VERSION 3.6 · NOVEMBER 2026

Privacy Notice: BitHive Reporting Desk application

Version 3.6 · November 2026 · Replaces version 3.5. Changes: Jira Cloud as a destination the customer chooses, and where data leaves the European Union (6). This notice covers the application at app.bithive-it.com and its API. The privacy policy of our website bithive-it.com applies to the website.

1. Controller

BitHive UG (haftungsbeschränkt), Heisenbergstraße 3, 10587 Berlin, Germany, represented by its managing director Alireza Khalili. E-mail: contact@bithive-it.com.

2. Who is responsible for which data

Our customers use the application to manage their products, software bills of materials, vulnerability cases, incident and breach records and report texts, and they decide who in their organisation uses it. For personal data that customers and their users enter into the application, the **customer is the controller** and we process the data on its behalf under a data processing agreement (Art. 28 GDPR). If you are a user of a customer account, please contact that customer about your rights regarding this data; we support them in answering.

We are the controller for the processing described in Sections 3 to 5 and 9.

3. Customer contract, ordering and payment

We process the name, business contact details and billing information of our customers' contact persons in order to conclude and perform the contract and to communicate about it. We receive these data from you or your company during the order, from our payment service provider and, for bank transfers, from our bank.

We sell the Service ourselves and issue the invoices. Payments are processed by our payment service provider Stripe Payments Europe, Limited, Dublin, Ireland ("Stripe"). You enter your payment details directly on a Stripe payment page; we do not receive full card or account numbers (IBAN). We pass to Stripe the company name, billing address, VAT identification number, the e-mail address for invoices, and the amounts and dates of charges. From Stripe we receive the status of payments and subscriptions, the card brand, the last four digits and the expiry date of the card or, for direct debit, the last four digits of the IBAN and the mandate reference, and identifiers of transactions. If you pay with Apple Pay, Google Pay or Link, the provider of that service also processes your payment data under its own privacy terms; we receive the same information as for a card payment. Stripe processes these data on our behalf to execute payments and to create and send invoices, and as an independent controller for fraud prevention and to meet its own legal obligations, for example under anti-money-laundering law, under its own privacy notice (stripe.com/privacy). Stripe may transfer data to Stripe, LLC in the USA. Such transfers are based on the EU-U.S. Data Privacy Framework (Art. 45 GDPR) and on the European Commission's standard contractual clauses (Art. 46 (2) (c) GDPR).

Legal basis: Art. 6 (1) (b) GDPR (contract) and, for the contact persons of business customers, Art. 6 (1) (f) GDPR (our legitimate interest in performing contracts with companies); Art. 6 (1) (c) GDPR for statutory retention; Art. 6 (1) (c) GDPR for issuing invoices (§ 14 UStG).

Retention:

- After the end of the contract, we keep exact copies of order, plan-change and cancellation confirmations and of messages that conclude, change or end the contract.
- We also keep the records of acceptance of our Terms and the Data Processing Agreement (version, time, account identifier, name and e-mail address of the accepting user), and a minimal index of the contract (account identifier, company name, identifiers at our payment service provider, plan, amounts, dates).
- These records are kept for six years from the end of the calendar year in which they were sent or created (§ 257 HGB, § 147 AO). They are stored separately, accessible only to our managing director, and used only for commercial and tax duties and for legal claims (Art. 6 (1) (c) and (f), Art. 17 (3) (b) and (e) GDPR).
- Invoices, credit notes and other accounting vouchers, such as our payment service provider's payout reports, are kept for eight years from the end of the calendar year in which they were issued, and longer while they are relevant to taxes whose assessment period has not yet expired (§ 14b UStG, § 147 AO).

Before we activate an order, we check the company name against the sanctions lists of the European Union (Art. 6 (1) (c) GDPR in conjunction with the EU sanctions regulations). If there is a possible match, we review it manually and keep the result for five years as evidence.

If you pay by bank transfer, we receive from our bank the payer's name, the IBAN and BIC of the paying account, the amount, the date and the payment reference, and use them to match the payment to the invoice, for refunds and for our accounting (Art. 6 (1) (b) and (c) GDPR); your bank and our bank process these data as payment service providers under their own responsibility, and we keep bank statements as accounting vouchers for eight years (§ 147 AO).

3a. One free trial per company

To offer the free trial only once per company, we check at sign-up whether an account with the same VAT identification number or the same e-mail domain already exists or has used a trial. For this we compare these details with the data of existing accounts. When an account is deleted, we keep only a keyed hash of its VAT identification number and of its e-mail domain (no company name, no other account data), so that a company that has used a trial cannot start a second one. We delete these hashes at the end of the third calendar year after the deletion. You may object to this processing (Section 7). Legal basis: Art. 6 (1) (f) GDPR; our legitimate interest is preventing misuse of the free trial.

Trial limit records. Each time an account that had a trial reaches the product limit of its plan, during the trial or afterwards, we keep a record of the account identifier, the start of the trial and the time the limit applied. We keep these records also after the account has been deleted. We use them only to evaluate our trials and plan limits, for example how often an account that had a trial reaches the limit of its plan. The legal basis is Art. 6(1)(f) GDPR; our legitimate interest is evaluating and improving the trials and plans we offer. We delete each record 12 months after the start of the trial.

3b. Support requests

When you write to our support address, we process your name, your e-mail address and the content of your message in order to answer it. The mailbox is hosted on our behalf by STRATO GmbH, Berlin, on servers in Germany. Legal basis: Art. 6 (1) (b) GDPR where the request concerns the contract, otherwise Art. 6 (1) (f) GDPR (answering requests addressed to us). We delete support e-mails at the latest two years after the end of the year in which the request was closed, unless they are business letters under Section 3.

4. Security and operation of the application

When the application or the API is used, our servers record technical data: IP address, time, requested address, result status and, for logged-in users, the user ID. We use this data to operate the application, detect and defend against attacks and misuse, and investigate errors.

Legal basis: Art. 6 (1) (f) GDPR (our legitimate interest in the secure and stable operation of the application). The data is deleted after 30 days, unless it is needed longer to investigate a specific security incident.

5. Login and cookies

You log in without a password, using a one-time link sent by e-mail. After login, the application sets a single cookie that keeps you logged in. It is technically necessary for the service you have requested (Section 25 (2) no. 2 TDDDG) and is deleted when you log out, or at the latest after 14 days. We use no analytics, tracking or advertising cookies. For payment, the application takes you to a payment page that Stripe provides on its own website, where Stripe's terms and privacy notice apply (Section 3). Apart from that, the application loads no content from third parties.

Legal basis for processing the login data: Art. 6 (1) (b) GDPR or, for users of customer accounts, Art. 6 (1) (f) GDPR (secure access to the service booked by the customer).

Partner demo accounts. If you use a demo account that we provide to one of our referral partners, we process your name, your business e-mail address and your sign-in and activity records as described in this notice, to provide the demo account and keep it secure (Art. 6 (1) (f) GDPR; our legitimate interest is providing the demo to our partner). A demo account contains sample data only and is deleted with its data when it is closed.

6. Recipients and hosting

The application is operated exclusively in data centres in Germany by our hosting provider Hetzner Online GmbH, Gunzenhausen, Germany. E-mails (login links and notifications) are delivered by the e-mail service provider Scaleway SAS, Paris, France, which processes them in data centres in the European Union. Our e-mails contain no tracking pixels and no tracked links. Our support mailbox is hosted by STRATO GmbH, Berlin, on servers in Germany. All three act on our behalf under data processing agreements. Our payment service provider Stripe receives the data described in Section 3, partly on our behalf and partly as an independent controller. Where a customer configures alert channels such as Slack, Microsoft Teams, a webhook or its own Jira Cloud site, alert messages and, for Jira, issues and comments about its cases are sent to the destinations the customer has chosen, on its instruction. The providers of these destinations (for Jira: Atlassian) are chosen by the customer and receive the data as the customer's recipients, not as our processors. To connect Jira, we store the access granted by Atlassian (OAuth tokens) encrypted, use it only to list the Jira sites and projects the customer can choose from and to create those issues and comments, and delete it when the customer disconnects Jira or the account is deleted. We do not store names or e-mail addresses from the customer's Atlassian account.

Referral partners: if you order with a referral partner's code in commission mode, we give that partner the information needed to settle its commission: your company name, the net amounts you pay for your subscription for the 12 months from the start of your first paid billing period, any refunds, credits or chargebacks on them, and, if your order does not count as a referral, the reason. Legal basis: Art. 6(1)(f) GDPR; our legitimate interest is settling referral commissions correctly. You may object (Art. 21(1) GDPR); the partner then receives a reference number instead of your company name. If your order did not include these commission terms, or once your account has been deleted, the partner receives only a reference number instead of your company name. Referral partners may be established outside the European Union, in the United Kingdom, the United States, Canada or Australia. Where your company name identifies a person, transfers to them are based on an adequacy decision (United Kingdom, Canada; in the United States, for partners certified under the EU-U.S. Data Privacy Framework) or on the EU standard contractual clauses (Art. 45 and Art. 46(2)(c) GDPR).

The data stored in the application remains in Germany. Data leaves the European Union only as described in Section 3 (Stripe), under "Referral partners" above, and where a customer sends it to alert channels or a Jira Cloud site it has chosen (above).

7. Your rights

You have the right of access (Art. 15 GDPR), rectification (Art. 16), erasure (Art. 17), restriction of processing (Art. 18) and data portability (Art. 20). Where we process data on the basis of Art. 6 (1) (f) GDPR, you have the right to object at any time on grounds relating to your particular situation (Art. 21). To exercise your rights, contact contact@bithive-it.com.

You also have the right to lodge a complaint with a data protection supervisory authority. The authority responsible for us is the Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragte für Datenschutz und Informationsfreiheit).

8. No automated decisions

We do not use automated decision-making, including profiling, within the meaning of Art. 22 GDPR.

9. Deletion

- **Account deletion.** If the owner of your company's account deletes the account, the deletion takes effect 14 days later. Until then, only the owner can sign in, to export the data or to cancel the deletion.
- **What is deleted.** When the deletion takes effect, all data of the account, including its audit log, is deleted.
- **Backups.** Backups are overwritten at the latest 35 days after the deletion.
- **What we keep.** Only the records described in Section 3, the keyed hashes described in Section 3a, and a record without personal data stating that the account was deleted and when.
- **Unfinished orders** are deleted seven days after their last change.

10. Obligation to provide data

Providing the data described in Sections 3 to 5 is required to conclude the contract and to use the application; without them we cannot provide the application. There is no statutory obligation to provide them.

This notice exists in a German and an English version.

Download as PDF·All legal documents