Atlassian Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of the Agreement (defined below) by and between the customer (or its Affiliate(s), as applicable) as identified in the Agreement ("**Customer**") and Atlassian and will be effective on the later of (i) the effective date of the Agreement; or (ii) the date both parties execute this DPA in accordance with Section 1 below ("**Effective Date**"). All capitalized terms not defined in this DPA have the meanings set forth in the Agreement.

1. Instructions and Effectiveness

1.1. This DPA has been pre-signed on behalf of Atlassian. To enter into this DPA, Customer must:

(a) have a valid Agreement in place for the provision of Services;

(b) complete the signature block below by signing and providing all relevant information; and

(c) submit the completed and signed DPA to Atlassian.

1.2. This DPA will only be effective (as of the Effective Date) if executed and submitted to Atlassian accurately and in full accordance with Section 1. Where Customer makes any deletions or other revisions to this DPA, this DPA will be null and void.

1.3. Customer signatory represents to Atlassian that he or she has the legal authority to bind Customer and is lawfully able to enter into this DPA.

2. Data Protection

2.1. ***Definitions***: In this DPA, the following terms have the following meanings:

(a) "**Australian Data Protection Law**" means the Australian Privacy Act 1988 (Cth).

(b) "**Agreement**" means the agreement in place between Customer and Atlassian covering Customer's use of the Services.

(c) "**Applicable Data Protection Law**" means all data protection laws and regulations applicable to the processing of personal data under this DPA, including, but not limited to, the Australian Data Protection Law, Brazilian Data Protection Law, European Data Protection Law, Japanese Data Protection Law, and U.S. Data Protection Law.

(d) "**Brazilian Data Protection Law**" means the Brazilian General Data Protection Law No. 13,709/2018 ("**LGPD**").

(e) "**controller**", "**processor**", "**data subject**", "**personal data**", "**personal information**", "**processing"** (and "**process**"), "**commercial purpose**", and "**service provider**" have the meanings given in Applicable Data Protection Law, as appropriate.

(f) "**Customer Personal Data**" means any personal data provided by (or on behalf of) Customer to Atlassian in connection with the Services, all as further described in Exhibit A, Annex 1(B), Part A of this DPA.

(g) "**Deidentified Data**" means data that cannot reasonably be used to infer information about, or otherwise be linked to, a data subject.

(h) "**End Users**" or "**Users**" means an individual the Customer permits or invites to use the Cloud Products. For the avoidance of doubt: (a) individuals invited by End Users, (b) individuals under managed accounts, and (c) individuals interacting with a Cloud Product as Customer`s customers are also considered End Users.

(i) "**Europe**" means, for the purposes of this DPA, the Member States of the European Economic Area ("**EEA**"), the United Kingdom ("**UK**") and Switzerland.

(j) "**European Data Protection Law**" means: (i) 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) ("**EU GDPR**"); (ii) in respect of the United Kingdom the Data Protection Act 2018 and the EU GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK Data Protection Law**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) the Swiss Federal Act on Data Protection and its implementing regulations ("**Swiss FADP**"), in each case as may be amended, superseded or replaced from time to time.

(k) **"Japanese Data Protection Law**" means the Japanese Act on the Protection of Personal Information.

(l) "**Restricted Transfer**" means a transfer (directly or via onward transfer) of personal data subject to European Data Protection Law from Europe to a country outside of Europe that is not subject to an adequacy decision by the European Commission, or the competent UK or Swiss authorities (as applicable).

(m) "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data processed by Atlassian and/or its Sub-processors in connection with the provision of the Services. For the avoidance of doubt, "**Security Incident**" does not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

(n) "**Services**" means the provision of the products and services by Atlassian to Customer pursuant to the Agreement.

(o) "**special categories of personal data**" or "**sensitive data**" means any Customer Personal Data (i) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (ii) that is genetic data, biometric data processed for the purposes of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, and (iii) relating to criminal convictions and offences.

(p) "**Standard Contractual Clauses**" or "**EU SCCs**" means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

(q) "**Sub-processor**" means any other processor engaged by Atlassian in its role as a processor to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA where such entity processes Customer Personal Data. Sub-processors may include Atlassian's affiliates or other third parties.

(r) "**UK Addendum**" means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioner's Office under S119(A) of the UK Data Protection Act 2018, as may be amended, superseded, or replaced from time to time.

(s) "**U.S. Data Protection Law**" means all state laws in effect in the United States of America that are applicable to the processing of personal data under this DPA, including, but not limited to, the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("**CCPA**"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.

2.2. ***Relationship of the parties***: Where Applicable Data Protection Law provides for the roles of "controller," "processor," and "sub-processor":

(a) Where Atlassian processes Customer Personal Data on behalf of Customer in connection with the Services, Atlassian will process such personal data as a processor or Sub-processor on behalf of Customer (who, in turn, processes such personal data as a controller or a processor) and this DPA will apply accordingly. A description of such processing is set out in Exhibit A, Annex 1(B), Part A.

(b) Where Atlassian processes personal data as a controller, as further detailed in Exhibit A, Annex 1(B), Part B, Atlassian will process such personal data in compliance with Applicable Data Protection Law and only for the purposes that are compatible with those described in Exhibit A, Annex 1(B), Part B. For these purposes, only Sections 2.3 and 2.6 of this DPA will apply, to the extent applicable.

2.3. ***Description of Processing***: A description of the processing of personal data related to the Services, as applicable, is set out in Exhibit A. Atlassian may update the descriptions of processing from time to time to reflect new products, features or functionality comprised within the Services. Atlassian will update relevant documentation to reflect such changes. The Customer can subscribe to receive notifications regarding such updates using this link: https://www.atlassian.com/legal/data-processing-addendum.

2.4. ***Customer Processing of Personal Data***: Customer agrees that (i) it will comply with its obligations under Applicable Data Protection Law in its processing of Customer Personal Data and any processing instructions it issues to Atlassian, and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under Applicable Data Protection Law for Atlassian to process personal data (including but not limited to any special categories of personal data) and provide the Services pursuant to the Agreement (including this DPA).

2.5. ***Atlassian Processing of Personal Data:***

(a) When Atlassian processes Customer Personal Data in its capacity as a processor on behalf of the Customer, Atlassian will (I) comply with Applicable Data Protection Law, and (ii) process the Customer Personal Data as necessary to perform its obligations under the Agreement, and only in accordance with the documented lawful instructions of Customer (as set forth in the Agreement, in this DPA, or as directed by the Customer or Customer's End Users through the Services), unless required to do so by the applicable Laws to which Atlassian is subject. In this case Atlassian shall inform the Customer of such legal requirement before processing, unless relevant Laws prohibit such information on important grounds of public interest. Atlassian will promptly inform Customer if it becomes aware that Customer's processing instructions infringe Applicable Data Protection Law.

(b) To the extent Customer Personal Data includes personal information protected under the CCPA that Atlassian processes as a service provider acting on behalf of Customer, Atlassian will process such Customer Personal Data in accordance with the CCPA, including by complying with applicable sections of the CCPA and providing the same level of privacy protection as required by CCPA, and in accordance with Customer's written instructions, as necessary for the limited and specified purposes identified in Exhibit A, Annex 1(b), Part A of this DPA, the Agreement, and/or any related Order. Atlassian will not:

i. retain, use, disclose or otherwise process such Customer Personal Data other than for the limited and specified purposes identified in this DPA, the Agreement, and/or any related Order;

ii. retain, use, disclose or otherwise process such Customer Personal Data for a commercial purpose other than for the limited and specified purposes identified in this DPA, the Agreement, and/or any related Order, or as otherwise permitted under the CCPA;

iii. "sell" or "share" such Customer Personal Data within the meaning of the CCPA; and

iv. retain, use, disclose or otherwise process such Customer Personal Data outside the direct business relationship with Customer and not combine such Customer Personal Data with personal information that it receives from other sources, except as permitted under the CCPA.

Atlassian must inform Customer if it determines that it can no longer meet its obligations under U.S. Data Protection Laws within the timeframe specified by such laws, in which case Customer may take reasonable and appropriate steps to prevent, stop, or remediate any unauthorized processing of such Customer Personal Data.

(c) To the extent Customer discloses or otherwise makes available Deidentified Data to Atlassian or to the extent Atlassian creates Deidentified Data from Customer Personal Data, in each case in its capacity as a service provider, Atlassian will:

i. adopt reasonable measures to prevent such Deidentified Data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

ii. publicly commit to maintain and use such Deidentified Data in a deidentified form and to not attempt to re-identify the Deidentified Data, except that Atlassian may attempt to re-identify such data solely for the purpose of determining whether its deidentification processes are compliant with the U.S. Data Protection Law; and

iii. before sharing Deidentified Data with any other party, including Sub-processors, contractors, or any other persons ("**Recipients**"), contractually obligate any such Recipients to comply with all requirements of this Section 2.5(c) of the DPA (including imposing this requirement on any further Recipients).

(d) Atlassian participates in and certifies compliance with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and Swiss-U.S. Data Privacy Framework (together, the "**Data Privacy Framework**"). As required by the Data Privacy Framework, Atlassian will (i) provide at least the same level of privacy protection as is required by the Data Privacy Framework Principles; (ii) notify Customer if Atlassian makes a determination it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Framework Principles, and (iii) upon notice, including under Section 2.5(d)(ii), take reasonable and appropriate steps to remediate unauthorized processing.

2.6. ***Restricted transfers**:* Parties agree that when the transfer of personal data from Customer (as "**data exporter**") to Atlassian (as "**data importer**") is a Restricted Transfer and Applicable Data Protection Law requires that appropriate safeguards are put in place, the transfer will be subject to the Standard Contractual Clauses, which are deemed incorporated into and form a part of this DPA, as follows:

(a) In relation to transfers of Customer Personal Data governed by the EU GDPR and processed in accordance with Section 2.2(a) of this DPA, the EU SCCs will apply, completed as follows:

i. Module Two or Module Three will apply (as applicable);

ii. in Clause 7, the optional docking clause will not apply;

iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes will be as set out in Section 2.10 of this DPA;

iv. in Clause 11, the optional language will not apply;

v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

vi. in Clause 18(b), disputes will be resolved before the courts of Ireland;

vii. Annex I of the EU SCCs is deemed completed with the information set out in Exhibit A to this DPA, as applicable; and

viii. Subject to Section 2.8 of this DPA, Annex II of the EU SCCs is deemed completed with the information set out in Exhibit B to this DPA;

(b) In relation to transfers of personal data governed by the EU GDPR and processed in accordance with Section 2.2(b) of this DPA, the EU SCCs apply, completed as follows:

i. Module One will apply;

ii. in Clause 7, the optional docking clause will not apply;

iii. in Clause 11, the optional language will not apply;

iv. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

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

vi. Annex I of the EU SCCs is deemed completed with the information set out in Exhibit A to this DPA, as applicable; and

vii. Subject to Section 2.8 of this DPA, Annex II of the EU SCCs is deemed completed with the information set out in Exhibit B to this DPA;

(c) In relation to transfers of personal data governed by UK Data Protection Law, the EU SCCs: (i) apply as completed in accordance with paragraphs (a) and (b) above; and (ii) are deemed amended as specified by the UK Addendum, which is deemed executed by the parties and incorporated into and forming an integral part of this DPA. In addition, Tables 1 to 3 in Part 1 of the UK Addendum is deemed completed respectively with the information set out in Section 2.9, as well as Exhibits A and B of this DPA; Table 4 in Part 1 is deemed completed by selecting "neither party." Any conflict between the terms of the EU SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

(d) In relation to transfers of personal data governed by the Swiss FADP, the EU SCCs will also apply in accordance with paragraphs (a) and (b) above, with the following modifications:

i. any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FADP, and references to specific Articles of "Regulation (EU) 2016/679" will be replaced with the equivalent article or section of the Swiss FADP;

ii. references to "EU", "Union", "Member State" and "Member State law" will be interpreted as references to Switzerland and Swiss law, as the case may be, and will not be interpreted in such a way as to exclude data subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs;

iii. Clause 13 of the EU SCCs and Part C of Annex 1 are modified to provide that the Federal Data Protection and Information Commissioner ("**FDPIC**") of Switzerland will have authority over data transfers governed by the Swiss FADP. Subject to the foregoing, all other requirements of Clause 13 will be observed;

iv. references to the "competent supervisory authority" and "competent courts" will be interpreted as references to the FDPIC and competent courts in Switzerland;

v. in Clause 17, the EU SCCs will be governed by the laws of Switzerland; and

vi. Clause 18(b) states that disputes will be resolved before the applicable courts of Switzerland.

(e) It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA), the Standard Contractual Clauses prevail to the extent of such conflict.

2.7. ***Confidentiality of processing**:* Atlassian must ensure that any person that it authorizes to process Customer Personal Data (including Atlassian's staff, agents and Sub-processors) will be subject to a duty of confidentiality (whether a contractual duty or a statutory duty), and must not permit any person to process Customer Personal Data who is not under such a duty of confidentiality.

2.8. ***Security****:* Atlassian and, to the extent required under the Agreement, Customer must implement appropriate technical and organizational measures in accordance with Applicable Data Protection Law (e.g., Art. 32 GDPR) to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data. Atlassian's current technical and organizational measures are described in Exhibit B ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that Atlassian may update or modify the Security Measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Services.

2.9. ***Sub-processing****:* Customer consents to Atlassian engaging Sub-processors to process Customer Personal Data, provided that Atlassian maintains an up-to-date list of its sub-processors at https://www.atlassian.com/legal/sub-processors, which contains a mechanism for Customer to subscribe to notifications of new Sub-processors. Atlassian will: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Personal Data to the standard required by Applicable Data Protection Law (and in substance, to the same standard provided by this DPA); and (ii) remain liable to Customer if such Sub-processor fails to fulfill its data protection obligations with regard to the relevant processing activities under the Agreement.

2.10. ***Changes to Sub-processors****:* If Customer subscribes to Sub-processor notifications, Atlassian will provide a notice to Customer of any new Sub-processors as soon as reasonably practicable, however at least fourteen (14) days' prior to allowing such Sub-processor to process Customer Personal Data (the "**Notice Period**"). Customer may object in writing to Atlassian's appointment of a new Sub-processor during the Notice Period, provided that such objection is based on reasonable grounds relating to data protection. In such an event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties are not able to achieve resolution within the Notice Period, Customer, as its sole and exclusive remedy, may terminate the applicable Order(s) or parts of the Service provided by the Sub-processor in question for convenience. If the Customer does not object during the Notice Period, Atlassian will deem Customer to have authorized the new Sub-processor.

2.11. ***Cooperation obligations*** **and** ***data subjects' rights****:*

(a) Taking into account the nature of the processing, Atlassian must provide reasonable and timely assistance to Customer to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, to rectification, to erasure, to restriction, to objection, and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party, in each case in respect of Customer Personal Data that Atlassian processes on Customer's behalf;

(b) In the event that any request, correspondence, enquiry or complaint (referred to under paragraph (a) above) is made directly to Atlassian, Atlassian acting as a processor will not respond to such communication directly without Customer's prior authorization, unless legally required to do so, and instead, after being notified by Atlassian, Customer may respond. If Atlassian is legally required to respond to such a request, Atlassian will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so; and

(c) To the extent Atlassian is required under Applicable Data Protection Law, Atlassian will provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities, taking into account the nature of processing and the information available to Atlassian.

2.12. ***Security incidents****:* Upon becoming aware of a Security Incident, Atlassian will notify Customer without undue delay and provide timely information (taking into account the nature of processing and the information available to Atlassian) relating to the Security Incident as it becomes known or as is reasonably requested by Customer to allow Customer to fulfill its data breach reporting obligations under Applicable Data Protection Law. Atlassian will further take reasonable steps to contain, investigate, and mitigate the effects of the Security Incident. Atlassian's notification of or response to a Security Incident in accordance with this Section 2.12 will not be construed as an acknowledgment by Atlassian of any fault or liability with respect to the Security Incident.

2.13. ***Deletion or return of Data****:* After the end of the provision of Services, Atlassian will delete or return to Customer all Customer Personal Data (including copies) processed on behalf of the Customer in accordance with the procedures and retention periods outlined in the DPA, Product-Specific Terms or Trust Center. This requirement does not apply to the extent Atlassian is required by applicable Laws to retain some or all of the Customer Personal Data which Customer Personal Data Atlassian will securely isolate and protect from any further processing.

2.14. ***Audit:***

(a) Customer acknowledges that Atlassian is regularly audited by independent third-party auditors and/or internal auditors, including as may be described from time to time at https://www.atlassian.com/trust/compliance. Upon request, and on the condition that Customer has entered into an applicable non-disclosure agreement with Atlassian, Atlassian will:

i. supply (on a confidential basis) a summary copy of relevant audit report(s) ("**Report**") to Customer, so Customer can verify Atlassian's compliance with the audit standards against which it has been assessed, and this DPA; and

ii. provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its Processing of Customer Personal Data that are necessary to confirm Atlassian's compliance with this DPA, provided that Customer cannot exercise this right more than once per calendar year.

(b) Only to the extent Customer cannot reasonably satisfy Atlassian's compliance with this DPA through the exercise of its rights under Section 2.14(a) above, or where required by Applicable Data Protection Law or a regulatory authority, Customer, or its authorized representatives, may conduct audits (including inspections) during the term of the Agreement to assess Atlassian's compliance with the terms of this DPA. Any audit must (i) be conducted during Atlassian's regular business hours, with reasonable advance notice of at least 45 calendar days; (ii) be subject to reasonable confidentiality controls; (iii) occur no more than once annually; (iv) restrict its findings to only data and information relevant to Customer; and (v) obligate Customer, to the extent permitted by law or regulation, to keep confidential any information disclosed that, by its nature, should be confidential.

2.15. ***Law enforcement***: If a law enforcement agency sends Atlassian a demand for Customer Personal Data (e.g., a subpoena or court order), Atlassian will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Atlassian may provide Customer's contact information to the law enforcement agency. If compelled to disclose Customer Personal Data to a law enforcement agency, then Atlassian will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy, to the extent Atlassian is legally permitted to do so.

3. Relationship with the Agreement

3.1. The parties agree that this DPA replaces and supersedes any existing DPA the parties may have previously entered into in connection with the Services.

3.2. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. The order of precedence in case of any conflict, exclusively in relation to the processing of personal data under this DPA, will be, in order of priority:

(a) Standard Contractual Clauses, if applicable;

(b) this DPA;

(c) the Agreement.

3.3. Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party's affiliates under this DPA is subject to the exclusions and limitations of liability set out in the Agreement.

3.4. Any claims against Atlassian or its affiliates under this DPA can only be brought by the Customer entity that is a party to the Agreement against the Atlassian entity that is a party to the Agreement. In no event will this DPA or any party restrict or limit the rights of any data subject or of any competent supervisory authority.

3.5. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law.

3.6. This DPA and the Standard Contractual Clauses will terminate simultaneously and automatically upon deletion by Atlassian of the Customer Personal Data processed on behalf of the Customer, in accordance with Section 2.13 of this DPA.

Customer Signatures

CUSTOMER	Customer name (Required): ____________________ Address: ____________________ 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 Signatures

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.

Data Protection Point of Contact: Kelly Gertridge

Contact Details: dataprotection@atlassian.com

Atlassian Entity	Atlassian Cloud Products	Signature
Atlassian PTY Ltd.	Jira Software Jira Service Management Jira Work Management Confluence Bitbucket Atlassian Access Atlassian Cloud Apps	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: 07/30/2023
Trello Inc.	Trello Trello Power-Ups	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: 07/30/2023
Dogwood Labs, Inc. (dba Statuspage.io)	Statuspage	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: 07/30/2023

OpsGenie, Inc.	Opsgenie	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: 07/30/2023

Agile Craft LLC	Jira Align	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: 07/30/2023

EXHIBIT A
Description of the Processing Activities / Transfer

Annex 1(A) List of Parties:

Data Exporter	Data Importer
Name: Customer	**Name**: Atlassian
Address / Email Address: As provided for in the DPA	**Address / Email Address**: As provided for in the DPA
Contact Person's Name, position, and contact details: As provided for in the DPA	**Contact Person's Name, position, and contact details**: As provided for in the DPA
Activities relevant to the transfer: See Annex 1(B) below	**Activities relevant to the transfer**: See Annex 1(B) below
Role: See Annex 1(B)	**Role**: See Annex 1(B)

ATLASSIAN

Annex 1(B) Description of processing and transfer (as applicable)

The parties acknowledge that Atlassian's processing of personal data will include all personal data submitted or uploaded to the Services by Customer from time to time, for the purposes of, or otherwise in connection with, Atlassian providing the Services to Customer.

Set out below are descriptions of the processing and transfers of personal data as contemplated as of the date of this DPA. Such descriptions are subject to change or may be supplemented pursuant to Section 2.3 of the DPA.

Part A: Description of processing and transfer (as applicable) for Modules 2 and 3 of the Standard Contractual Clauses (reference to Sections 2.2(a) as well as 2.6(a) DPA)

Atlassian cloud account profile (Identity)	
Categories of data subjects	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Cloud Product on behalf of the Customer.
Categories of personal data transferred	*User Account Information, for example:* • Atlassian identifier associated with user account • About Me • Avatar Image and URL • Full name • Email address • Time zone *Employment Information, for example:* • Job title / role • Office / location • Company/organization
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	The nature of the processing (incl. transfer) is described in the Agreement and respective Orders for relevant Cloud Product, especially referring to its technical capabilities and various features, including but not limited to collection, structuring, storage, transmission, or otherwise making available Customer Personal Data by automated means and in accordance with Cloud Product functionalities.
Purpose of the data transfer	The purpose of data processing (incl. transfer) is the provision and enablement of the use of the Cloud Product in accordance with the Agreement and respective Orders, in particular: • Hosting, transmission, storage and display of Customer Personal Data. • Hosting of End-User profiles as well as the company profile. • Enabling the use of various features and functionalities, as described in the Documentation.
Duration of processing	Data will be deleted 15 days (for evaluation sites) or 60 days (for paid subscription sites) after Customer has been unsubscribed due to missed payment for an Atlassian product subscription or if Customer cancels their Atlassian product subscription. For more information see https://support.atlassian.com/security-and-access-policies/docs/track-storage-and-move-data-across-products/

Jira Software Cloud, Confluence Cloud, Jira Product Discovery, Atlas, Atlassian Intelligence	
Categories of data subjects	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Cloud Products on behalf of the Customer.
Categories of personal data transferred	*User Account Information, for example:* • Atlassian identifier associated with user account • About Me • Avatar Image and URL • Full name • Email address • Time zone *Employment Information, for example:* • Job title / role • Office / location • Company/organization *Personal data included in user generated content.*
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	The nature of the processing (incl. transfer) is described in the Agreement and respective Orders for the relevant Cloud Products, especially referring to their technical capabilities and various features of, including but not limited to collection, structuring, storage, transmission, or otherwise making available Customer Personal Data by automated means and in accordance with functionalities.
Purpose of the data transfer	The purpose of data processing (incl. transfer) is the provision and enablement of the use of relevant Cloud Product in accordance with the Agreement and respective Orders, in particular: • Hosting, transmission, storage and display of Customer Personal Data. • Hosting of End-User profiles as well as the company profile. • Enabling the use of various features and functionalities, as described in the Documentation.
Duration of processing	Upon termination, Customer accounts are deactivated within 15 days (for monthly subscriptions) and 17 days (for annual subscriptions) after the end of the Customer’s current subscription period. Atlassian retains data for deactivated products for 15 days (for evaluation licenses) or 60 days (for Free, Standard, and Premium product plans) after the end of the Customer’s current subscription period. Upon deletion, an archive of the data is kept for an additional 30 days.

Jira Service Management (JSM) / Jira Work Management (JWM) **(Also see section for OpsGenie, which is integrated into JSM)**	
Categories of data subjects	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Cloud Products on behalf of the Customer.
Categories of personal data transferred	*User Account Information, for example:* • Atlassian identifier associated with user account • About Me • Avatar Image and URL • Full name • Email address • Time zone *Personal Identification, for example:* • IP address • Language setting • Location/ Region/ City • Phone numbers • Screen name/ Handle/ Nickname *Employment Information, for example*: • Job title / role • Office / location • Company/organization *Personal data included in user generated content*
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	The nature of the processing (incl. transfer) is described in the Agreement and respective Orders for relevant Cloud Product, especially referring to their technical capabilities and various features, including but not limited to collection, structuring, storage, transmission, or otherwise making available Customer Personal Data by automated means and in accordance with Cloud Product functionalities.
Purpose of the data transfer	The purpose of data processing (incl. transfer) is the provision and enablement of the use of Cloud Products in accordance with the Agreement and respective Orders, in particular: • Hosting, transmission, storage and display of Customer Personal Data. • Hosting of End-User profiles as well as the company profile. • Enabling the use of various features and functionalities, as described in the Documentation.
Duration of processing	Upon termination of service, Customer accounts are deactivated within 15 days (for monthly subscriptions) and 17 days (for annual subscriptions) after the end of the Customer's current subscription period. Atlassian retains data for deactivated products for 15 days (for evaluation licenses) or 60 days (for Free, Standard, and Premium product plans) after the end of the Customer's current subscription period. Upon deletion, an archive of the data is kept for an additional 30 days.

Bitbucket Cloud	
Categories of data subjects	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Cloud Product on behalf of the Customer.
Categories of personal data transferred	*User Account Information, for example:* • Atlassian identifier associated with user account • About Me • Avatar Image and URL • Full name • Email address • Time zone • Bitbucket ID *Personal Identification, for example:* • IP address • Language setting • Location/ Region/ City • Phone numbers • Screen name/ Handle/ Nickname *Employment Information, for example:* • Job title / role • Office / location • Company/Organization *Personal data included in user generated content*
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	The nature of the processing (incl. transfer) is described in the Agreement and respective Orders for the relevant Cloud Product, especially referring to its technical capabilities and various features, including but not limited to collection, structuring, storage, transmission, or otherwise making available Customer Personal Data by automated means and in accordance with Cloud Product functionalities.
Purpose of the data transfer	The purpose of data processing (incl. transfer) is the provision and enablement of the use of Cloud Product in accordance with the Agreement and respective Orders, in particular: • Hosting, transmission, storage and display of Customer Personal Data. • Hosting of End-User profiles as well as the company profile. • Enabling the use of various features and functionalities, as described in the Documentation.
Duration of processing	On termination of a Bitbucket Cloud account, and at the request of the Customer, customer data will be removed from the live production database. The team's data will remain in encrypted Bitbucket Cloud database backups until those backups fall out of the 35-day backup retention window and are destroyed in accordance with Bitbucket Cloud's data retention policy. In the event a database restore is necessary within 35 days of a requested data deletion, the Bitbucket Cloud operations team will re-delete the data as soon as reasonably possible after the live production system is fully restored.

Trello	
Categories of data subjects	Customer, Customers’ employees, Customers’ collaborators, as well as all relevant End Users of the Cloud Product on behalf of the Customer.’’
Categories of personal data transferred	*User Account Information, for example:* • Atlassian identifier associated with user account • About Me • Avatar Image and URL • Full Name • Email address • Time zone *Personal Identification, for example:* • IP address • Cookie information • Language setting • Location/ Region/ City • Phone numbers • Screen name/ Handle/ Nickname *Employment Information, for example:* • Job title / role • Office / location • Company/organization *Personal data included in user generated content*
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	The nature of the processing (incl. transfer) is described in the Agreement and respective Orders for the relevant Cloud Product, especially referring to its technical capabilities and various features, including but not limited to collection, structuring, storage, transmission, or otherwise making available Customer Personal Data by automated means and in accordance with Cloud Product functionalities.
Purpose of the data transfer	The purpose of data processing (incl. transfer) is the provision and enablement of the use of Cloud Product in accordance with the Agreement and respective Orders, in particular: • Hosting, transmission, storage and display of Customer Personal Data. • Hosting of End-User profiles as well as the company profile. • Enabling the use of various features and functionalities, as described in the Documentation.
Duration of processing	On termination of a Trello enterprise contract, and at the request of the Customer, the data belonging to the enterprise teams will be completely removed from the live production database and all file attachments uploaded directly to Trello will be removed within 30 days. The team’s data will remain in encrypted Trello database backups until those backups fall out of the 90-day backup retention window and are destroyed in accordance with Trello’s data retention policy. In the event a database restore is necessary within 90 days of a requested data deletion, the Trello operations team will re-delete the data as soon as reasonably possible after the live production system is fully restored.

Opsgenie	
Categories of data subjects	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Cloud Product on behalf of the Customer.
Categories of personal data transferred	*User Account Information, for example:* • Atlassian identifier associated with user account • About Me • Avatar Image and URL • Full Name • Email address • Time zone *Personal Identification, for example:* • IP address • Cookie information • Language setting • Location/ Region/ City • Phone numbers • Screen name/ Handle/ Nickname *Employment Information, for example:* • Job title / role • Office / location • Company/organization *Personal data included in user generated content*
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	The nature of the processing (incl. transfer) is described in the Agreement and respective Orders for the relevant Cloud Products, especially referring to its technical capabilities and various features, including but not limited to collection, structuring, storage, transmission, or otherwise making available Customer Personal Data by automated means and in accordance with Cloud Product functionalities.
Purpose of the data transfer	The purpose of data processing (incl. transfer) is the provision and enablement of the use of the Cloud Product in accordance with the Agreement and respective Orders, in particular: • Hosting, transmission, storage and display of Customer Personal Data. • Hosting of End-User profiles as well as the company profile. • Enabling the use of various features and functionalities, as described in the Documentation.
Duration of processing	When a configuration item, user, or alert, incident is deleted from Opsgenie, the entity and child data will be deleted by Opsgenie. When a user is deleted from Opsgenie, Audit Logs (Alert Log - Incident Timeline) will still have audit records like "Email notification sent to x@y.com", this is important as part of Incident audit. Customers can delete Alerts & Incident, Alert logs & Incident Timeline will be deleted. Customer Logs visible on the Logs page are immutable, and have a retention of 1 year. Customers can delete data from web applications manually or automatically by using Opsgenie rest api. When paid subscription ends, Customers may contact Atlassian Customer Support so that all data of Customers can be deleted. Legal & Security Auditing reasons: Customer Logs, Data Backup & System Log Archives will be stored as an archive for 1 year, regardless of whether Customer data is fully deleted or not. Archives can not be accessed directly by Customers, access is restricted to Opsgenie authorized employees.

Statuspage	
Categories of data subjects	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Cloud Product on behalf of the Customer.
Categories of personal data transferred	*User Account Information, for example:* • Atlassian identifier associated with user account • About Me • Avatar Image and URL • Full name • Email address • Time zone • Phone number • Company/Organization *Personal data included in user generated content* *Browsing information within Admin settings*
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	The nature of the processing (incl. transfer) is described in the Agreement and respective Orders for the relevant Cloud Product, especially referring to its technical capabilities and various features, including but not limited to collection, structuring, storage, transmission, or otherwise making available Customer Personal Data by automated means and in accordance with Cloud Product functionalities.
Purpose of the data transfer	The purpose of data processing (incl. transfer) is the provision and enablement of the use of Cloud Product in accordance with the Agreement and respective Orders, in particular: • Hosting, transmission, storage and display of Customer Personal Data. • Hosting of End-User profiles as well as the company profile. • Enabling the use of various features and functionalities, as described in the Documentation.
Duration of processing	On termination of a Statuspage account, and at the request of the Customer, customer data will be removed from the live production database. The customer data will remain in encrypted Statuspage database backups until those backups fall out of the 30-day backup retention window and are destroyed in accordance with Atlassian's data retention policy. In the event that a database restore is necessary within 30 days of a requested data deletion, the Statuspage operations team will re-delete the data as soon as reasonably possible after the live production system is fully restored.

Jira Align	
Categories of data subjects	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Cloud Product on behalf of the Customer.
Categories of personal data transferred	*User Account Information, for example:* • Jira Align ID • Avatar Image and URL • Full name • Email address • Time zone *Personal Identification, for example:* • Screen name/ Handle/ Nickname • Language setting • Location/ Region/ City Employment Information, *for example*: • Job Title/ Role *Browsing information on Admin settings* *Personal data included in user generated content*
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	The nature of the processing (incl. transfer) is described in the Agreement and respective Orders for the relevant Cloud Product, especially referring to its technical capabilities and various features, including but not limited to collection, structuring, storage, transmission, or otherwise making available Customer Personal Data by automated means and in accordance with Cloud Product functionalities.
Purpose of the data transfer	The purpose of data processing (incl. transfer) is the provision and enablement of the use of Cloud Products in accordance with the Agreement and respective Orders, in particular: • Hosting, transmission, storage and display of Customer Personal Data. • Hosting of End-User profiles as well as the company profile. • Enabling the use of various features and functionalities, as described in the Documentation.
Duration of processing	On termination of a Jira Align Enterprise contract, and at the request of the Customer, the database will be dropped from the live production database. This will be done within the support team service level agreement. The customer data will remain in encrypted Jira Align database backups until those backups fall out of the 35-day backup retention window and are destroyed in accordance with Atlassian's data retention policy. In the event a database restore is necessary within 35 days of a requested data deletion, the Jira Align operations team will re-delete the data as soon as reasonably possible after the live production system is fully restored.

Part B: Description of processing and transfer (as applicable) for Module 1 of the Standard Contractual Clauses (reference to Sections 2.2(b) as well as 2.6(b) DPA)

All Cloud Products: Atlassian as a controller	
Categories of data subjects	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Services on behalf of the Customer.
Categories of personal data transferred	**Personal data relating to or obtained in connection with the operation, support or use of the Services, e.g.:** *User Account Information,* for example pseudonymous Atlassian IDs, Cloud IDs, Site IDs,Tenant ID, Segment Anonymous IDs *Payment and billing information, to the extent it includes personal data* *Device and connection information, for example:* • IP address • Cookie information • Device information • Browser information *Information on the use of the Services, for example:* • Event Name (i.e., what action the user performed) • Event Timestamp • Page URL • Referring URL *Support data** Personal data provided through various Atlasian support channels, including for example Atlassian ID, SEN (Support Entitlement Number), username, contact information and any personal data contained within a summary of the problem experienced or information needed to resolve the support case. * *If any user generated content is submitted as attachments via support tickets, Atlassian acts as a processor of such personal data and Sections 2.2(a)as well as 2.6(a) DPA apply accordingly*.
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Collection, storage, and processing of relevant personal data for the purposes identified in this Part B.
Purpose of the data transfer	Personal data will be processed for Atlassian's legitimate business purposes. This entails in particular the following: • To facilitate security, fraud prevention, performance monitoring, business continuity and disaster recovery in order to protect Customers, End Users and Atlassian. • To engage and to provide support and assistance to Customer and End Users as requested from time to time. • To comply with legal and financial reporting obligations • To administer the Services, including to calculate usage-based billing • To derive insights in order to maintain, develop, and improve the Services and support, including for research and development purposes • To derive insights in order to inform internal business analysis and product strategy.
Duration of processing	Atlassian may process personal data for the purposes described above for the duration of the DPA, and for as long as Atlassian has a legitimate need to retain the personal data for the purposes it was collected or transferred, in accordance with Applicable Data Protection Law.

Annex 1(C): Competent supervisory authority

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

EXHIBIT B
Technical and Organizational Security Measures

1. Purpose.

This Exhibit describes Atlassian's security program, security certifications, and physical, technical, organizational and administrative controls and measures to protect Customer Data from unauthorized access, destruction, use, modification or disclosure (the "**Security Measures**"). The Security Measures are intended to be in line with the commonly-accepted standards of similarly-situated software-as-a-service providers (**"industry standard"**). Unless otherwise specified in the applicable Product-Specific Terms, the Security Measures apply to all Atlassian Cloud Products (other than No-Charge Products or Free and Beta Products) that are available under the Agreement.

2. Updates and Modifications.

The Security Measures are subject to technical progress and development and Atlassian may update or modify the Security Measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Cloud Products, as described in this document.

3. Definitions.

Any capitalized terms used but not defined in this document have the meanings set out in the Agreement. The term "**Customer Data**" means any data, content or materials provided to Atlassian by or at the direction of Customer or its End Users via the Cloud Products, including from Third-Party Products.

4. Security Measures.

The Security Measures are described in the following table:

Measure	**Description**
Measures of pseudonymisation and encryption of data	**<u>Encryption</u>** Atlassian has and will maintain: (i) an established method to encrypt Customer Data in transit and at rest; (ii) an established method to securely store passwords following industry standard practices; and (iii) use established key management methods. Any Customer Data is encrypted in transit over public networks using TLS 1.2 or greater, with Perfect Forward Secrecy (PFS) to protect it from unauthorized disclosure or modification. Data drives on servers holding Customer Data and attachments use full disk, industry-standard, AES-256 encryption at rest. **<u>Pseudonymisation</u>** Atlassian has and will maintain: (i) an established method to create pseudonymised data sets using industry standard practices; and (ii) appropriate technical and organisational measures governing the systems capable of remapping pseudonymous identifiers.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	**<u>Security Program</u>** Atlassian will maintain a security management program that includes but is not limited to: a) executive review, support and accountability for all security related policies and practices; b) a written information security policy and framework that meets or exceeds industry standards and that, as a baseline, includes (i) defined information security roles and responsibilities, (ii) a formal and effective risk mitigation program and (iii) a service provider security management program; c) periodic risk assessments of all Atlassian owned or leased systems processing Customer Data; d) prompt review of security incidents affecting the security of Atlassian systems processing Customer Data, including determination of root cause and corrective action; e) a formal controls framework based on, among other things, formal audit standards such as the AICPA SOC 2 Type II report, ISO27001, and NIST 800-53 (or any successor standard); f) processes to document non-compliance with the security measures;

Measure	Description
	g) processes to identify and quantify security risks, develop mitigation plans, which must be approved by Atlassian's Chief Trust Officer (or one of their delegates), and track the implementation of such plans; and h) a comprehensive security testing methodology that consists of diverse and independent approaches that, when combined, are reasonably designed to maximize coverage for a varied and diverse set of attack vectors. Atlassian will periodically (and, in any event, no less frequently than annually) review, test and, where applicable, update such security management program. **<u>Security Incident Notification</u>** Atlassian will notify Customer of Security Incidents in accordance with the Atlassian Data Processing Addendum. **<u>Employee Screening, Training, Access and Controls</u>** Atlassian will maintain policies and practices that include the following controls and safeguards applied to Atlassian staff who have access to Customer Data and/or provide Support and Services to Customer: a) pre-hire background checks (including criminal record inquiries) on Atlassian job candidates, conducted by a third-party background check provider, subject to and in accordance with applicable Laws and generally accepted industry standards; b) periodic security awareness training; c) a disciplinary policy and process to be used when Atlassian staff violate Atlassian's security policies; d) access to Atlassian IT systems only from approved Atlassian-managed devices with appropriate technical security controls (including two-factor authentication); e) controls designed to limit access to Customer Data to only those Atlassian staff with an actual need-to-know such Customer Data. Such controls include the use of a formal access management process for the request, review, approval and provisioning for all Atlassian staff with access to Customer Data; and f) separation of duties to prevent a single Atlassian employee from controlling all key aspects of a critical transaction or business process related to Customer Data or systems.
Measures for ensuring the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident	During the Subscription Term, Atlassian's business continuity and disaster recovery plans (collectively, the "**BCDR Plans**") will address at least the following topics: a) the availability of human resources with appropriate skill sets; b) the availability of all IT infrastructure, telecommunications capabilities and any other technology used or relied upon by Atlassian in the provision of the Products; c) Atlassian's plans for storage and continuity of use of data and software; d) clear recovery time objectives (RTOs) and recovery point objectives (RPOs); e) mechanisms for the geographic diversity or back-up of business operations; f) the potential impact of cyber events and Atlassian's ability to maintain business continuity in light of such events, as well as a framework and procedure to respond to and remediate such events; g) the management of data corruption incidents; and h) procedures and frequency of testing of the BCDR Plans. Atlassian will periodically (and, in any event, no less frequently than annually) review, test and, where applicable, update the BCDR Plans.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	**<u>Compliance Program</u>** Atlassian will maintain a compliance program that includes independent third-party audits and certifications. Atlassian will make available to Customer, via the [Atlassian Compliance Site](), copies of the most up-to-date version of the following third-party certifications or reports in relation to the Cloud Products: (i) a SOC2 Type II report; (ii) an International Organization for Standardization (ISO) 27001 certificate (which includes adherence to ISO 27002 and 27018 standards) and, upon

Measure	Description
	written request, the relevant Statement of Applicability; or (iii) any successor of any of the foregoing. All such reports or certificates will be made available on the Atlassian Compliance Site, and will be made available within a commercially reasonable time of the relevant audit and/or certification process being completed. **Vulnerability Management** Atlassian will maintain the following vulnerability management processes: *Vulnerability Scanning and Remediation*. Atlassian employs processes and tools in line with industry standards to conduct frequent vulnerability scanning to test Atlassian's network and infrastructure and application vulnerability testing to test Atlassian applications and services. Atlassian applies security patches to software components in production and development environments as soon as commercially practicable in accordance with our Security Bug Fix Policy. *Identifying Malicious Threats*. Atlassian employs processes and tools in line with industry standards to identify malicious actors and prevent them from accessing Customer Data or Atlassian systems that process Customer Data. These include, but are not limited to, maintaining software that attempts to identify and detect attempted intrusions, behaviors consistent with Internet-based attacks, and indicators of potential compromise. Atlassian will maintain a security incident and event management system and supporting processes to notify appropriate personnel in response to threats. *Vulnerability Testing*. a) Atlassian conducts internal vulnerability testing, as described here. This includes our bug bounty program. We make the results of these internal tests publicly available and commit to making bug fixes in line with our Security Bug Fix Policy. b) Customer may, either itself or through an independent third party (who has entered into confidentiality obligations with Atlassian), perform its own vulnerability testing of its Cloud Products in accordance with the Security Test Rules. Customer may report any vulnerabilities impacting the Cloud Products to Atlassian in accordance with the procedures set forth in the Security Test Rules. c) Atlassian will use commercially reasonable efforts to address identified security vulnerabilities in our Cloud Products and our infrastructure in accordance with the Security Bug Fix Policy. The parties acknowledge that Atlassian may update the Security Bug Fix Policy from time to time in its discretion, provided such updates do not result in a material derogation of the Security Bug Fix Policy.
Measures for user identification and authorisation	Atlassian cloud users can authenticate using username and password, or external IdPs (incl. via SAML, Google, Microsoft and Apple). All credentials are hosted in the application database, which is encrypted at rest. Passwords are stored using a secure hash + salt algorithm. Administrators are able to configure and enforce password complexity requirements for managed accounts via Atlassian Access: https://support.atlassian.com/security-and-access-policies/docs/manage-your-password-policy/. Administrators are also able to enforce SSO via Atlassian Access.
Measures for the protection of data during transmission	See the item above titled "*Measures of pseudonymisation and encryption of data*"
Measures for the protection of data during storage	**Data Hosting Facilities** Atlassian will, no less frequently than annually, request assurances (e.g., in the form of an independent third party audit report and vendor security evaluations) from its data hosting providers that store or process Customer Data that: a) such data hosting provider's facilities are secured in an access-controlled location and protected from unauthorized access, damage, and interference; b) such data hosting provider's facilities employ physical security appropriate to the classification of the assets and information being managed; and

Measure	Description
	c) such data hosting provider's facilities limit and screen all entrants employing measures such as on-site security guard(s), badge reader(s), electronic lock(s), or a monitored closed caption television (CCTV). **Tenant Separation** Atlassian will use established measures to ensure that Customer Data is kept logically segregated from other customers' data when at-rest. **Data Encryption** See the item above titled "*Measures of pseudonymisation and encryption of data*"
Measures for ensuring physical security of locations at which data are processed	See the item above titled "*Measures for the protection of data during storage*".
Measures for ensuring events logging	Audit logging is available via API. See: https://support.atlassian.com/security-and-access-policies/docs/track-organization-activities-from-the-audit-log/
Measures for ensuring system configuration, including default configuration	See the item above titled "*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*".
Measures for internal IT and IT security governance and management	See the item above titled "*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*".
Measures for certification/assurance of processes and products	See the item above titled "*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*".
Measures for ensuring data minimisation	See "What information we collect about you" section of the Atlassian Privacy Policy.
Measures for ensuring data quality	See the items above titled "*Measures of pseudonymisation and encryption of data*", "*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*", and "*Measures for the protection of data during storage*". In addition, Customer and its Users have the ability to update any Customer Data provided to Atlassian using in-built product functionality, as further described in the Documentation.
Measures for ensuring limited data retention	**Data Retention and Destruction Standard** Atlassian maintains a Data Retention and Destruction Standard, which designates how long we need to maintain data of different types. The Data Retention and Destruction Standard is guided by the following principles: • Records should be maintained as long as they serve a business purpose. • Records that serve a business purpose, or which Atlassian has a legal, regulatory, contractual or other duty to retain, will be retained. • Records that no longer serve a business purpose, and for which Atlassian has no duty to retain, should be disposed. Copies or duplicates of such data should also be disposed. To the extent Atlassian has a duty to retain a specified number of copies of a Record, such number of copies should be retained. • Atlassian's practices implementing this Standard may vary across departments, systems and media, and will of necessity evolve over time. These practices will be reviewed under our company-wide policy review practices.

Measure	**Description**
Measures for ensuring accountability	See the item above titled "*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*".
Measures for allowing data portability and ensuring erasure	**Data Export** Atlassian allows Customer to export its Customer Data from the Cloud Products as described in the Documentation. **Secure Deletion** Atlassian will maintain a process reasonably designed to ensure secure destruction and deletion of any and all Customer Data as provided in the Agreement. Such Customer Data will be securely destroyed and deleted by Atlassian so that: (a) Customer Data cannot be practicably read or reconstructed, and (b) the Atlassian systems that store Customer Data are securely erased and/or decommissioned disks are destroyed. **Privacy Rights** See: • "Managing Individual privacy rights" on our Manage your business' data privacy page; and • "Privacy requests" on https://www.atlassian.com/hu/trust/privacy/personal-data-privacy.