# BOMvault Privacy Policy

*Last Updated: September 16, 2025*

## Introduction

At BOMvault, we value your privacy and are committed to protecting your data. This Privacy Policy explains what information we collect, how we use and safeguard it, and your rights in relation to it. **This Policy applies to all data processed through the BOMvault platform**, whether you interact via our web application, REST API, command-line interface (CLI), CI/CD integrations, or self-hosted agents. By using BOMvault, you agree to the practices described in this Policy.

## Data We Collect

We collect and process **two main categories of data** to provide and improve our services:

* **Account and Operational Data:** Personal and account information you provide to us, as well as data generated through your use of BOMvault. This includes your name, email address, login credentials (hashed passwords or single sign-on tokens), organization and billing contact details (including payment information), IP addresses and device information, usage telemetry (e.g. feature usage logs and access times), and any communications with us (such as support emails or chat messages). We collect this data to create and secure your account, process payments, provide customer support, monitor system performance, and improve the user experience.
* **DevSecOps Artifacts and Content:** Technical data you submit to BOMvault as part of using our DevSecOps features. This includes software Bill of Materials (SBOM) files, source code commit hashes, repository and project metadata, contributor names or emails associated with commits, and optional security scan results or vulnerability reports that you choose to upload. We use this data to perform the services you request - for example, to generate compliance reports, detect vulnerabilities, and track software components. While this category of data is primarily technical, it can incidentally contain personal identifiers (for instance, an open-source contributor’s name or email in a commit history). We handle all such data with the same care as personal information.

**Note:** We do **not** intentionally collect sensitive personal information such as government IDs, financial account numbers (aside from billing info for payments), or health/medical data through BOMvault. We ask that you **do not upload** any sensitive personal data or protected health information into our platform (see the **HIPAA and Health Information** section below). Any data you provide should be limited to what is necessary for using our DevSecOps tools.

## Data Storage and International Transfers

BOMvault is a cloud-based service, and we **host your data on Amazon Web Services (AWS) infrastructure**. By default, all data is stored and processed in the United States, within AWS’s **us-east-1** region (North Virginia). For customers who require data residency in Europe, we offer an **EU hosting option** - your data can be stored in the European Union, specifically in AWS’s **eu-central-1** region (Frankfurt, Germany). In either case, your data will remain in the region you choose.

We will **not move your data out of your selected region** unless it is necessary and lawful to do so. If we ever need to transfer personal data from one region to another (for example, from the EU to the US), we will ensure appropriate safeguards are in place. In particular, when transferring personal data from the European Economic Area (EEA) to a country not deemed adequate by the EU, we rely on the European Commission’s **Standard Contractual Clauses (SCCs)** or other approved legal mechanisms to guarantee that your information receives an equivalent level of protection. Our commitment is that cross-border data transfers will always comply with applicable data protection laws and that your data won’t be accessed from outside your chosen region unless such safeguards are in effect.

## Subprocessors (Third-Party Service Providers)

To operate BOMvault efficiently and reliably, we use a small number of trusted third-party service providers (also known as **subprocessors**) who may process certain data on our behalf. We vet all subprocessors for strong security and privacy practices and only share the minimum information necessary for them to perform their functions. Our key subprocessors include:

* **Amazon Web Services (AWS)** - Cloud infrastructure host for the BOMvault platform. All of our servers, databases, and storage run on AWS data centers (in your chosen region). AWS acts as our infrastructure provider for storing and processing your data.
* **Cloudflare** - Network security and content delivery. We use Cloudflare to help secure our website and API (providing firewall, DDoS protection, and TLS encryption) and to speed up content delivery globally via their content delivery network (CDN).
* **Stripe** - Payment processing. If you subscribe to a paid BOMvault plan, your billing information (such as credit card details and billing email) is handled by Stripe on our behalf. Stripe is a PCI-DSS compliant payment processor; we do not store your raw payment card details on our own servers.
* **Sentry** - Error monitoring service. BOMvault uses Sentry to track and log software errors or exceptions in our application. This helps us quickly identify and fix bugs. Error reports may include contextual information like your user ID or device info at the time of an error, but they do not intentionally collect the contents of your DevSecOps data.
* **Resend** - Email delivery service. We use Resend to send out transactional emails and notifications, such as account verification emails, password reset links, alert notifications, and support correspondence. Your name and email address may be used by this service to send you these messages.

We **never sell** your personal data, and we do not share it with any third parties for their own marketing or advertising purposes. The above subprocessors act only under our instructions and for the purposes described in this Policy. We maintain an up-to-date **Subprocessors List** on our website (at **bomvault.com/subprocessors**), which identifies all authorized subprocessors and their functions. We will provide **at least 30 days’ advance notice** on that page (and/or via email notification) before adding any new subprocessor that will handle personal data, giving you the opportunity to review and object if you have concerns.

## Security Measures

We take the security of your information very seriously. BOMvault implements **industry-standard security measures** to protect your data from unauthorized access, disclosure, or loss. For example, all data exchanged with our platform is **encrypted in transit** using TLS (HTTPS), and all stored data (including databases and file storage) is **encrypted at rest**. We employ strict access controls so that only authorized BOMvault personnel with a valid business need can access customer data, and all access is logged and monitored. We also separate each customer’s data logically to ensure that no other customer can access your information.

Our security program is aligned with best practices and regulatory standards. We are in line with SOC 2 Type II compliance, and we follow frameworks such as ISO 27001 to continually assess and improve our security posture. We conduct regular security testing, including vulnerability scans and penetration tests, to identify and address potential weaknesses. Additionally, we monitor our systems 24/7 for suspicious activities and have incident response plans ready. While no method of transmission or storage is absolutely foolproof, we strive to use commercially reasonable and state-of-the-art means to protect your personal data. **In plain terms,** we work hard to keep your data safe and to earn your trust through our security practices.

## Compliance with Privacy Laws

We understand the importance of privacy laws and regulations worldwide, and we design our practices to **comply with all applicable laws** in the regions where we operate. In particular:

**European Union (GDPR):** If you are located in the European Economic Area (EEA) or the United Kingdom, your personal information is protected by the EU General Data Protection Regulation (GDPR) (and equivalent UK data protection laws). BOMvault is fully committed to GDPR compliance. We only collect and use personal data as needed to provide our services or as otherwise permitted by law (for example, with your consent or to fulfill a contract with you). You have robust rights under the GDPR, including the right to access the data we hold about you, to correct or update it, to request deletion (the “right to be forgotten”), to restrict or object to certain processing, and to obtain a portable copy of your data. BOMvault honors these rights - you can contact us at any time to exercise your GDPR rights, and we will respond within the applicable legal timeframes. Moreover, as noted in the **Data Transfers** section, if we transfer your data out of the EEA, we rely on approved safeguards like Standard Contractual Clauses to ensure compliance with GDPR’s requirements for international data transfers.

**United States State Privacy Laws:** We also comply with U.S. state privacy laws that apply to our operations. For example, under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), California residents have the right to know what personal information we collect, the right to request deletion of their personal information, the right to correct inaccurate information, and the right to opt out of the “sale” or certain sharing of personal information. BOMvault does **not** sell personal data, and we only share personal data with third parties as described in this Policy (for instance, with our service providers, and always for the purpose of providing our services to you). If you are a California resident, you can contact us to exercise your privacy rights, and we will not discriminate against you for doing so. Similarly, we adhere to other state privacy laws such as the Colorado Privacy Act and Virginia’s Consumer Data Protection Act, extending similar rights and protections to residents of those states. No matter where you’re located in the U.S., we are committed to transparency and fairness in how we handle your information.

**Other Jurisdictions:** For users in other countries or regions, we will comply with relevant privacy laws applicable to us. We continually monitor the evolving privacy regulatory landscape (for instance, new laws in states or countries) and adjust our practices and this Policy as needed to ensure ongoing compliance. Our goal is to provide a consistent level of privacy protection to all our users, regardless of location.

## HIPAA and Health Information

BOMvault is **not intended for use with medical or health information**. We are not a “Covered Entity” or “Business Associate” as defined by the U.S. Health Insurance Portability and Accountability Act (**HIPAA**), and our services are not HIPAA-compliant. This means you should not store or transmit Protected Health Information (PHI) using BOMvault. We do not knowingly collect any health or medical information about individuals, and our platform is not designed to meet the stringent requirements necessary to safeguard PHI.

By using BOMvault, you agree **not to upload any PHI or other sensitive health data** to our service. If you do choose to include health-related information in the data you upload (which you should avoid), you do so at your own risk. BOMvault will not be responsible for any unauthorized disclosure or liability arising from such data, since our systems are not certified for healthcare data. If your organization is subject to HIPAA or similar healthcare privacy laws and you require a solution to handle PHI, please contact us to discuss alternatives - but by default, **BOMvault should not be used to store medical records or personal health information**.

## Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our services, technology, legal obligations, or other factors. When we make changes, we will revise the “Last Updated” date at the top of this Policy. If there are material changes that affect your rights or the way we handle your data, we will take additional steps to inform you, such as posting a prominent notice on our website or emailing you a notification. We encourage you to review this Policy periodically to stay informed about how we are protecting your information. **Your continued use of BOMvault after any update to this Privacy Policy will constitute your acceptance of the changes.**

## Contact Us

Your trust is our priority. If you have any questions, concerns, or requests regarding this Privacy Policy or how BOMvault handles your data, please do not hesitate to reach out to us. You can contact our team at **privacy@bomvault.com**. We will gladly assist you and address any issues or inquiries you may have about your privacy.