VERSION 3.5 · NOVEMBER 2026

Data Processing Agreement pursuant to Article 28 GDPR

between the Customer (the "**Controller**") and BitHive UG (haftungsbeschränkt), Heisenbergstraße 3, 10587 Berlin, Germany (the "**Processor**"), for the BitHive Reporting Desk (the "**Service**").

Version 3.5 · November 2026 · Replaces version 3.4. Changes: Jira Cloud as a destination (1.6, Annex 1), restore tests (Annex 2).

1. Subject matter, duration and specification of processing

1.1 The Processor processes personal data on behalf of the Controller for the purpose of providing the Service under the Terms of Service (the "**Main Contract**"). This Agreement applies to all such processing.

1.2 The term of this Agreement corresponds to the term of the Main Contract. Obligations that by their nature continue beyond it (in particular Sections 8 and 9) remain in force.

1.3 Nature and purpose of processing, types of personal data and categories of data subjects are set out in Annex 1.

1.4 **Place of processing.** The Service is hosted exclusively in data centres in Germany by a hosting provider established in Germany. All data stored in the Service, in particular SBOMs, vulnerability cases, report texts and the audit log, remains in Germany. E-mails to the Processor's support address are processed in a mailbox hosted in Germany by the sub-processor listed for this purpose in Annex 3. E-mails sent by the Service (login links and notifications) are delivered by the e-mail sub-processor listed in Annex 3, a company established in France that processes them in data centres in the European Union, without processing in third countries. Any transfer of personal data to a third country requires the prior consent of the Controller in text form and takes place only in accordance with Articles 44 to 49 GDPR.

1.5 **Audit log and retention.** The Service keeps an append-only audit log of actions in the Service as evidence of how the Controller handles its reporting obligations. Entries name the acting person, cannot be changed or deleted individually by users of the Service, and keep a person's name after that person has been removed as a user. The Controller chooses in the Service the retention period for audit log entries and report records (24 months or 10 years); when it expires, the Processor deletes the entries concerned. The choice of retention period is an instruction of the Controller within the meaning of Section 2.1. Removing a module or reducing a plan neither shortens the retention period nor deletes entries; only a shorter retention period chosen by the Controller does, subject to Section 7.6 (c) of the Main Contract. If the Controller decides that an entry must be erased or pseudonymised, for example following a request from a data subject, the Processor carries this out on the Controller's instruction in text form. If the Controller's Owner deletes the account (Section 8.6 of the Main Contract), the audit log is deleted together with the account; the export offered beforehand contains it. After the end of the Main Contract, Section 7 applies.

1.6 **Alert channels and Jira.** Where the Controller configures alert channels in the Service, such as Slack, Microsoft Teams or a webhook address, or connects its own Jira Cloud site, the Processor sends alert messages and, for Jira, issues and comments about the Controller's cases to the destinations the Controller specifies, on the Controller's instruction. The providers of these destinations (for Jira: Atlassian) are chosen by the Controller and are not sub-processors of the Processor; the Controller is responsible for its relationship with them, including any transfer to a third country. Alert messages, issues and comments contain the information needed to act on the alert, such as the product, the vulnerability, the deadline and a link to the case. To connect Jira, the Processor stores the access granted by Atlassian encrypted, uses it only for these issues and comments and for what they require, and deletes it when the Controller disconnects Jira or the account is deleted.

1.7 **Use as a processor.** Where the Controller itself processes personal data on behalf of its own customers and enters such data into the Service (in particular in the processor mode of the GDPR breach module), the Processor acts as a further processor (sub-processor) of the Controller within the meaning of Article 28 (4) GDPR, and this Agreement applies as the contract required by that provision. The Controller warrants that it is authorised under its own contracts to engage the Processor and its sub-processors (Annex 3) and informs its customers where required. Instructions are given only by the Controller.

2. Instructions

2.1 The Processor processes personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law; in such a case, the Processor informs the Controller of that legal requirement before processing, unless that law prohibits such information. The Main Contract, this Agreement and the Controller's use of the Service's functions constitute the Controller's instructions.

2.2 Further instructions are given in text form. The Processor informs the Controller without undue delay if it considers that an instruction infringes data protection law. It may suspend the execution of that instruction until the Controller confirms or changes it.

3. Obligations of the Processor

3.1 The Processor ensures that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.2 The Processor takes all measures required under Article 32 GDPR. The technical and organisational measures are described in Annex 2. The Processor may adapt them to technical progress, provided the level of protection is not reduced.

3.3 Taking into account the nature of the processing, the Processor assists the Controller with appropriate technical and organisational measures in fulfilling its obligations to respond to requests from data subjects (Articles 12 to 23 GDPR). If a data subject contacts the Processor directly, the Processor forwards the request to the Controller without undue delay.

3.4 The Processor assists the Controller in ensuring compliance with Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to it.

3.5 The Processor notifies the Controller without undue delay, and at the latest within 24 hours, after becoming aware of a personal data breach affecting the Controller's data. The notification is sent by e-mail to the Owner and all administrators of the Controller's account. It contains, as far as available, the information set out in Article 33 (3) GDPR; information that is not yet available is provided without undue delay as it becomes available.

3.6 If a public authority of a third country requests the disclosure of the Controller's personal data, the Processor will inform the Controller without undue delay, unless prohibited by law, will challenge the request where there are reasonable grounds to do so, and will disclose only the minimum necessary. The Processor will pass on any such request received by a sub-processor.

3.7 The Processor has designated a contact person for data protection: contact@bithive-it.com. The Processor is not obliged to appoint a data protection officer as long as the statutory requirements for this are not met.

4. Sub-processors

4.1 The Controller grants general authorisation to engage the sub-processors listed in Annex 3.

4.2 The Processor informs the Controller in text form at least four weeks in advance of any intended addition or replacement of a sub-processor or, where a sub-processor of the Processor gives the Processor shorter notice, without undue delay after the Processor receives it. The Controller may object to the change within this period for important data protection reasons. If the Processor does not refrain from the change, the Controller may terminate the Main Contract with effect from the date of the change.

4.3 The Processor imposes on each sub-processor, by contract, the same data protection obligations as set out in this Agreement, in particular sufficient guarantees for appropriate technical and organisational measures, and ensures that the standard contractual clauses are in place where a sub-processor or one of its own sub-processors processes data in or from a third country. The Processor remains liable to the Controller for the performance of the sub-processor's obligations.

4.4 Services that the Processor uses as ancillary services, such as telecommunications or postal services, are not sub-processing within the meaning of this Section.

5. Rights and obligations of the Controller

5.1 The Controller is responsible for the lawfulness of the processing, including the lawfulness of the disclosure of personal data to the Processor, and for safeguarding the rights of data subjects.

5.2 The Controller informs the Processor without undue delay if it detects errors or irregularities in the processing results.

6. Audits

6.1 The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations under Article 28 GDPR, in particular this Agreement, the description of technical and organisational measures and, where available, certificates or audit reports, including those of its sub-processors.

6.2 The Controller or an auditor mandated by it and bound to confidentiality may carry out inspections, as a rule after notice of at least four weeks, during normal business hours and without disrupting operations, and no more than once per calendar year unless there are specific indications of a breach. Inspections of sub-processors take place by means of the sub-processor's certificates and audit reports.

6.3 The Processor may charge reasonable compensation for its effort in supporting inspections that go beyond Section 6.1, unless the inspection reveals a breach by the Processor.

7. Deletion and return

7.1 After the end of the provision of services, the Controller chooses between the return of the personal data by export, which is available for 30 days after the end of the Main Contract (Section 8.5 of the Main Contract), and their earlier deletion on instruction in text form. After this period, or on that instruction, the Processor deletes all personal data processed on behalf of the Controller, unless Union or Member State law requires their storage. The Processor confirms the deletion in text form on request.

7.2 Backups are overwritten in the regular backup cycle, at the latest 35 days after deletion from the production system.

7.3 If the Controller's Owner deletes the account (Section 8.6 of the Main Contract), the deletion takes effect 14 days after its confirmation; until then the Controller can export its data or cancel the deletion. The confirmed deletion is an instruction within the meaning of Section 7.1.

8. Liability

Liability is governed by Article 82 GDPR. In the internal relationship between the parties, the liability provisions of the Main Contract apply, unless mandatory law provides otherwise.

9. Final provisions

9.1 In the event of contradictions, this Agreement takes precedence over the Main Contract with regard to data protection.

9.2 Changes and additions to this Agreement require text form.

9.3 The law of the Federal Republic of Germany applies. The place of jurisdiction is determined by the Main Contract.

9.4 This Agreement exists in a German and an English version. The version in the contract language of the Main Contract is binding. The contract language is that of the Main Contract (Section 12.6 of the Main Contract). Versions in other languages are provided for information only.

9.5 If the Controller is established in a third country for which no adequacy decision exists and its processing is not subject to the GDPR, the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914, Module Four (transfer processor to controller), are incorporated into this Agreement. For this purpose, the Processor is the data exporter and the Controller the data importer; the optional Clause 7 does not apply; for Clause 17 the parties choose the law of Germany, and for Clause 18 the courts of Berlin; the information required by the annexes to the clauses is taken from Annexes 1 to 3 of this Agreement. In the event of a conflict, the standard contractual clauses prevail. For Controllers subject to the UK GDPR, references to the GDPR also refer to the corresponding provisions of the UK GDPR.

Annex 1: Specification of processing

Item	Description
Nature and purpose	Hosting and operation of the Service: user administration, invitations and login, storage and analysis of SBOMs, comparison with vulnerability information, sending notifications, deadline tracking, preparation of report texts, audit log, support; case management for incidents, personal data breaches and contractual notifications (modules booked by the Controller): recording of events, deadline calculation, drafts, alerts and evidence records. Where the Controller connects its Jira Cloud site: creating issues and comments about its cases in that site.
Types of personal data	User master data (name, business e-mail address, role, team); invitations (e-mail address, name and role of the invited person, status and expiry); authentication data (login links, hashed API tokens); usage and log data (time stamps, IP addresses, actions in the Service); contents entered by users (comments, report texts, which may contain names of contact persons); contact data of notification recipients; where the Controller uses a vulnerability-intake function: name and contact details of reporting persons and the content of their reports; descriptions of incidents and breaches, which may include categories and approximate numbers of affected persons and records, and in exceptional cases limited identifying data the Controller considers necessary for documentation (Art. 33(5) GDPR); names and business contact data of contact persons at authorities, controllers, processors and other recipients of notifications; where the Controller connects its Jira Cloud site: the access granted by Atlassian (OAuth tokens, stored encrypted), which contains the Atlassian account ID of the user who connected it.
Categories of data subjects	Employees and agents of the Controller who use the Service, are invited to it or receive notifications; contact persons named in reports; persons who report vulnerabilities to the Controller through the Service; persons affected by an incident or breach recorded by the Controller (as categories, see above); contact persons of the Controller's customers, suppliers and competent authorities.
Special categories (Art. 9 GDPR)	Not intended. The Controller shall not enter such data into the Service. Breach records describe the categories of data affected; they must not contain the special categories of personal data themselves.

Annex 2: Technical and organisational measures (Article 32 GDPR)

Confidentiality

- **Physical access:** the Service runs exclusively in data centres in Germany of the hosting provider listed in Annex 3, which operates physical access control and whose information security management system is certified to ISO/IEC 27001. The Processor operates no own server rooms. The hosting provider also holds a BSI C5:2020 Type 2 attestation covering cloud servers, block storage and object storage.
- **System access:** administrative access only via personal accounts with multi-factor authentication; no shared accounts; access keys stored encrypted; principle of least privilege.
- **Data access:** strict separation of customers (tenants): every customer data record carries a tenant identifier, and the database enforces isolation through row-level security in addition to the application; users log in without passwords via one-time links; API tokens are stored only as cryptographic hashes and can be restricted and revoked.
- **Separation:** production, test and development environments are separate; no customer data in test or development.

Integrity

- **Transmission:** all connections encrypted with TLS 1.2 or higher; e-mail notifications contain no vulnerability details beyond what is necessary and link to the Service.
- **Input control:** append-only audit log of relevant actions per tenant, with time stamp and user.
- **Software integrity:** every change is reviewed and passes automated tests, static analysis and a dependency vulnerability scan before deployment.

Availability and resilience

- PostgreSQL database with continuous archiving and point-in-time recovery; backups are encrypted before they leave the server and are stored in object storage in Germany with write-once locking; restore procedures are tested at least once in every calendar month, and each test is recorded.
- Encryption of stored data at rest: the storage volume holding the database, application data and logs is encrypted; the server's system disk holds no personal data; backups are encrypted.
- Availability monitoring with alerting: heartbeats of all background processes and a check of the public address at least once a minute. The monitoring service receives no personal data of the Controller. A documented incident-response procedure is in place.

Procedures for regular review

- Review of access rights at least quarterly; review of these measures at least annually and after significant changes.
- Automated checks for updates: operating-system security updates are installed automatically; application dependencies and build tools are checked at least monthly.
- Data protection by default: only data necessary for the Service is collected; no tracking, no advertising, no use of customer data for other purposes, in particular not for training AI models.

Annex 3: Approved sub-processors

Sub-processor	Service	Location of processing	Third-country safeguards
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany	Cloud hosting: servers, storage volumes, object storage for backups	Germany (data centres in Nuremberg and Falkenstein)	Not applicable (no third-country processing)
STRATO GmbH, Otto-Ostrowski-Straße 7, 10249 Berlin, Germany	Hosting of the support mailbox (e-mails to the support address)	Germany	Not applicable (no third-country processing)
Scaleway SAS, 8 rue de la Ville l'Evêque, 75008 Paris, France	Delivery of transactional e-mails (login links, notifications)	European Union (data centres in the Paris region, France)	Not applicable (no third-country processing)

The details above reflect each sub-processor's data processing agreement as of October 2026.

Download as PDF·All legal documents