DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is entered into between TNG Technology Consulting GmbH, Beta-Straße 13a, 85774 Unterföhring, Germany ("TNG" or “Processor”) and Customer as identified in this DPA ("Customer" or “Controller”) and will be effective the date both parties execute this DPA in accordance with Section 1 below ("Effective Date").

1. Instructions and Effectiveness

1.1. To enter into this DPA, Customer must:

1.1.1. be a customer of the Atlassian Cloud Apps provided by TNG;

1.1.2. complete the signature block below by signing and providing all relevant information; and

1.1.3. submit the completed and signed DPA to TNG via service desk (https://tng-tech.atlassian.net/servicedesk/customer/portal).

1.2. TNG will countersign the completed and signed DPA submitted by Customer and will submit the countersigned version of this DPA back to Customer.

1.3. This DPA will only be effective (as of the Effective Date) if countersigned and submitted from TNG to Customer. Where Customer makes any deletions or other revisions to this DPA, this DPA will be null and void.

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

2. Definitions

In this DPA, the following terms have the following meanings:

2.1. “Applicable Data Protection Law” means European Data Protection Law and Californian Data Protection Law that are applicable to the Processing of personal data under this DPA.

2.2. “Californian Data Protection Law” means the California Consumer Privacy Act (as amended) (the “CCPA”), including as modified by the California Privacy Rights Act of 2020 (the “CPRA”), upon the CPRA’s enforcement date of July 1, 2023, as applicable to Customer Personal Data.

2.3. “Controller”, “Processor”, “Data Subject”, “Personal Data” and “Processing” (and “process”) have the meanings given in European Data Protection Law.

2.4. “Customer Personal Data” means any personal data provided by (or on behalf of) Customer to TNG in connection with the Services, all as further described in ANNEX 1 of this DPA.

2.5. “End Users” or “Users” means an individual the Customer permits or invites to use the Atlassian Cloud Apps provided by TNG. For the avoidance of doubt: (a) individuals invited by End Users, (b) individuals under managed accounts, and

(c) individuals interacting with an Atlassian Cloud App provided by TNG as Customer`s customers are also considered End Users.

2.6. "End User License Agreement" means the End User License Agreement published at https://tngtech.atlassian.net/l/cp/BpuqhWEA in its latest revision.

2.7. “Europe” means for the purposes of this DPA, the Member States of the European Economic Area (“EEA”).

2.8. “European Data Protection Law” means the 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”).

2.9. “Third Country 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.

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

2.11. “Services” means the provision of the Atlassian Cloud Apps provided by TNG to Customer pursuant to the End User License Agreement.

2.12. “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.

2.13. “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.

2.14. “Sub-Processor” means any Processor engaged by TNG to assist in fulfilling its obligations with respect to providing the Services pursuant to this DPA where such entity processes Customer Personal Data. Sub-Processors may include TNG’s affiliates or other third parties.

3. Purpose and scope

3.1. The Customer is a user of Atlassian Cloud-Services. TNG is a provider of Plug-Ins/Apps for the Atlassian Cloud-Services. In its capacity as a provider of Atlassian Plug-Ins/Apps TNG processes Customer Personal Data on behalf of Customer in connection with the Services. While TNG will act as a Processor on

behalf of Customer, Customer processes such Personal Data as a Controller and this DPA will apply accordingly.

3.2. In its role as a Processor, as further detailed in ANNEX 1, TNG will process such Personal Data in compliance with Applicable Data Protection Law and only for the purposes that are compatible with those described in ANNEX 1.

4. Customer Processing of Personal Data

With regard to the Processing of Customer Personal Data, Customer shall be the Controller. 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 TNG, and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under Applicable Data Protection Law for TNG to process Personal Data (including but not limited to any Special Categories of Personal Data) and provide the Services pursuant the End User License Agreement (including this DPA).

5. TNG Processing of Personal Data

With regard to the Processing of Customer Personal Data, TNG shall be the Processor. When TNG processes Customer Personal Data in its capacity as a Processor on behalf of the Customer, TNG will process the Customer Personal Data as necessary to perform its obligations under this DPA, and only in accordance with the documented lawful instructions of Customer (as set forth in this DPA, or as directed by the Customer) (the “Permitted Purpose”). TNG will not retain, use, disclose or otherwise process the Customer Personal Data for any purpose other than the Permitted Purpose except where otherwise required by law(s) that are not incompatible with Applicable Data Protection Law, and will not “sell” the Customer Personal Data within the meaning of Californian Data Protection Law. TNG will promptly inform Customer if it becomes aware that Customer's Processing instructions infringe Applicable Data Protection Law.

6. Third Country Transfers

The parties agree that when the transfer of Personal Data from TNG (as “data exporter”) to a Sub-Processor (as “data importer”) is a Third Country Transfer and Applicable Data Protection Law requires that appropriate safeguards are put in place, the transfer will be Subject to the Standard Contractual Clauses.

7. Sub-Processing

7.1. Customer agrees that TNG may engage Sub-Processors to process Customer Personal Data on Customer’s behalf. The Sub-Processors currently engaged by TNG and authorized by Customer are listed in ANNEX 3. TNG 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 fulfil its data protection obligations with regard to the relevant Processing activities under Applicable Data Protection Law.

7.2. TNG must (i) make available an up-to-date list of the Sub-Processors it has appointed upon written request from Customer; and (ii) notify Customer if it adds any new Sub-Processors at least fourteen (14) days' prior to allowing such Sub-Processor to process Customer Personal Data. The Customer may object in writing to TNG'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 parties will discuss such concerns in good faith with a view to achieving resolution. If the parties are not able to achieve resolution, 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.

8. Deletion or return of Data

Upon the termination of the End User License Agreement TNG will delete or return to Customer all Customer Personal Data (including copies) processed on behalf of the Customer within a reasonable time-frame in compliance with legal requirements and technical limitations; this requirement does not apply to the extent TNG is required by applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data it has stored on back-up systems, which Customer Personal Data TNG will securely isolate and protect from any further Processing.

9. Technical and organizational measures

TNG and, to the extent required under the DPA, 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. TNG's current technical and organizational measures (TOMs) are described in ANNEX 2. Customer acknowledges that the TOMs are Subject to technical progress and development and that TNG may update or modify the TOMs from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

10. Cooperation obligations and Data Subjects' rights

10.1. Taking into account the nature of the Processing, TNG must provide reasonable and timely assistance to Customer (at Customer's expense) 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 TNG processes on Customer's behalf.

10.2. In the event that any request, correspondence, enquiry or complaint (referred to under section 10.1. above) is made directly to TNG, TNG 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 TNG, Customer may respond. If TNG is legally required to respond to such a request, TNG will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

10.3. To the extent TNG is required under Applicable Data Protection Law, TNG will (at Customer's request and expense) 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 TNG.

11. Californian Data Protection Law / CCPA

11.1. The term "Data Subject" within this DPA includes "Consumer" as defined under the CCPA. Any Data Subject rights outlined in Section 10 of this DPA shall be applicable to Consumer rights.

11.2. The term "Controller" in this DPA encompasses the definition of "Business" as defined under the CCPA. Similarly, the term "Processor" includes "Service Provider" as defined under the CCPA.

11.3. TNG shall process, retain, use, and disclose Personal Data solely as necessary to provide the Services as specified in the End User License Agreement. TNG commits to the following: (i) refraining from selling or sharing (as defined by the CCPA) Customer's Personal Data; (ii) not retaining, using, or disclosing Customer's Personal Data for any commercial purpose (as defined by the CCPA) beyond the provision of the Services; (iii) not retaining, using, or disclosing Customer's Personal Data beyond the scope outlined in this DPA.

11.4. As part of performing the Services TNG may deidentify (as defined by the CCPA) Customer Personal Data, adhering to the limitations imposed on Service Providers under the CCPA. TNG shall not reidentify any Customer deidentified Data.

11.5. TNG affirms that its Sub-Processors, as described in Section 7 of this DPA, are considered Service Providers under the CCPA. TNG has entered into agreements with these Sub-Processors, incorporating terms that require the Sub-Processor to protect the Customer Personal Data to the standard required by Californian Data Protection Law (and in substance, to the same standard provided by this DPA).

11.6. In the event that TNG becomes aware of its inability to fulfill any of its obligations under the CCPA, TNG shall promptly notify Customer.

12. Security Incidents

Upon becoming aware of a Security Incident, TNG will inform Customer without undue delay and provide timely information (taking into account the nature of Processing and the information available to TNG) relating to the Security Incident as it becomes known or as is reasonably requested by Customer to allow Customer to fulfil its data breach reporting obligations under Applicable Data Protection Law. TNG will further take reasonable steps to contain, investigate, and mitigate the effects of the Security Incident. TNG's notification of or response to a Security Incident in accordance with this Section

12 will not be construed as an acknowledgment by TNG of any fault or liability with respect to the Security Incident.

13. Law Enforcement

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

14. Audit

14.1. Where required by Applicable Data Protection Law, Customer may conduct audits (including inspections) during the term of the Agreement to establish TNG's compliance with the terms of this DPA, on the condition that Customer have entered into an applicable non-disclosure agreement with TNG. The Customer has the liberty to employ their own third-party auditors or appoint third parties of their choice to carry out those audits. The Customer shall limit the steps necessary for the audit to the minimum required and shall take care to hinder TNG as little as possible in its own operations. Notwithstanding the foregoing, any audit must be conducted during TNG's regular business hours, with reasonable advance notice (which may not be less than 14 calendar days) and Subject to reasonable confidentiality procedures.

14.2. Specifically, audits Subject to Section 14.1 may not require TNG to disclose to Customer or to allow Customer to access:

14.2.1. any data or information of any other TNG customer (or such customer's End Users);

14.2.2. any TNG internal accounting or financial information;

14.2.3. any TNG trade secret;

14.2.4. any information that, in TNG's reasonable opinion, could: (i) compromise the security of TNG systems or premises; or (ii) cause TNG to breach its obligations under Applicable Data Protection Law or its security, confidentiality and or privacy obligations to any other TNG customer or any third party; or

14.2.5. any information that Customer or its authorized representatives seek to access for any reason other than the good faith fulfilment of Customer's obligations under the Applicable Data Protection Law and TNG's compliance with the terms of this DPA.

14.3. An audit or inspection permitted in compliance with Section 14.1 will be limited to once per calendar year, unless (i) TNG has experienced a Security Incident within the prior twelve (12) months which has impacted Customer Personal Data; or (ii) Customer is able to evidence an incidence of TNG's material non-compliance with this DPA.

14.4. If a breach is detected, TNG shall reimburse the Customer for the costs incurred in conducting the audit. Conversely, if the audit determines no breach has occurred, the Customer shall bear the costs for the audit. Any other internal costs related to the audit will be borne by the respective parties themselves.

15. Miscellaneous

15.1. The parties agree that this DPA replaces and supersedes any existing DPA the parties may have previously entered into in connection with the Services. Amendments and supplements to this agreement must be made in writing. This also applies to the waiver of this formal requirement.

15.2. This DPA will be governed by and construed in accordance with the laws of the Federal Republic of Germany, unless required otherwise by Applicable Data Protection Law.

15.3. Any claim or dispute arising from or in connection with this DPA must be settled by the courts of Munich as first instance.

15.4. In case of doubt, the provisions of this agreement shall take precedence over the provisions of the End User License Agreement. Should individual provisions of this agreement prove to be invalid or unenforceable in whole or in part or become invalid or unenforceable as a result of changes in legislation after conclusion of the agreement, the validity of the remaining provisions shall not be affected thereby. The invalid or unenforceable provision shall be replaced by the valid and enforceable provision which comes as close as possible to the meaning and purpose of the invalid provision.

TNG Signature

TNG Technology Consulting GmbH
Signed:
Name:
Title:
Date:

Data Protection Point of Contact: Dr. Daniel Wortmann

Contact Details: datenschutz@tngtech.com

Customer Signature

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:

_____

ANNEX 1 – Purposes and scope of the Processing, type of data and categories of Data Subjects

For details on the nature of Processing by specific apps, see TNG's representation in the Atlassian Marketplace

Type of Controller Data	• Atlassian identifier associated with user account • Personal Data included in user generated content processed by the Apps
Type of Processing	• Collecting, storing and Processing Customer Data necessary to fulfil the function of Apps provided by TNG
Purposes of Processing	• Enable the functionality of the Apps
Categories of Data Subjects	• Users of Customer's Atlassian Cloud products • Subjects of Personal Data contained in user generated content

ANNEX 2 – Technical and Organizational Measures in Accordance with Section 9 of this DPA

Data Management using the Atlassian Forge Platform

- All data is processed exclusively within the Atlassian Forge Platform, which is provided by Atlassian to host Atlassian Cloud Apps provided by TNG.
- TNG does not store Customer Personal Data outside of the Atlassian Forge Platform, and has no direct access to the data processed by the apps.
- In accordance with the Shared Responsibility Model of Atlassian Forge, Atlassian has in particular implemented the following measures:
    - Transport encryption with TLS
    - Data encryption at rest

- Isolation of tenants
- Backup of data
- DoS mitigation

Software Lifecycle Management

- TNG aims to have all Atlassian Cloud Apps provided by TNG participating in Atlassian's security bug bounty program.
- All Atlassian Cloud Apps provided by TNG take part in internal penetration testing sessions which are conducted by IT experts from TNG who do not work on our Atlassian Cloud Apps on a day-to-day basis.
- Adherence to the resolution time frames of Atlassian's security bug fix policy.

Secure Development Environment

- Use of single sign-on (SSO) and multi-factor authentication (MFA) with hardware tokens for all personalized accounts.
- All personalized accounts have individual passwords that must fulfil current recommendations for secure passwords.
- Workstations are individually assigned and not shared between employees.
- Data on hard drives of all workstations is fully encrypted.
- Security patches are installed regularly.
- All employees are ordered to lock their workstations on absence.
- Access is granted by roles, following an access minimizing "need to know" principle.
- Strict separation of development, staging, and production environments.

Organizational Measures

- TNG has laid down an internal security policy and implemented response protocols to respond to security incidents promptly and effectively.
- All employees have committed themselves to confidentiality, in particular regarding Personal Data.
- Knowledge on data protection regulations is maintained with yearly briefings.

ANNEX 3 – Sub-Processors

Sub-Processor	Address and Country	Services	Guarantees for Third Country Transfer
Atlassian Pty. Ltd.	Level 6, 341 George Street Sydney NSW 2000 Australia	Providing infrastructure for development and operation of Plug-Ins/Apps for Atlassian Cloud-Services (Atlassian Forge Platform)	Standard Contractual Clauses according to Art. 46 GDPR https://developer.atlassian.com/platform/forge/resources/Forge-Data-Processing-Addendum.pdf