Data Processing Agreement

USING THIS DPA

This DPA has 2 parts: (1) the Key Terms on this Cover Page and (2) the Common Paper DPA Standard Terms Version 1.1 posted at commonpaper.com/standards/data-processing-agreement/1.1 ("**DPA Standard Terms**"), which is incorporated by reference. If there is any inconsistency between the parts of the DPA, the Cover Page will control over the DPA Standard Terms. Capitalized and **highlighted** words have the meanings given on the Cover Page. However, if the Cover Page omits or does not define a highlighted word, the default meaning will be "none" or "not applicable" and the correlating clause, sentence, or section does not apply to this DPA. All other capitalized words have the meanings given in the DPA Standard Terms or the **Agreement**.

Key Terms

The key legal terms of the DPA are as follows:

Agreement	This DPA supplements the following agreement: https://www.atlassian.com/licensing/marketplace/end-user-agreement-v1
Approved Subprocessors	**Name**: Hetzner Online GmbH **Country of location**: Germany **Anticipated processing task**: Cloud hosting and infrastructure for the servers operated by Provider in the EU, on which scan results, metadata and connection and security logs are processed and stored. **Name**: Atlassian Pty Ltd **Country of location**: United States and other regions, depending on the customer's Atlassian data residency selection **Anticipated processing task**: Provision of the Atlassian Forge platform on which part of the App runs, including Forge hosted storage for intake keys and configuration and the transit of scan content, under Atlassian's Forge Data Processing Addendum.
Provider Security Contact	contact@revin-tech.com
Security Policy	As defined in the **Agreement**.

Changes to the Agreement

Service Provider Relationship	To the extent California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq ("CCPA") applies, the parties acknowledge and agree that Provider is a service provider and is receiving Personal Data from Customer to provide the Service as agreed in the Agreement and detailed below (*see* Nature and Purpose of Processing), which constitutes a limited and specified business purpose. Provider will not sell or share any Personal Data provided by Customer under the Agreement. In addition, Provider will not retain, use, or disclose any Personal Data provided by Customer under the Agreement except as necessary for providing the Service for Customer, as stated in the Agreement, or as permitted by Applicable Data Protection Laws. Provider certifies that it understands the restrictions of this paragraph and will comply with all Applicable Data Protection Laws. Provider will notify Customer if it can no longer meet its obligations under the CCPA.

Restricted Transfers

Governing Member State	EEA Transfers: Germany UK Transfers: England and Wales

Annex I(A) List of Parties

Data Exporter	**Name:** the **Customer** signing this DPA **Activities relevant to transfer:** See Annex 1(B) **Role:** Controller
Data Importer	**Name:** the **Provider** signing this DPA **Contact person:** Lukas Werner Büttner, Managing Director (Geschäftsführer) **Address:** St. Wendeler Str. 2 A, Namborn, Saarland 66640, Germany **Activities relevant to transfer:** See Annex 1(B) **Role:** Processor

Annex I(B) Description of Transfer and Processing Activities

Service	**The Service is:** Security Provider for Jira (Built for Trivy): an Atlassian Marketplace app that brings security scanner findings (vulnerabilities and detected secrets) into the customer's Jira instance as security findings.
Categories of Data Subjects	**Customer's** employees Any individuals whose personal data is incidentally contained in the scan content the customer submits (for example in free-text fields, labels, or detected secrets such as embedded credentials or tokens), and holders of the IP addresses recorded in the Provider's connection and security logs
Categories of Personal Data	Name Contact information such as email, phone number, or address User activity and analysis such as device information or IP address Personal data incidentally contained in the scan content the customer submits, including detected secrets such as embedded credentials or tokens. The App neither seeks nor requests personal data; any such data is processed solely on the customer's behalf to deliver the App.
Special Category Data **Is special category data (as defined in Article 9 of the GDPR) Processed?**	No

Frequency of Transfer	Continuous
Nature and Purpose of Processing	Receiving data, including collection, accessing, retrieval, recording, and data entry Holding data, including storage, organization, and structuring Protecting data, including restricting, encrypting, and security testing Sharing data, including disclosure, dissemination, allowing access, or otherwise making available Returning data to the data exporter or data subject Erasing data, including destruction and deletion
Duration of Processing	**Provider** will process Customer Personal Data as long as required (i) to conduct the Processing activities instructed in Section 2.2(a)-(d) of the Standard Terms; or (ii) by Applicable Laws.

Annex I(C)

Competent Supervisory Authority	The supervisory authority will be the supervisory authority of the data exporter, as determined in accordance with Clause 13 of the EEA SCCs or the relevant provision of the UK Addendum.

Annex II

Technical and Organizational Security Measures	Pseudonymization and encryption of personal data: The Provider encrypts Customer Personal Data in transit using TLS for all transmissions to its servers and to the Atlassian Forge platform. The Provider does not rely on pseudonymization, as most of the data it processes is technical; where personal data occurs, it is protected by the encryption and access controls described in this Annex. Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services: The Provider maintains the confidentiality, integrity, availability and resilience of its systems through the measures described in this Annex: encryption in transit (TLS), least-privilege access controls with end-user authentication handled by Atlassian, logical separation of each installation's data by a unique installation identifier, connection and security logging with automatic blocking of abusive IP addresses, data minimization, and limited retention. The App runs on the Atlassian Forge platform and on servers the Provider operates at Hetzner in the EU, whose data centres provide physical and network infrastructure security. Personal data is restricted to what is necessary to deliver the App and is not used for advertising, analytics, profiling, or AI training. Ability to restore the availability of and access to the Customer Personal Data in a timely manner following a physical or technical incident: Customer Personal Data is stored on servers the Provider operates at Hetzner in the EU, with backups that allow the data to be restored following a physical or technical incident such as corruption or accidental loss. Backups are taken daily and retained for 7 days. User identification and authorization process and protection:

End-user authentication is handled entirely by Atlassian through the Forge platform; the Provider does not receive or store end-user login credentials. Access to the Provider's own systems and infrastructure is limited to authorized personnel on a least-privilege basis.

Protecting Customer Personal Data during transmission (in transit):

All transmissions of Customer Personal Data to and from the Provider's servers, and to the Atlassian Forge platform, are encrypted in transit using current TLS (HTTPS).

Protecting Customer Personal Data during storage (at rest):

Customer Personal Data stored on the Provider's servers at Hetzner in the EU is protected by access controls limited to authorized personnel on a least-privilege basis, logical separation of each installation's data by a unique installation identifier, and the physical and infrastructure security of the hosting data centres.

Physical security where Customer Personal Data is processed:

The Provider does not operate its own data centres. Physical security is provided by the Provider's sub-processors: the servers the Provider operates are hosted in Hetzner's data centres in the EU, and part of the App runs on the Atlassian Forge platform. Both maintain physical access controls, building and facility security, and monitoring at their data centres.

Events logging:

The Provider maintains connection and security logs for its servers, recording incoming connections (including IP addresses) to detect and prevent automated attacks, misuse, and unauthorized access. Abusive IP addresses are blocked automatically. Connection logs are rotated and deleted weekly, and blocked IP addresses are kept for at most 30 days.

Systems configuration, including default configuration:

The App runs on the managed Atlassian Forge platform and on a server the Provider operates at Hetzner in the EU, which the Provider keeps maintained and monitored. Data from different installations is held in a single shared database and is logically separated by a unique installation identifier, with the App enforcing that each installation can access only its own data.

Ensuring data minimization:

The Provider limits the data it processes to what is necessary to deliver the App. It does not read Jira account, profile or user data and does not store login credentials; it processes only the scan content the customer chooses to send. Installation data is deleted after uninstallation, connection logs are rotated weekly, and blocked IP addresses are kept at most 30 days. The Provider does not use personal data for advertising, analytics, profiling, or AI training.

Ensuring limited data retention:

The Provider retains Customer Personal Data only as long as needed to provide the App. Installation data (metadata, scan results, installation identifiers, intake keys, and configuration) is kept for the life of the installation and deleted after the App is uninstalled. Connection logs are rotated and deleted weekly, and blocked IP addresses are kept for at most 30 days. Where data cannot be deleted at once because it remains in backups, it is isolated from further processing until deletion is possible.

Allowing data portability and erasure:

On the customer's instruction, the Provider deletes Customer Personal Data from its systems and can remove content the App had written into the customer's Jira instance. Where an individual contacts the Provider about personal data contained in scan content, the Provider forwards the request to the customer, as the controller, without undue delay and acts on the customer's instruction. The Provider does not operate its own data-processing hardware; secure disposal of storage media is handled by its sub-processors' data centres (Hetzner in the EU; Atlassian for Forge).

Other Changes to the DPA Standard Terms

Additional modifications or customizations

Provider and Customer have not changed the DPA Standard Terms except for the details on the Cover Page above. By signing this Cover Page, each party agrees to enter into this DPA as of the last date of signature below.

	PROVIDER: Revin Technologies UG (haftungsbeschränkt)	CUSTOMER:
Signature		
Print Name	Lukas Werner Büttner	
Title	Managing Director (Geschäftsführer)	
Legal Notice Address	St. Wendeler Str. 2 A Namborn, Saarland 66640 Germany	
Date		