Atlassian Data Processing Addendum

This Data Processing Addendum (the "**Addendum**") amends the terms of the Atlassian Customer Agreement (the "**Agreement**") by and between Atlassian Pty Ltd and you.

This Addendum will be effective as of the date Atlassian, Inc. ("**Atlassian**," "**we**," "**us**," or "**our**") receives a complete and executed Addendum from the Customer indicated in the signature block below ("**You**" "**your**") in accordance with the instructions under Sections I and II below. This Addendum shall apply to personal data that Atlassian processes in the course of providing you the Hosted Service under the Agreement.

Atlassian, Inc. is fulfilling data processing services on behalf of Atlassian Pty Ltd. The scope and duration, as well as the extent and nature of the collection, processing and use of 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 Atlassian. To enter into this Addendum, You must:

i. be a customer of the Hosted Services;

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

iii. submit the completed and signed Addendum to Atlassian via email at dpasubmission@atlassian.com.

II. EFFECTIVENESS

A. This Addendum will be effective only if it is executed and submitted to Atlassian accurately and in full in 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. If You have Affiliates with their own Atlassian accounts that need coverage under an Atlassian Data Processing Addendum with Atlassian, each such Affiliate must sign its own Atlassian Data Processing Addendum with Atlassian, in which case, the full legal entity name entered in the "Company Name" field associated with the Atlassian account will be the name of the applicable Affiliate.

B. Customer signatory represents to Atlassian that he or she has the legal authority to bind Customer and Affiliates 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.

Data Processing Terms

1. DEFINITIONS:

1.1 The terms below shall have the following meanings;

"**Customer Personal Data**" means the personal data processed by Atlassian on your behalf in the course of providing Hosted Service to you, other than Atlassian Business Contact Data;

"**Atlassian Business Contact Data"** means personal data processed by Atlassian for billing purposes, to send information about our new products and services, to improve our products and services, to provide support, to comply with law (including law enforcement requests) and to ensure security of our services and to prevent fraud or mitigate risk;

"**Data Protection Legislation**" means European Directives 2002/58/EC, the General Data Protection Regulation and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including the General Data Protection Regulation);

"**data processor**", "**data subject**", "**personal data**", "**processing**" and "**appropriate technical and organisational measures**" (written herein as "appropriate technical and organizational measures") shall be interpreted in accordance with applicable Data Protection Legislation; and

"**Hosted Service**", "**Affiliate**" and **"Authorized Users"** shall have the meaning set forth in the Agreement (as applicable).

2. DATA PROTECTION

2.1 The provisions of this Section 2 shall apply where Data Protection Legislation applies to your processing of Customer Personal Data and where we process that Customer Personal Data in the course of providing you the Hosted Service. We are the data processor in relation to Customer Personal Data.

2.2 The subject-matter of the data processing is providing the Hosted Service and the processing will be carried out until we cease to provide any Hosted Service 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.

2.3 When we process Customer Personal Data in the course of providing Hosted Service to you, we will:

2.3.1 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 Service). 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;

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

2.3.3 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 General Data Protection Regulation, 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 General Data Protection Regulation have been met.

2.3.4 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. Substantial changes must be documented;

2.3.5 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 Hosted Service) without your prior written consent. You consent to our appointment of the 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 by terminating the Agreement for convenience. To receive notice of updates to the list of subprocessors please subscribe at https://www.atlassian.com/legal/sub-processors. When engaging subprocessors in the processing of Customer Personal Data, we are responsible for the conduct and 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 Legislation;

2.3.6 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;

2.3.7 except as set forth in Section 2.3.5 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 Service), ensure that none of our personnel publish, disclose or divulge any Customer Personal Data to any third party;

2.3.8 upon expiration or earlier termination of the Agreement, upon your written request, securely destroy or return to you such Customer Personal Data, and destroy existing copies unless applicable laws require storage of such Customer Personal Data; and

2.3.9 on the condition that you and Atlassian have entered into an applicable non-disclosure agreement:

(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 Legislation and in accordance with this Section 2.3.9, allow you and authorized representatives to conduct audits or 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 Legislation 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 Legislation and our compliance with the terms of this Addendum.

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 or inspections under this subsection 2.3.9, you are entitled to terminate this Addendum and the Agreement for convenience.

2.4 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 Hosted Service (a "**Security Breach**"), we will notify you without undue delay.

2.5 All Customer Personal Data processing is covered by our Privacy Shield certification. We agree to maintain our Privacy Shield certification throughout the term of the Agreement, provided Privacy Shield certification remains a valid basis under the Data Protection Legislation for establishing adequate protections in respect of a transfer of Customer Personal Data outside of the European Economic Area. In the event that we cease to maintain our Privacy Shield certification or if Privacy Shield certification is no longer a valid basis to transfer personal data under Data Protection Legislation, we agree to execute additional terms as required by Data Protection Legislation, including but not limited to the European Commission Standard Contractual Clauses for Data Processors (2010/87/EU). We will promptly notify you if we cease to maintain, or anticipate the revocation or withdrawal, 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.

2.6 Through use of the Hosted Service, as further described in the Agreement, you 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 Hosted Service may be publicly visible. Nothing in this Addendum prohibits (and, for the avoidance of doubt, Sections 2.3.5 and 2.3.7 above do not apply to) Atlassian's making visible your data or content (which may include Customer Personal Data) to third parties consistent with this paragraph, as directed by you through the Hosted Service.

3. MISCELLANEOUS

3.1 Where you use multiple of our Hosted Service, you acknowledge that we may combine information from your use of the Hosted Service to deliver integrated services across the suite of Hosted Service that you have purchased (for example to allow you to search across our Hosted Service or to combine notifications from multiple Hosted Service). You also acknowledge that we may process information generated by your users for research and analytical purposes, in order to improve, benchmark and develop our Hosted Service. We will ensure that the results of this processing do not identify you or any of your users and that all such processing is subject to appropriate technical and organizational measures.

3.2 In the event of any conflict or inconsistency between the provisions of the Agreement and this Addendum, the provisions of this Addendum shall prevail. For avoidance of doubt and to the extent allowed by applicable law, any and all liability under this Addendum will be governed by the relevant provisions of the Agreement, including limitations of liability, venue and jurisdiction. 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 to acknowledge the supplementation of these terms to the Agreement.

Customer (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

Signature: 

Name: Erika Fisher Title: Head of Privacy

Date: June 6, 2018

Data Protection Point of Contact: Erika Fisher

Contact details: dataprotection@atlassian.com

Annex 1

Data subjects

The personal data concern Authorized Users of the Hosted Service as defined in the Agreement.

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 Hosted Service.

Special categories of data

Atlassian does not knowingly collect (and Customer shall not submit) any special categories of data (as defined under the Data Protection Legislation) and our Product terms do not permit customers or end-users of the Hosted Service to upload any such special categories of data.

Purposes of processing

The personal data is processed for the purposes of providing the Hosted Service in accordance with this 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
- Ensure 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
- Ensure 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 to ensure that data are protected against accidental destruction or loss.

These measures must include:

- Ensuring that installed systems may, in the case of interruption, be restored
- Ensure systems are functioning, and that faults are reported
- Ensure 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 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