ATLASSIAN

Forge Data Processing Addendum

This Data Processing Addendum, including the Standard Contractual Clauses and the Exhibits ("**DPA**"), is incorporated into and forms part of the Forge Terms, and is entered into by and between Developer and Atlassian (as these capitalized terms are defined below)**.** All capitalized terms not defined in this DPA have the meaning set forth in the Forge Terms or the Developer Terms, as applicable.

1. Data Protection

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

(a) "**Applicable Data Protection Law**" means U.S. Data Protection Law and European Data Protection Law that are applicable to the processing of Personal Data under this DPA.

(b) "**Atlassian**" means, for the purposes of this DPA, Atlassian Pty Ltd (ABN 53 102 443 916) and Atlassian US, Inc.

(c) "**controller**", "**processor**", "**data subject**", "**processing"** (and "**process**"), and "**supervisory authority**" have the meaning given to them in Applicable Data Protection Law.

(d) **"Developer"** has the meaning given to it in the Developer Terms.

(e) "**Developer Personal Data**" means Personal Data relating to Developer, Developer's employees or Developer's collaborators that Atlassian processes as a controller under this DPA, as further described in Annex 1(B), Part B of Exhibit A to this DPA.

(f) "**Developer Terms**" means the Atlassian Developer Terms.

(g) "**End Users**" means individuals interacting with the Forge Apps as Developer's customers. For the avoidance of doubt, individuals invited by End Users to use the Forge Apps are also considered End Users.

(h) **"End User Personal Data"** means Personal Data relating to End Users that Atlassian processes as a processor on behalf of Developer in connection with the Services, as further described in Annex 1(B), Part A of Exhibit A to this DPA. For certainty, End User Personal Data does not include Personal Data that Atlassian processes as a processor on behalf of Atlassian's customers.

(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 Data Protection Act and its implementing regulations ("**Swiss DPA**"); in each case as may be amended, superseded or replaced from time to time.

(k) "**Forge Apps**" has the meaning given to it in the Developer Terms.

(l) **"Forge Framework"** has the meaning given to it in the Developer Terms.

(m) **"Forge Terms"** means the Forge Terms.

(n) "**Personal Data**" means any data that is protected as "personal data", "personal information" or "personally identifiable information" under Applicable Data Protection Law.

(o) "**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced from time to time).

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

(q) "**Security Incident**" means any confirmed breach of security that leads to the accidental, or unlawful destruction, loss, alteration, unauthorized disclosure of or access to End User Personal 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 End User Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

(r) "**Services**" means the provision of the Forge Framework by Atlassian to Developer pursuant to the Developer Terms and the Forge Terms.

(s) "**Sensitive Data**" means any 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 and (iv) any other form of Personal Data that is afforded enhanced protection under Applicable Data Protection Law.

(t) "**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, as may be amended, superseded, or replaced from time to time.

(u) "**Sub-processor**" means any processor engaged by Atlassian to assist in fulfilling its obligations with respect to providing the Services pursuant to the Forge Terms, the Developer Terms or this DPA, where such entity processes End User Personal Data. Sub-processors may include Atlassian's affiliates or other third parties.

(v) "**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.

(w) "**U.S. Data Protection Law**" means those data protection or privacy laws and regulations within the United States, including the California Consumer Privacy Act (as amended by the California Privacy Rights Act or otherwise) (the "**CCPA**"), as applicable to Personal Data.

1.2. ***Relationship of the parties***: Where Applicable Data Protection Law provides for the roles of "controller" and "processor":

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

(b) Where Atlassian processes Developer Personal Data, Atlassian will process such Developer Personal Data as an independent controller, as further detailed in Annex 1(B), Part B of Exhibit A to this DPA. Atlassian will process the Developer Personal Data in compliance with Applicable Data Protection Law and only for the purposes that are compatible with those described in Annex 1(B), Part B of Exhibit A to this DPA. For these purposes, only Sections 1.3, 1.4, 1.6 and 1.8 of the body of this DPA will apply, to the extent applicable.

1.3. ***Description of Processing***: Atlassian may update the description 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.

1.4. ***Developer Responsibilities***: Developer is responsible for determining whether the Services are appropriate for the storage and processing of Personal Data under Applicable Data Protection Law. Developer agrees that (i) it will comply with its obligations under Applicable Data Protection Law in its use of the Services, the processing of Personal Data and any processing instructions it issues to Atlassian, (ii) it is responsible for the accuracy, quality and legality of Personal Data, (iv) 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 Sensitive Data) and provide the Services pursuant to the Forge Terms and the Developer Terms (including this DPA), and (v) it will notify Atlassian if it is unable to comply with its obligations under Applicable Data Protection Law or its processing instructions will cause Atlassian or its Sub-processors to be in breach of Applicable Data Protection Law.

1.5. ***Atlassian Processing of End User Personal Data:*** When Atlassian processes End User Personal Data in its capacity as a processor on behalf of the Developer, Atlassian will process the End User Personal Data as necessary to perform its obligations under the Forge Terms and the Developer Terms, and only in accordance with the documented lawful instructions of Developer (as set forth in the Forge Terms and the Developer Terms, in this DPA, or as directed by the Developer through the Forge Apps or the Forge Framework) (the "**Permitted Purpose"**). Atlassian will not retain, use, disclose or otherwise process the End User Personal Data for any purpose other than the Permitted Purpose except where otherwise required by law(s) to which Atlassian is subject, in which case Atlassian will inform the Developer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; and will not "sell" the End User Personal Data within the meaning of the CCPA or otherwise. Atlassian will promptly inform Developer if it becomes aware that Developer's processing instructions infringe Applicable Data Protection Law. To the extent Atlassian processes End User Personal Data that is subject to the CCPA, Atlassian will process such End User Personal Data in compliance with the CCPA as a "service provider" (as defined by the CCPA), including by providing no less than the level of privacy protection required by the CCPA.

1.6. ***Restricted transfers:*** The parties agree that when the transfer of Personal Data from Developer (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 Restricted 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 Restricted Transfers of End User Personal Data protected by the EU GDPR and processed in accordance with Section 1.2(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 1.8 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 Restricted Transfers of Developer Personal Data protected by the EU GDPR and processed in accordance with Section 1.2(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 1.8 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 Restricted Transfers of Personal Data protected by UK Data Protection Law, the EU SCCs: (i) apply as completed in accordance with paragraph (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 this DPA. In addition, Tables 1 to 3 in Part 1 of the UK Addendum are deemed completed respectively with the information set out in Section 1.9, as well as Exhibits A and B of this DPA; and 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 Restricted Transfers of Personal Data protected by the Swiss DPA, 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 DPA, and references to specific Articles of "Regulation (EU) 2016/679" will be replaced with the equivalent article or section of the Swiss DPA;

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 DPA. 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;

(f) Although Atlassian does not rely on the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks ("**Privacy Shield**") as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for so long as Atlassian US, Inc. and its covered entities are self-certified to the Privacy Shield, Atlassian will continue to process Personal Data in accordance with the Privacy Shield Principles. Atlassian will promptly notify Developer if it makes a determination that Atlassian can no longer meet its obligations under the Privacy Shield Principles; and

(g) If Atlassian adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield adopted pursuant to Applicable Data Protection Law) for the transfer of Personal Data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism will apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Applicable Data Protection Law and extends to the territories to which Personal Data is transferred).

1.7. ***Confidentiality of processing****:* Atlassian must ensure that any person that it authorizes to process End User 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).

1.8. ***Security****:* Atlassian and, to the extent required under the Forge Terms and the Developer Terms, Developer, must implement appropriate technical and organizational measures in accordance with Applicable Data Protection Law (including Art. 32 GDPR) to protect Personal Data from Security Incidents and to preserve the security and confidentiality of the Personal Data. Atlassian's current technical and organizational measures are described in Exhibit B to this DPA ("**Security Measures**"). Developer acknowledges that 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 degrade or diminish the overall security.

1.9. ***Sub-processing****:* Developer agrees that Atlassian may engage Sub-processors to process End User Personal Data on Atlassian's behalf. The Sub-processors currently engaged by Atlassian and authorized by Developer are listed at https://www.atlassian.com/legal/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 End User Personal Data to the standard provided by this DPA; and (ii) remain liable to Developer if such Sub-processor fails to fulfill its data protection obligations under that agreement. Furthermore, Atlassian must (i) make available an up-to-date

list of the Sub-processors it has appointed upon written request from Developer; and (ii) notify Developer if it adds or replaces any new Sub-processors at least fourteen (14) days' prior to allowing such Sub-processor to process End User Personal Data. Developer must subscribe to receive notice of updates to the list of Sub-processors, using the link above in this Section 1.9. Developer may object in writing to Atlassian's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such an event, the Developer, as its sole and exclusive remedy, may terminate the Forge Terms and the Developer Terms (including this DPA) for convenience.

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

(a) Taking into account the nature of the processing, Atlassian must provide reasonable and timely assistance to Developer (at Developer's expense) to enable Developer to respond to any request from a data subject to exercise any of its rights under Applicable Data Protection Law.

(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 Developer's prior authorization, unless legally required to do so, and instead, after being notified by Atlassian, Developer may respond. To the extent Atlassian is required under Applicable Data Protection Law, Atlassian will (at Developer's request and expense) provide reasonably requested information regarding the Services to enable the Developer 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.

1.11. ***Security incidents:*** Upon becoming aware of a Security Incident, Atlassian will inform Developer without undue delay and provide timely information (taking into account the nature of the processing and the information available to Atlassian) relating to the Security Incident as it becomes known or as is reasonably requested by Developer to allow Developer 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 1.11 will not be construed as an acknowledgment by Atlassian of any fault or liability with respect to the Security Incident.

1.12. ***Deletion or return of End User Personal Data:*** Upon written request from Developer, Atlassian will delete all End User Personal Data (including copies) processed on behalf of the Developer in compliance with the procedures and retention periods outlined in the DPA; this requirement does not apply to the extent Atlassian is required by applicable law to retain some or all of the End User Personal Data, or to End User Personal Data it has archived on back-up systems, which Atlassian will securely isolate and protect from any further processing, as further detailed in Exhibit A, Annex 1(B), Part A.

1.13. ***Audit:*** Developer 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 Developer has entered into an applicable non-disclosure agreement with Atlassian, Atlassian must:

i. supply (on a confidential basis) a summary copy of its audit report(s) ("**Report**") to Developer, so Developer 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 Developer related to its Processing of End User Personal Data, including responses to information security and audit questionnaires, that are necessary to confirm Atlassian's compliance with this DPA, provided that Developer cannot exercise this right more than once per calendar year.

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

2. Relationship with the Forge Terms and the Developer Terms

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

2.2. Developer's click-through acceptance of the Forge Terms or Developer's submission of the Forge Apps to the Atlassian Platform shall constitute a valid signature for the purposes of this DPA, including Annex 1(A) and the Standard Contractual Clauses.

2.3. Except for the changes made by this DPA, the Forge Terms and the Developer Terms remain unchanged and in full force and effect. If there is any conflict between this DPA and the Forge Terms and/or Developer Terms, this DPA will prevail to the extent of that conflict in connection with the processing of Personal Data governed under the DPA. If there is any conflict between the Standard Contractual Clauses and the Forge Terms and/or the Developer Terms (including this DPA), the Standard Contractual Clauses will prevail to the extent of that conflict in connection with the processing of Personal Data governed under the Standard Contractual Clauses.

2.4. Notwithstanding anything to the contrary in the Forge Terms and/or the Developer Terms, the liability of each party and each party's affiliates under this DPA is subject to any exclusions and limitations of liability set out in the Forge Terms and the Developer Terms.

2.5. Any claims against Atlassian under this DPA can only be brought by the Developer entity that is a party to the Developer Terms and the Forge Terms against Atlassian Pty Ltd (ABN 53 102 443 916) or Atlassian US, Inc. In no event will this DPA or any party restrict or limit the rights of any data subject.

2.6. This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Developer Terms unless required otherwise by Applicable Data Protection Law and the Standard Contractual Clauses.

2.7. This DPA will terminate simultaneously and automatically upon deletion by Atlassian of the End User Personal Data processed on behalf of the Developer, in accordance with Section 1.12 of this DPA.

ATLASSIAN

EXHIBIT A
Description of the Processing Activities / Transfer

Annex 1(A) List of Parties:

Data Exporter	**Data Importer**
Name: Developer	**Name**: Atlassian
Address / Email Address: As set out in the Developer's Atlassian cloud account.	**Address / Email Address**: dataprotection@atlassian.com
Contact Person's Name, position, and contact details: As set out in the Developer's Atlassian cloud account.	**Contact Person's Name, position, and contact details**: Kelly Gertridge, Head of Privacy dataprotection@atlassian.com
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) below	**Role**: See Annex 1(B) below

Developer's click-through acceptance of the Forge Terms or Developer's submission of the Forge Apps to the Atlassian Platform shall constitute a valid signature for the purposes of this Annex 1(A) and the Standard Contractual Clauses.

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

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 1.3 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 1.2(a) as well as 1.6(a) of the DPA)

End User Personal Data : Atlassian as a processor	
Categories of data subjects	End Users
Categories of personal data transferred	*User Account Information, for example*: ● Atlassian identifier associated with user account ● Time zone *Inferred location information, for example:* ● IP address Any other Personal Data relating to End Users, as provided to Atlassian via the Services by (or at the instruction of) Developer, that is stored in the Forge Apps.
Sensitive data transferred	None
Frequency of the transfer	Continuous
Nature of the processing	Providing the Services, including maintaining End User profiles and providing storage and compute capabilities.
Purpose of the data transfer and further processing	Providing the Services, including maintaining End User profiles and providing storage and compute capabilities.
Retention period (or, if not possible to determine, the criteria used to determine that period)	Atlassian will retain End User Personal Data for the duration of the Forge Terms and any period after the termination of or expiry of the Forge Terms during which Atlassian processes End User Personal Data.
For transfers to (sub-) processors: subject matter, nature and duration of the processing	Subject matter: As further specified at https://www.atlassian.com/legal/sub-processors. Nature: See above. Duration: In accordance with the data protection terms agreed to with Sub-processors in accordance with Section 1.9 of the DPA.

ATLASSIAN

Part B: Description of processing and transfer as per Sections 1.2(b) and 1.6(b) of the DPA.

Developer Personal Data: Atlassian as a controller	
Categories of data subjects	Developer, Developer's employees and Developer's collaborators
Categories of personal data transferred	*User account information, for example*: ● Atlassian identifier associated with user account ● Email address ● Atlassian account password ● Forge command line interface (CLI) login token
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Collection, storage, and processing of Developer Personal Data for the purposes identified in this Part B.
Purpose of the data transfer	Developer Personal Data will be processed for Atlassian's legitimate business purposes. This entails in particular the following: ● To administer the Services, including the Forge command line interface (CLI) and Developer console. ● To facilitate security, fraud prevention, performance monitoring, business continuity and disaster recovery in order to protect Developers, End Users, Atlassian and third parties (as applicable). ● To comply with legal and financial reporting obligations. ● 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.
Retention period (or, if not possible to determine, the criteria used to determine that period)	Atlassian will not retain Developer Personal Data for longer than the period for which Atlassian has a legitimate need to retain Developer 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 European Data Protection Law.

ATLASSIAN

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 Personal 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 Developer Guidelines, the Security Measures apply to the Forge Framework that is available to the Developer under the Forge Terms.

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 degrade or diminish the overall security of the Forge Framework, as described in this document.

3. Definitions.

Any capitalized terms used but not defined in this document have the meanings set out in the Forge Terms or the Developer Terms, as applicable.

4. Security Measures.

The Security Measures are described in the following table:

Measure	**Description**
Measures of pseudonymisation and encryption of personal data	**Data Encryption** Atlassian has and will maintain: (i) an established method to encrypt Personal 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 Personal 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 Personal Data and attachments use full disk, industry-standard, AES-256 encryption at rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	**Security Program** 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 Personal Data; d) prompt review of security incidents affecting the security of Atlassian systems processing Personal 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; 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. **Security Incident Notification** Atlassian will notify Developer of Security Incidents in accordance with the DPA.

Measure	**Description**
	Employee Screening, Training, Access and Controls Atlassian will maintain policies and practices that include the following controls and safeguards applied to Atlassian staff who have access to Personal Data and/or provide Services to Developer: a) pre-hire background checks (including criminal record inquiries) on Atlassian job candidates, which are conducted by a third-party background check provider 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 Personal Data to only those Atlassian staff with an actual need-to-know such Personal 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 Personal 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 Personal Data or systems. **Other matters** See the items below titled "Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident," and "Measures for the protection of data during storage".
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	**Resilience Program** 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 Forge Framework; c) Atlassian's plans for storage and continuity of use of data and software; d) 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; e) the management of data corruption incidents; and f) 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	**Compliance Program** Atlassian will maintain a compliance program that includes independent third-party audits and certifications. Atlassian will make available to Developer, 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 Forge Framework: (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 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.

Measure	**Description**
	Identifying Malicious Threats. Atlassian employs processes and tools in line with industry standards to identify malicious actors and prevent them from accessing Personal Data or Atlassian systems that process Personal 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) Atlassian will use commercially reasonable efforts to address identified security vulnerabilities in the Forge Framework 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 the protection of data during transmission	See the item above titled "*Measures of pseudonymisation and encryption of personal 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 Personal 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 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 Personal Data is kept logically segregated from other Developers' data when at-rest. **Data Encryption** See the item above titled "*Measures of pseudonymisation and encryption of personal data*"
Measures for ensuring physical security of locations at which personal data are processed	See the item above titled "*Measures for the protection of data during storage*".
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 personal data*", "*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*", and "*Measures for the protection of data during storage*".
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:

Measure	**Description**
	● 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.
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 ensuring erasure	**Secure Deletion** Atlassian will maintain a process reasonably designed to ensure secure destruction and deletion of any and all Personal Data as provided in the Agreement. Such Personal Data will be securely destroyed and deleted by Atlassian so that: (a) Personal Data cannot be practicably read or reconstructed, and (b) the Atlassian systems that store Personal 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.