Atlassian Data Processing Addendum

This Data Processing Addendum (the "**Addendum**") amends the terms and forms part of the Atlassian Cloud Terms of Service or other agreement governing your use of the applicable Atlassian Cloud Product(s) (the "**Agreement**") by and between you and the applicable Atlassian Entity from which you are purchasing the Cloud Products.

This Addendum will be effective as of the date we receive a complete and executed Addendum from the Customer indicated in the signature block below in accordance with the instructions under Sections I and II below (the "**Effective Date**"). This Addendum shall apply to Customer Personal Data that we process in the course of providing you the Cloud Products under the Agreement.

The scope and duration, as well as the extent and nature of the collection, processing and use of Customer Personal Data under this Addendum shall be as defined in the Agreement. The term of this Addendum corresponds to the duration of the Agreement.

I. INSTRUCTIONS

A. This Addendum has been pre-signed on behalf of the applicable Atlassian Entity. To enter into this Addendum, you must:

   i. be a customer of the Cloud Products;

   ii. complete the signature block below by signing and providing all items identified as "Required"; and

   iii. submit the completed and signed Addendum to Atlassian as instructed.

II. EFFECTIVENESS

A. This Addendum will only be effective (as of the Effective Date) if executed and submitted to Atlassian accurately and in full accordance with paragraph I above and this paragraph II. If you make any deletions or other revisions to this Addendum, then this Addendum will be null and void.

B. Customer signatory represents to Atlassian that he or she has the legal authority to bind Customer and is lawfully able to enter into contracts (e.g., is not a minor).

C. This Addendum will terminate automatically upon termination of the Agreement or as earlier terminated pursuant to the terms of this Addendum.

III. DATA PROCESSING TERMS

1. Definitions:

1.1 The terms below shall have the following meanings:

"Atlassian", "we", "us", "our" means the applicable Atlassian Entity that provides the relevant Cloud Product(s), as designated in the Agreement.

“Atlassian Entities”, “Atlassian Entity” means the Atlassian entities listed in Annex 3 (as may be updated from time to time).

“CCPA” means the California Consumer Privacy Act, as may be amended from time to time, and any rules or regulations implementing the foregoing.

“**Cloud Product(s)**” means our hosted or cloud-based solutions (currently designated as “Cloud” deployments) provided to you under the Agreement, including any client software we provide as part of the Cloud Products.

“**Controller**” means the entity which determines the purposes and means of the processing of Personal Data, including as applicable any "business' as defined under the CCPA.

“Customer”, “you”, “your” means the entity listed in the “Customer name” field on the signature block below.

"Customer Personal Data" means the personal data processed by Atlassian on your behalf in the course of providing the Cloud Products to you.

"**data processor**", "**data subject**", "**personal data**", "**processing**" and "**appropriate technical and organisational measures”** as used in this Addendum shall have the meanings given in the GDPR irrespective of whether GDPR or U.S. Data Protection Law applies.

"**Data Protection Law**" means the GDPR and the applicable U.S. Data Protection Law that are applicable to the processing of Customer Personal Data under this Addendum.

“End Users” means an individual you permit or invite to use the Cloud Products. For the avoidance of doubt: (a) individuals invited by your End Users, (b) individuals under managed accounts, and (c) individuals interacting with a Cloud Product as your customer are also considered End Users.

“**GDPR**” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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).

“**U.S. Data Protection Law**” means data protection or privacy laws applicable to Customer Personal Data in force within the United States, including the CCPA.

“**Processor**” means the entity which Processes Customer Personal Data on behalf of the Controller, including as applicable any “service provider” as defined by the CCPA.

2. **Scope of Data Protection Law**. The parties acknowledge that GDPR will apply to the processing of Customer Personal Data if, for example, the processing is carried out in the context of the activities of an establishment of Customers in the territory of the EU. The parties further agree that U.S. Data Protection Laws, including the CCPA, may also apply to the processing of Customer Personal Data. Unless expressly stated in this Addendum, this Addendum will apply irrespective of whether GDPR or U.S. Data Protection Law applies to the processing of Customer Personal Data.

3. Processing of Personal Data

3.1 The provisions of this Section 3 shall apply where Data Protection Law applies to your processing of Customer Personal Data and where we process that Customer Personal Data as a data processor in the course of providing you the Cloud Products. If U.S. Data Protection Law applies to either party's processing of Customer Personal Data, the relevant party will comply with any obligations applicable to it under that law with respect to the processing of that Customer Personal Data.

3.2 The subject-matter of the data processing is providing the Cloud Products and the processing will be carried out until we cease to provide any Cloud Products to you. Annex 1 of this Addendum sets out the nature and purpose of the processing, the types of Customer Personal Data we process and the data subjects whose Customer Personal Data is processed.

3.3 When we process Customer Personal Data in the course of providing Cloud Products to you, we will:

3.3.1 process the Customer Personal Data only in accordance with documented instructions from you (as set forth in this Addendum or the Agreement or as directed by you through the Cloud Products). If applicable law requires us to process the Customer Personal Data for any other purpose, we will inform you of this requirement first, unless such law(s) prohibit this on important grounds of public interest;

3.3.2 notify you promptly if, in our opinion, an instruction for the processing of Customer Personal Data given by you infringes applicable Data Protection Law;

3.3.3 assist you, taking into account the nature of the processing:

(i) by appropriate technical and organizational measures and where possible, in fulfilling your obligations to respond to requests from data subjects exercising their rights;

(ii) in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the information available to us; and

(iii) by making available to you all information reasonably requested by you for the purpose of demonstrating that your obligations relating to the appointment of processors as set out in Article 28 of the GDPR have been met.

3.3.4 not give access to or transfer any Customer Personal Data to any third party for such third party's independent use (e.g., not directly related to providing the Cloud Products) without your prior written consent. You consent to our appointment of the Atlassian affiliates and applicable third party subprocessors listed at https://www.atlassian.com/legal/sub-processors for the purposes described in this Addendum. We may update the list of approved subprocessors, at which point you will have the opportunity to object within forty-five (45) days by terminating the Agreement for convenience. To receive notice of updates to the list of subprocessors please subscribe at the link

provided above. When engaging subprocessors in the processing of Customer Personal Data, we are responsible for the performance of each subprocessor. We will include in our agreement with any such third party subprocessor terms which are at least as favourable to you as those contained herein and as are required by applicable Data Protection Law.;

3.3.5 ensure that our personnel required to access the Customer Personal Data are subject to a binding duty of confidentiality with regard to such Customer Personal Data;

3.3.6 except as set forth in Section 3.3.5 above or in accordance with documented instructions from you (as set forth in this Addendum or the Agreement or as directed by you through the Cloud Products), ensure that none of our personnel publish, disclose or divulge any Customer Personal Data to any third party;

3.3.7 upon your written request following the expiration or earlier termination of the Agreement securely return to you such Customer Personal Data, and unless prohibited under applicable law delete such Customer Data in our possession in compliance with procedures and retention periods outlined in our Cloud Product specific terms or Trust Center;

3.3.8 on the condition that you have entered into an applicable non-disclosure agreement with us:

(i) allow you and your authorized representatives to access and review up-to-date attestations, certifications, reports or extracts thereof from independent bodies (e.g., external auditors, internal audit, data protection auditors) or other suitable certifications to ensure compliance with the terms of this Addendum; or

(ii) where required by Data Protection Law or the Standard Contractual Clauses (where the GDPR is applicable) contained in Annex 4 (and in accordance with this Section 3.3.8), allow you and authorized representatives to conduct audits (including inspections) during the term of the Agreement to ensure compliance with the terms of this Addendum. Notwithstanding the foregoing, any audit must be conducted during our regular business hours, with reasonable advance notice to us and subject to reasonable confidentiality procedures. The scope of any audit shall not require us to disclose to you or your authorized representatives, or to allow you or your authorized representatives to access:

a. any data or information of any other Atlassian customer;

b. any Atlassian internal accounting or financial information;

c. any Atlassian trade secret;

d. any information that, in our reasonable opinion could: 1) compromise the security of our systems or premises; or 2) cause us to breach our obligations under Data Protection Law or our security, confidentiality

and or privacy obligations to any other Atlassian customer or any third party; or

e. any information that you or your authorized representatives seek to access for any reason other than the good faith fulfilment of your obligations under the Data Protection Law and our compliance with the terms of this Addendum.

(iii) In addition, audits shall be limited to once per year, unless 1) we have experienced a Security Breach within the prior twelve (12) months which has impacted your Customer Personal Data; or 2) an audit reveals a material noncompliance. If we decline or are unable to follow your instructions regarding audits permitted under this Section 3.3.10 (or the Standard Contractual Clauses, where applicable), you are entitled to terminate this Addendum and the Agreement for convenience.

4. Processing of Customer Personal Data Subject to U.S. Data Protection Law. The parties agree that this section 4 shall apply only to Customer Personal Data that is protected by U.S. Data Protection Law. In addition to the processing requirements set out in Section 3 above, where we process Customer Data Under U.S. Data Protection Law, we shall not retain, use, sell or otherwise disclose Customer Personal Data other than as required by law or as needed to provide the Cloud Products to you. For purposes of this section 4, the term "sell" shall have the meanings given in the CCPA irrespective of whether CCPA or GDPR applies.

5. **Security**.

5.1 We shall implement and maintain appropriate technical and organizational measures to protect the Customer Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure in accordance with Annex 2. These measures shall be appropriate to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of Customer Personal Data and appropriate to the nature of the Customer Personal Data which is to be protected. We may amend the technical and organizational measures, provided that the new measures do not fall short of the level of security provided by the specified measures

5.2 If we become aware of and confirm any accidental, unauthorized or unlawful destruction, loss, alteration, or disclosure of, or access to your Customer Personal Data that we process in the course of providing the Cloud Products (a "**Security Breach**"), we will notify you without undue delay.

6. **Data Transfers.** The parties agree that this section 6 shall apply only to Customer Personal Data that is protected by GDPR and such Customer Personal Data is transferred outside the European Economic Area (EEA) to Atlassian, either directly or via onward transfer.

6.1 **EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.** Atlassian, Inc., Trello, Inc., Dogwood Labs, Inc., and their U.S. affiliates self-certify to and comply with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks ("**Privacy Shield**"). Where the transfer of Customer Personal Data is made to a Privacy Shield-certified entity, we agree to process Customer Personal Data covered by Privacy Shield in accordance with the Privacy Shield

Principles. We agree to maintain our Privacy Shield certification throughout the term of the Agreement, provided Privacy Shield certification remains a valid basis under the GDPR for establishing adequate protections in respect of a relevant transfer of Customer Personal Data. We will promptly notify you if we cease to maintain, or anticipate the revocation or withdrawal of, or are otherwise challenged by any regulatory authority as to the status of our Privacy Shield certification, or if we make a determination that we can no longer meet our obligations under Privacy Shield.

6.2 **European Commission Standard Contractual Clauses (2010/87/EU).** The terms of the Standard Contractual Clauses outlined in Annex 4 will apply where the applicable transfer of Customer Personal Data is (a) not subject to the laws of a jurisdiction recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR); or (b) not covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. In the event of any conflict or inconsistency between the provisions of this Addendum and the Standard Contractual Clauses outlined in Annex 4, the provisions of the Standard Contractual Clauses shall prevail. In the event that any provision of the Standard Contractual Clauses is held illegal or unenforceable in a judicial proceeding, such provision shall be severed and shall be inoperative, and the remainder of the Standard Contractual Clauses and the terms of this Addendum shall remain operative and binding on the parties.

7. **Miscellaneous**.

7.1 Customer acknowledges and agrees that as part of providing the Cloud Products and services, Atlassian has the right to use data relating to or obtained in connection with the operation, support or use of the Cloud Products for its legitimate internal business purposes, such as to support billing processes, to administer the Cloud Products, to improve, benchmark, and develop our products and services, to comply with applicable laws (including law enforcement requests), to ensure the security of our Cloud Products and to prevent fraud or mitigate risk. To the extent any such data is personal data, Atlassian warrants and agrees that: (i) it will process such personal data in compliance with Data Protection Law and only for the purposes that are compatible with those described in this Section 7.1; (ii) it will not use Customer Personal Data for any other purpose or disclose it externally unless it has first aggregated and anonymised the data so that it does not identify the Customer or any other person or entity. Atlassian further agrees that it shall be a Controller and solely responsible and liable for any of its processing of personal data pursuant to this Section 7.1.

7.2 Through use of the Cloud Products, as further described in the Agreement, you or your End Users, as applicable, may elect to grant third parties visibility to your data or content (which may include Customer Personal Data). You also understand that user profile information for the Cloud Products may be publicly visible. Nothing in this Addendum prohibits (and, for the avoidance of doubt, Sections 3.3.5 and 3.3.7 above do not apply to) Atlassian making visible your data or content (which may include Customer Personal Data) to third parties consistent with this paragraph, as directed by you or your End Users through the Cloud Products.

7.3 In the event of any conflict or inconsistency between the provisions of the Agreement and this Addendum, the provisions of this Addendum shall prevail. This Addendum is subject to the governing law and venue terms in the Agreement, except as otherwise provided in

Annex 4 to the extent Annex 4 applies. For avoidance of doubt and to the extent allowed by applicable law, any and all liability under this Addendum (including its Annexes) will be governed by the limitations of liability and other relevant provisions of the Agreement. Without limiting the foregoing, any liability arising under this Addendum shall be subject to the limitations of liability under the Agreement as if such liability arose under the Agreement or the applicable order, and any liability of a party, its affiliates, their signatories or their suppliers arising under this Addendum will be aggregated with any other applicable liability arising under the Agreement for purposes of applying any applicable liability caps. Save as specifically modified and amended in this Addendum, all of the terms, provisions and requirements contained in the Agreement shall remain in full force and effect and govern this Addendum. Except as otherwise expressly provided herein, no supplement, modification, or amendment of this Addendum will be binding, unless executed in writing by a duly authorized representative of each party to this Addendum. If any provision of the Addendum is held illegal or unenforceable in a judicial proceeding, such provision shall be severed and shall be inoperative, and the remainder of this Addendum shall remain operative and binding on the parties.

Please sign and return the enclosed copy of this Addendum as instructed to acknowledge the supplementation of these terms to the Agreement.

CUSTOMER

Customer name (Required): _____

Signature (Required): _____

Name (Required): _____

Title (Optional): _____

Date (Required): _____

EU Representative (Required only where applicable): _____

Contact details: _____

Data Protection Officer (Required only where applicable): _____

Contact details: _____

ATLASSIAN

Notwithstanding the signatures below of any other Atlassian Entity, an Atlassian Entity is not a party to this Addendum unless they are a party to the Agreement for the provision of the Cloud Products to you. Where

the Cloud Products are provided under an Agreement with Atlassian Pty Ltd, Atlassian, Inc. is also a party to this Addendum.

Data Protection Point of Contact: Kelly Gertridge
Contact details: dataprotection@atlassian.com

Atlassian PTY Ltd.	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: December 24, 2019
Atlassian, Inc.	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: December 24, 2019
Trello Inc.	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: December 24, 2019
Dogwood Labs, Inc. **(dba Statuspage.io)**	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: December 24, 2019
OpsGenie, Inc.	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: December 24, 2019
Agile Craft LLC	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: December 24, 2019

Annex 1

Data subjects

The personal data concern End Users of the Cloud Products, in addition to individuals whose personal data is supplied by End Users of the Cloud Products.

Categories of data

The personal data transferred concern the following categories of data:

- Direct identifying information (e.g., name, email address, telephone).
- Indirect identifying information (e.g., job title, gender, date of birth).
- Device identification data and traffic data (e.g., IP addresses, MAC addresses, web logs).
- Any personal data supplied by users of the Cloud Product.

Special categories of data

Atlassian does not knowingly collect (and Customer or End Users shall not submit or upload) any special categories of data (as defined under the Data Protection Legislation).

Purposes of processing

The personal data is processed for the purposes of providing the Cloud Products in accordance with the Agreement.

Annex 2

Security Measures

1. Access control to premises and facilities

Measures must be taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures shall include:

- Access control system
- ID reader, magnetic card, chip card
- (Issue of) keys
- Door locking (electric door openers etc.)
- Surveillance facilities
- Alarm system, video/CCTV monitor
- Logging of facility exits/entries

2. Access control to systems

Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, forced change of password)
- No access for guest users or anonymous accounts
- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators

3. Access control to data

Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorized input, reading, copying, removal modification or disclosure of data. These measures shall include:

- Differentiated access rights
- Access rights defined according to duties
- Automated log of user access via IT systems

- Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment

4. Disclosure control

Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures shall include:

- Compulsory use of a wholly-owned private network for all data transfers
- Encryption using a VPN for remote access, transport and communication of data.
- Creating an audit trail of all data transfers

5. Input control

Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained.

Measures should include:

- Logging user activities on IT systems
- That it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment
- That it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data have been input;

6. Job control

Measures should be put in place to ensure that data is processed strictly in compliance with the data importer's instructions. These measures must include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

7. Availability control

Measures should be put in place designed to ensure that data are protected against accidental destruction or loss.

These measures must include:

- Installed systems may, in the case of interruption, be restored
- Systems are functioning, and that faults are reported

- Stored personal data cannot be corrupted by means of a malfunctioning of the system
- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage
- Anti-virus/firewall systems

8. Segregation control

Measures should be put in place to allow data collected for different purposes to be processed separately.

These measures should include:

- Restriction of access to data stored for different purposes according to staff duties.
- Segregation of business IT systems
- Segregation of IT testing and production environments

Annex 3

Atlassian Entities

- Atlassian Pty Ltd.
- Atlassian, Inc.
- Dogwood Labs, Inc.
- Trello, Inc.
- OpsGenie, Inc.
- Agile Craft LLC

Annex 4 – Standard Contractual Clauses

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to processor transfers)

Data Transfer Agreement

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Atlassian (hereinafter the "**data importer**")

and

Customer (hereinafter the "**data exporter**")

each a "**party**"; together "**the parties**",
HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Annex 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Annex 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their

implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Annex 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Annex 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional

qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Annex 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the

subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

Data exporter

Customer

Data importer

Atlassian

Data subjects

The personal data concern End Users of the Cloud Products, in addition to individuals whose personal data is supplied by End Users of the Cloud Products.

Categories of data

The personal data transferred concern the following categories of data:

- Direct identifying information (e.g., name, email address, telephone).
- Indirect identifying information (e.g., job title, gender, date of birth).
- Device identification data and traffic data (e.g., IP addresses, MAC addresses, web logs).
- Any personal data supplied by users of the Cloud Product.

Special categories of data

Atlassian does not knowingly collect (and Customer or End Users shall not submit or upload) any special categories of data (as defined under the Data Protection Legislation).

Purposes of processing

The personal data is processed for the purposes of providing the Cloud Products in accordance with this Agreement.

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

The technical and organizational security measures implemented by the data importer are as described in Annex 2 of the Data Processing Addendum.