, Perforce shall: (a) enter into an agreement with the Subprocessor that imposes data protection terms on the Subprocessor regarding the processing of Customer Data to the standard required by Data Protection Laws, and (b) remain responsible for its compliance with the obligations subcontracted to the Subprocessor.

6. **Personal Data Breach.** In the event that Perforce becomes aware of a Personal Data Breach, Perforce will notify Customer without undue delay, in accordance with Data Protection Laws, and shall provide timely information relating to the Personal Data Breach as it becomes known or as is reasonably requested by Customer, unless otherwise prohibited by law or otherwise instructed by a law enforcement or supervisory authority. Following such notification, Perforce will take reasonable steps to mitigate the effects of the Personal Data Breach and provide reasonable assistance and cooperation regarding any notifications that Customer is legally required to send to affected Data Subjects and regulators.

7. **Security Reports and Audit Obligations.** Perforce shall provide written responses (on a confidential basis) to all reasonable requests for information made by Customer that Customer (acting reasonably) considers necessary to confirm Perforce's compliance with this DPA, as well as applicable Data Protection Laws (including the GLBA Safeguards Rule as it relates to service providers). Customer consents to Perforce satisfying the foregoing audit obligation by providing Customer with attestations, certifications, and summaries of audit reports conducted by accredited third party auditors.

8. **Customer Security Responsibilities.** Notwithstanding anything herein to the contrary, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of

Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services. Perforce's liability for a Personal Data Breach toward Customer and any third party is subject to the following conditions: (a) the Personal Data Breach is caused by a violation of Perforce's or its Subprocessor's obligations set forth in this DPA (including violation of Data Protection Laws); and (b) excluding liability caused by acts or omissions of Customer, or any person acting on behalf of or jointly with Customer.

9. **Information and Assistance.** To the extent required by an applicable Data Protection Law, Perforce will cooperate with Customer in compiling necessary records of processing activities for Customer as well as in necessary data protection impact assessments of the Customer or subsequent consultation with a data protection supervisory authority or regulator. Perforce may charge a reasonable fee for any such assistance, as permitted by applicable law.

10. **Data Subject Requests**. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, Perforce shall (to the extent permitted by law, at Customer's expense) taking into account the nature of the Processing, provide reasonable cooperation to assist Customer by appropriate technical and organizational measures, in so far as is possible, to respond to any requests from individuals or applicable data protection authorities relating to the processing of Customer Data under the Agreement. In the event that any such request is made directly to Perforce, Perforce shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so.

11. **Subpoenas and Court Orders.** If a law enforcement agency sends Perforce a demand for Customer Data (for example, through a subpoena or court order), Perforce shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Perforce is legally prohibited from doing so.

12. **Return or Disposal of Data.** Upon termination or expiration of the Agreement for any reason, Perforce will return or destroy Customer Data (including copies) in its possession or control at Customer's request and choice in accordance with the Agreement. Notwithstanding, this requirement shall not apply to the extent Perforce is required by applicable law to retain some or all of the Customer Data.

13. **Limitation of Liability.** Each party's and all of its Affiliates' liability, taken together in the aggregate, 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 in the Agreement, and any reference in provisions to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA together. For the avoidance of doubt, Perforce and its Affiliates' total liability for all claims from the Customer and all of its Affiliates arising out of or related to the Agreement and this DPA shall apply in the aggregate for all claims under both the Agreement and this DPA.

14. **International Data Transfers.** Perforce may transfer Customer Data to, and process Customer Data in, the United States and anywhere else in the world where Perforce or its Subprocessors maintain data processing operations, and Customer hereby consents to the transfer of Customer Data to Perforce and Subprocessor data processing operations located in the United States or anywhere else in the world where Perforce or its Subprocessors maintain data processing operations, provided that any transfers by Perforce that constitute Restricted Transfers will be subject to a

transfer impact assessment and/or any other legally-required transfer mechanism, which will be available to Customer for review upon request.

a) The Parties agree that when the transfer of Customer Data from Customer (as data exporter) to Perforce (as data importer) is an ex-EEA Transfer, such transfers will be subject to Module Two (*Controller to Processor*), in the case of Customer acting as the controller, or Module Three (*Processor to Processor*), in the case of Customer acting as the Processor to its customer who is the controller, of the Standard Contractual Clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021 (as amended and updated from time to time) ("**EU SCCs**"). The EU SCCs are deemed incorporated into the Agreement by reference, replace and supersede any former SCCs, take precedence over the rest of the Agreement to the extent of any conflict, and, for the purposes of this DPA (and the UK and Swiss provisions below), are completed as follows:

   i) The optional docking clause in Clause 7 does not apply;

   ii) In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of Subprocessor changes shall be as set forth in Schedule 3 to this DPA;

   iii) In Clause 11, the optional language does not apply;

   iv) In Clause 17 (Option 1), the EU SCCs will be governed by law of Ireland;

   v) In Clause 18(b), disputes will be resolved before the courts of Ireland;

   vi) Schedule 1 to this DPA contains the information required in Annex I of the EU SCCs;

   vii) Schedule 2 to this DPA contains the information required in Annex II of the EU SCCs; and

   viii) Schedule 3 to this DPA contains the information required in Annex III of the EU SCCs.

b) The Parties agree that when the transfer of Customer Data from Customer to Perforce is an ex-UK Transfer, such transfer will be subject to the EU SCCs, as amended by and together with the following terms which the Parties hereby agree are legally binding upon the parties with the same effect as the terms and conditions of this DPA:

   Part 1:

   1. *Start Date.* The effective date of this Addendum is this DPA Effective Date.

   2. *Parties' Details.* The "Customer" as defined in this DPA is the "Exporter." Perforce is the "Importer." The Parties' details are set forth in the Signature Section and Schedule 1.

   3. *Addendum EU SCCs.* For the purposes of this Addendum, the "Addendum EU SCCs" means the EU SCCs identified in Section 13(a) to this DPA, including the Appendix Information (defined below) and with only the modules, clauses, and optional provisions of the EU SCCs brought into effect for the purposes of this section as set forth in Section 13(a) of this DPA.

   4. *Appendix Information.* "Appendix Information" or "Table 3" for the purposes of the Mandatory Clauses, means the information which must be provided for the Approved EU

SCCs and which for this section is set forth as follows:

a. “Annex 1A” shall be deemed to mean that information as per Part 1, Section 2 above.

b. “Annex 1B” shall be deemed to mean that information in Schedule 1.

c. “Annex II” shall be deemed to mean that information in Schedule 2.

d. “Annex III” shall be deemed to mean that information in Schedule 3.

5. *Ending the Addendum when the Approved Addendum Changes.* The Importer may end the terms of this section as set forth in the Mandatory Clauses, Section 19.

Part 2:

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

c) The Parties agree that when the transfer of Customer Data from Customer (as data exporter) to Perforce (as data importer) is an ex-Swiss Transfer, such transfers are made pursuant to the EU SCCs with the modifications set forth below:

i) The terms of this section apply solely to the Processing of Customer Data of Data Subjects who are residents of Switzerland and not to the Processing of any other Personal Data.

ii) The transfer of Personal Data shall, to the extent legally permitted, be governed by the provisions of the revDPA; references to provisions of the GDPR in the EU SCCs shall be understood to be referring to the equivalent provisions of the revDPA.

iii) Clause 13 is modified so that the Federal Data Protection and Information Commissioner is the competent supervisory authority with respect to Personal Data transfers governed by the revDPA.

iv) For the purposes of the Clauses, the term “Member State” shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with Clause 18.c.

15. **CCPA.** This section only applies to the Personal Information of California Consumers included in the Customer Data. For the purposes of this section, “Collects,” “Consumer,” “Personal Information,” “Processing,” “Sell,” and “Share” shall have their meanings as set forth in the CCPA. The Parties acknowledge and agree that Perforce is Processing Personal Information pursuant to the Agreement as a “service provider” (as defined by the CCPA) of Customer for the Business Purposes (as defined in this DPA). As such, Perforce represents and warrants as follows: (a) Perforce will not retain, use, or disclose any Personal Information it Collects pursuant to the Agreement for any purpose other than the Business Purposes or as otherwise permitted by the CCPA; (b) Perforce shall not Sell or Share any Personal Information it Collects pursuant to the Agreement; (c) Perforce shall not retain, use, or disclose the Personal Information that it Collects pursuant to the Agreement outside of the direct business relationship between Perforce and Customer, except as permitted by the CCPA; and (d) Perforce shall not combine any Personal Information it Collects pursuant to

the Agreement with Personal Information that it receives from, or on behalf of, another person or business, or that it Collects from its own interactions with individuals, except as permitted by the CCPA. The parties acknowledge and agree that any combining contemplated by the Services is being performed by Perforce for the Business Purposes and such purposes constitute a "business purpose" (as defined by the CCPA). Perforce further agrees as follows: (a) Perforce will comply with all applicable sections of the CCPA, including by providing the same level of privacy protection as required by businesses subject to the CCPA; (b) Perforce will implement those reasonable security procedures and practices set forth in this DPA with respect to the Personal Information it Collects pursuant to the Agreement; (c) Customer may monitor Perforce's compliance with this section and Customer's obligations under the CCPA, in accordance with the audit terms set forth in this DPA; (d) Customer may, upon notice, take those reasonable and appropriate steps set forth in this DPA and the Agreement to stop and remediate any unauthorized use of Personal Information by Perforce; (e) Perforce will notify Customer of any Consumer requests pursuant to the terms of this DPA; (f) Perforce will notify Customer after it makes a determination that it can no longer meet its obligations under the CCPA; and (g) if Perforce subcontracts with another person in providing services to Customer, Perforce will have a contract with such subcontractor that complies with the CCPA.

16. **Miscellaneous.** To the extent applicable, the parties agree that by entering into and executing this DPA, the EU SCCs and all Schedules constitute legally binding contracts between the parties and are hereby deemed to be signed by the parties. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict. Unless otherwise provided for in this DPA or required by applicable Data Protection Law, this DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement. Any disputes between the parties arising under this DPA are to be handled as set out in the Agreement.

[The Remainder of this Page is Intentionally Left Blank]

Authority of Signatories. By signing below, each Party: (i) indicates that it agrees to all terms and conditions of this DPA; and (ii) further warrants to the other Party that (A) it has the authority to enter into this DPA, (B) all necessary corporate or other approvals have been or will be obtained, and (C) the individual who has signed this DPA on behalf of a Party is authorized to do so.

PERFORCE:

PERFORCE SOFTWARE, INC.

By: ______________________________
Name: Sara M. Kilian
Title: VP and General Counsel

Date: ______________________________

CUSTOMER:

____

By: ______________________________

Name: ______________________________

Title: ______________________________

Date: ______________________________

SCHEDULE 1:

DETAILS OF PROCESSING OF PERSONAL DATA

A. LIST OF PARTIES

***For the purposes of the EU SCCs, this information constitutes the details of "Annex 1.A".*

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name:

Address:

Contact person's name, position, and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date: ______________________________

Role (controller/processor): Controller or Processor (where Customer is acting on behalf of a third-party controller)

Data importer(s):

Name: Perforce Software, Inc.

Address: 400 North First Avenue, Suite 400, Minneapolis, Minnesota 55401 USA

Contact person's name, position, and contact details: Sara M. Kilian, Vice President and General Counsel; privacy@perforce.com; +1 (612) 517-2100.

Activities relevant to the data transferred under these Clauses: Perforce's provision of the Services under the Agreement.

Signature and date: ______________________________________

Role (controller/processor): Processor or subprocessor (where Perforce is a processor acting on behalf of a third-party controller)

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose Personal Data may be Processed and/or transferred as Customer Data: Employees and third-party contractors of Customer.

Categories of Personal Data that may be Processed and/or transferred as Customer Data: Business email address, business telephone, business address, job title.

Sensitive/special categories of data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved (such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures): None.

Frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis): Continuous during the term of the Agreement.

Nature of the processing: The Customer Data transferred will be Processed in accordance with this DPA and the Agreement and may be subject to the following processing activities:

- storage and other processing necessary to provide, maintain and improve the Services provided to Customer;

- to provide customer and technical support to Customer; and

- disclosures in accordance with the Agreement, as compelled by law.

Purpose(s) of the data transfer and further processing: For the purposes of: (i) providing the Services described in the Agreement, (ii) to prevent fraud and ensure the security of the Services, (iii) to perform any steps necessary for the performance of its obligations under the Agreement, (iv) as initiated by any Authorized User (as such term is defined in the Agreement) in its use of the Services, and (v) to comply with other reasonable and lawful instructions provided by Customer.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Within 60 calendar days of the date of cessation of any Services involving the Processing of Personal Data, unless retention is required by applicable law or regulations.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing: See details of **Schedule 3**. The subject matter of the Processing by such Subprocessors is described in Schedule 3 and above. The Processing is for the purposes described below and in **Schedule 3**, and for the duration of the Agreement, consistent and coterminous with the duration of Processing expected by Perforce under the Agreement, subject to the retention period criteria described above: Necessary for purposes of providing services under the contract with Customer, the information captured is the Customer employee's name, business email, job title, business address, and business phone numbers.

C. COMPETENT SUPERVISORY AUTHORITY

Competent Supervisory Authority (identify the competent supervisory authority/ies in accordance with Clause 13 of the EEA Standard Contractual Clauses): The competent supervisory authority will be determined in accordance with Clause 13 (a) of the EEA Standard Contractual Clauses or as otherwise provided herein.

***For the purposes of the EU SCCs, this information constitutes the details of "Annex 1.C".*

SCHEDULE 2:

TECHNICAL AND ORGANISATIONAL MEASURES

Perforce will have in place technical, physical, and organizational security measures that minimally meet the requirements set forth in this Schedule 2.

1. The technical and organizational security measures applicable to Personal Data will provide the same or better data-security protections as the Processor applies to its own Personal Data and confidential information, but in no event may those protections be anything less than that required to comply with Data Protection Laws and company policies. The Processor's technical and organizational security measures will ensure the protection of Personal Data, Customer systems, and the Processor's systems from unauthorized use, alteration, access, or disclosure and will ensure overall confidentiality, integrity, and availability of Personal Data.

2. Without limiting any other obligations and requirements, Processor has implemented and will maintain a comprehensive, written information security program that materially conforms to the ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. One or more designated qualified individuals will be responsible for maintaining the Processor information security program. Processor will regularly review the information security program, at least annually and whenever there is a material change in practice, to identify and assess reasonably foreseeable internal and external risks to the privacy, security, and/or integrity of any electronic, paper, or other records containing Personal Data and to ensure that Processor 's information security program continues to comply with applicable Data Protection Laws.

3. Any Processing of Personal Data will take place on information processing systems for which commercially reasonable technical and organizational measures for protecting Personal Data have been implemented. Each Processor will maintain reasonable and appropriate technical, physical, and administrative measures to protect Personal Data under its possession or control against unauthorized or unlawful Processing or accidental loss, destruction, or damage in accordance with the applicable Data Protection Laws, considering the harm that might result from unauthorized or unlawful processing or accidental loss, destruction, or damage and the sensitivity of the Personal Data.

4. Each Processor will take reasonable steps to ensure the reliability of employees, temporary workers, contractors, and other personnel (collectively "**Personnel**") having access to Personal Data and will limit access to Personal Data to those Personnel who have a business need to have access to such Personal Data and have received reasonable training regarding Processor's policies and procedures on privacy and security, appropriate handling of Personal Data, and Data Protection Laws.

5. Appropriate due diligence will be conducted on each Subprocessor to ensure that each can provide the level of protection for Personal Data that is required by this DPA and applicable Data Protection Laws.

6. Each Processor will ensure that its Personnel, agents, Sub-processors, and any authorized third parties with access to Customer's (or the relevant Processor's) premises follow all applicable general, visitor, privacy and physical security policies and only access authorized areas. The access rights to facilities must be removed upon termination of employment, contract or

agreement, or adjusted upon change. Additionally, each Processor will take commercially reasonable steps to secure Personal Data, including confidential and private documents and media, during non-working hours (e.g., locked cabinets).

7. **Minimum Controls**. Without limiting any other obligations herein, Processor will implement the following security controls:

a) Train Personnel handling Personal Data at least annually on appropriate and relevant information security-related policies, procedures, and agreements, the importance of privacy, security, and data protection, and the need to comply with obligations to properly handle Personal Data.

b) Document policies, procedures, and processes to manage the security risks related to Processing of Personal Data and review and update them as needed but at least annually.

c) Identify and manage Personnel, devices, systems, facilities, and other assets ("**Assets**") that access, store, and Process Personal Data and those that are material to the provision of the Services to Customer under the Agreement.

d) Perform security risk assessments regularly to identify and assess reasonably foreseeable internal and external security risks. Such risk assessments must be aligned with an enterprise-wide risk assessment framework and be performed at least annually to determine the likelihood and impact of all identified risks, using qualitative and quantitative methods. Such risk assessments must consider all relevant risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).

e) Limit access to Assets to authorized users, collect and analyze access logs, and further review them as appropriate.

f) Restrict and securely manage remote access to Assets by Personnel and others with multi-factor authentication (*i.e.*, authentication through verification of at least two of the following types of authentication factors (i) knowledge factors, such as a password, (ii) possession factors, such as a token or text message on a mobile phone, or (iii) inherence factors, such as a biometric characteristic).

g) Identify Personal Data and related records and manage access to them to protect the confidentiality, integrity, and availability of such information.

h) Physically and logically separate Personal Data from the Personal Data of other Processor clients.

i) Manage and control physical access to Assets, including measures to prevent and detect unauthorized access to Assets (including facilities). Monitoring equipment should be in place to allow for the review of unauthorized activity.

j) Securely destroy electronic and paper records containing Personal Data in accordance with secure destruction policies and procedures.

k) Implement and manage appropriate technical security solutions to protect the confidentiality, integrity, and availability of Personal Data.

l) Install critical operating system and software security patches in a timely manner on all devices used to Process Personal Data, and promptly install security-related fixes identified by Processor's hardware or software vendors.

m) Install and configure anti-malware software to check for updates on at least a daily basis on all devices used to Process Personal Data.

n) Deploy data loss prevention software or other technical solutions to prevent unauthorized copying or downloading Personal Data to removable drives or devices and/or unauthorized uploading or transferring Personal Data to unauthorized locations or recipients.

o) Run internal and external network vulnerability scans at least monthly and after any change in the network configuration.

p) Perform maintenance and repair of information system components in a controlled and secure manner.

q) Monitor Processor’s network and Assets to detect vulnerabilities, threats, anomalous or unauthorized activity, and other potential cyber security events (collectively “**Events**”) in a timely manner.

r) Personal Data will not be stored on any portable or removable media.

s) Personal Data will not be stored or used in test or other non-production environments.

t) Maintain and execute incident response processes and procedures to ensure timely response to detected Events. Ensure the following activities take place according to such established processes and procedures:

  i) Investigate, understand, and categorize Events;

  ii) Perform activities to contain an Event, mitigate its effects and address any remaining threat or vulnerability;

  iii) Restore affected Assets and Personal Data, and take other appropriate mitigating actions;

  iv) Document response and recovery activities; and

  v) Routinely review and update policies and procedures to incorporate lessons learned and address potential threats and vulnerabilities.

u) Maintain a disaster recovery plan to ensure the continuation of Services under the Agreement and backup of Personal Data in the event of a material disruption or impact to data or Assets.

v) Coordinate restoration activities with the Customer where Personal Data has been impacted.

8. **Encryption and Infrastructure Protection**.

Personal Data, including Personal Data on portable devices and backup media, will be encrypted in transmission and at rest, using industry-standard cryptographic techniques and secure management of keys; and

a) Each Processor will use appropriate encryption in connection with any transfer, communication, remote access, or storage involving Personal Data, using best industry standards considering the nature and extent of the Personal Data. Contractor will only use remote access or wireless connectivity to Customer systems or other storage involving Personal Data where Customer consents in writing.

9. **System Authentication and Authorization**. Access to Personal Data will be granted solely on a "need to know" basis, based on individual roles and responsibilities, and will be subject to secure user authentication protocols, including controls around user IDs, other identifiers, passwords, biometrics, authentication token devices, active account log-in procedures, log records that record access attempts, and blocking after multiple unsuccessful log-in attempts. Processor will:

a) Implement a formal documented process to grant, modify, and remove access to systems containing Personal Data;

b) Formally review user access rights to systems containing Personal Data at least semi-annually;

c) Not permit access permissions that allow public groups (*e.g.*, global, world, everyone, etc.) to have read or write access to Personal Data;

d) Ensure there are no common or group system user IDs on systems where Personal Data is maintained (i.e., users must be uniquely identified);

e) Conduct revalidation of access rights to Personal Data at least annually;

f) Maintain electronic logs of Personnel accessing Personal Data depicting the details of the access and transactional changes made and provide such electronic logs to Customer for inspection upon reasonable request; and

g) Conduct background checks for Personnel with responsibilities for or access to Personal Data, if permissible under applicable law.

10. **Business Continuity.** Each Processor will ensure that it always has in place an appropriate business continuity and disaster recovery plan for its business (the "**Business Continuity Plan**") that will ensure the continued performance of its obligations under this DPA and operational resilience generally. In addition, each Processor will:

a) Develop and update the Business Continuity Plan from time to time, and in any event annually, in accordance with good industry practice, and the Processor will, upon request, deliver a copy of the current Business Continuity Plan to Customer.

b) If required by the Customer, explain how the procedures set out in the Business Continuity Plan will interface with any of Customer's business continuity and disaster recovery plans and procedures of Customer that are known to the Processor.

c) Test the Business Continuity Plan at least annually, or when significant organizational or environmental changes are made by Processor, and, upon request, report results to Customer.

d) Provide geographically resilient hosting.

e) Provide infrastructure service failover.

f) Report any disruption of business activities related to an emergency to Customer.

11. **Software Development.** For any Services or deliverable that includes software or computer coding, Processor will take all necessary precautions to ensure the software is free of viruses, time bombs, worms, Trojan horses, or other intentionally destructive, disabling, or harmful devices ("**Destructive Code**"). If Customer discovers any Destructive Code or other verifiable security vulnerability at any time during the term of the Agreement, Processor will promptly remediate it. Processor must:

a) Follow a documented secure software development process.

b) Use automated or manual source code analysis tools to detect and remediate security defects in code prior to production deployment. Static application security testing (SAST) and dynamic application system testing (DAST) of the application code should be performed.

c) Perform application penetration testing on any publicly facing systems that contain Personal Data used in the Services provided to Customer.

d) Conduct, at Processor's expense, regular industry-standard reviews of Processor's software for security flaws. Reviews will cover all aspects of the software delivered, including third-party components and libraries. At a minimum, the review will cover common software vulnerabilities. The review may include a combination of static analysis of the binary code, dynamic web application vulnerability scanning, and manual penetration testing.

e) Processor will track all security issues (including but not limited to specific vulnerability instances and a summary of open security issues) uncovered during the security review of Processor's software and make available a report of the same to Customer upon Customer's reasonable demand. Processor will appropriately protect information regarding security issues and associated documentation to help limit the likelihood that vulnerabilities in operational software are exposed. Processor will use all commercially reasonable efforts consistent with sound software development practices, considering the nature and severity of the risk, to remediate all security issues as quickly as possible.

SCHEDULE 3:

APPROVED SUB-PROCESSORS

Below is a list of current Perforce Subprocessors. Not all Subprocessors process Personal Data in every case. Perforce may update this list as Subprocessors are added or deleted and provide updated lists to Customer. Perforce will provide thirty (30) days' prior notice to Customer of any changes to the below list of approved Subprocessors. If Customer objects to Perforce's appointment of a Subprocessor on reasonable grounds relating to the protection of Customer Data, then Perforce shall have the right to cure the objection through one of the following options (at Perforce's reasonable election) within sixty (60) days following Customer's objection: (a) Perforce will cease to use the new Subprocessor with regard to Customer Data; (b) Perforce will take the corrective steps requested by Customer in its objection and proceed to use the Subprocessor to Process Customer Data; or (c) Perforce may cease to provide, or Customer may agree not to use (temporarily or permanently), the particular aspect of a Service that would involve use of the Subprocessor to Process Customer Data.

Subprocessor Name	Address	Contact Person, Title, Contact Information	Description of Data Processing Activities
Salesforce.com, Inc.	Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, California 94105, USA	Lindsey Finch, DPO, privacy@salesforce.com	Hosting of customer relationship management software that includes the information about the Customer and its employees, including .
Atlassian Pty Ltd.	c/o Atlassian, Inc. 350 Bush Street, Floor 13 San Francisco, California 94104, USA	privacy@atlassian.com	Hosting of JIRA, JIRA Service Management, and Confluence tools
Amazon Web Services, Inc.	410 Terry Avenue, North Seattle, Washington 98109, USA	Attn: AWS Legal	Hosting of SAAS Services and infrastructure
Slack Technologies, LLC	50 Fremont Street San Francisco, California, 94105	privacy@slack.com	Workplace productivity tools

Microsoft Corporation	One Microsoft Way Redmond, Washington 98052	Microsoft Privacy Telephone: +1 (425) 882 8080	Microsoft Azure Cloud computing, storage, and related services
Google LLC	1600 Amphitheatre Parkway Mountain View, California 94043, USA	Google Privacy Telephone: +1 (650) 253 0000	Hosting of SAAS Services and infrastructure via Google Cloud Platform ("GCP")