

# LinearB AI Features - Security FAQ

March 2025

## 1. Does LinearB use customer data to train its AI models?

No, LinearB **does not** use customer data to train our AI models. We ensure that all customer data remains private and is never incorporated into any training dataset.

## 2. How does LinearB protect my sensitive data when using AI features?

We use **end-to-end encryption** to protect data in transit and at rest. Your data is only processed within secure, compliant environments, and we follow strict **access control policies** to prevent unauthorized access.

## 3. Is LinearB AI compliant with industry standards and regulations like GDPR and SOC 2?

Yes, our AI features are developed in compliance with **GDPR, SOC 2 Type II, DPF, ISO 27001, and other relevant security frameworks**. We ensure all processing adheres to these security and privacy standards.

## 4. Do you keep raw data that was required for generating AI insights?

No, we do not store raw data used to generate AI insights. We **only retain metadata** required for improving accuracy and performance, and even that data is fully anonymized.

## 5. Can I opt out of AI-powered features if I prefer not to use them?

Yes, customers can choose to **disable AI features** in their settings. We believe in giving full control to our users over how AI interacts with their data.

## 6. Where is LinearB's AI processing conducted?

Our AI processing happens in **secure, compliant cloud environments (AWS)**, ensuring data sovereignty and compliance with regional regulations.

## 7. Does LinearB share AI-generated data with third parties?

No, we do not share any AI-generated insights, processed data, or analytics with third parties. Our AI is built with a **privacy-first** approach.

## 8. Which AI infrastructure does LinearB utilize?

LinearB leverages **AWS Bedrock** as our AI provider, ensuring a secure and scalable foundation for our AI capabilities.

## 9. How does AWS Bedrock ensure the security of data processed by LinearB's AI features?

AWS Bedrock provides enterprise-grade security by implementing multiple layers of protection to safeguard data processed by LinearB's AI features. This includes end-to-end encryption, network isolation, and fine-grained access controls to prevent unauthorized access.

Additionally, AWS follows a shared responsibility model, where AWS secures the physical infrastructure, networking, and underlying AI service framework, while LinearB ensures the secure handling of customer data within the application. AWS Bedrock is built on AWS's highly secure cloud infrastructure, which complies with SOC 2, ISO 27001, GDPR, and HIPAA security standards, ensuring that data remains private, encrypted, and protected at all times.

## 10. Is the data processed by AWS Bedrock encrypted?

Yes, data processed by AWS Bedrock is **encrypted in transit and at rest**, with keys managed via AWS Key Management Service (AWS KMS).

## 11. What compliance certifications does AWS Bedrock hold?

AWS Bedrock is compliant with several industry standards, including **ISO, SOC, CSA STAR Level 2**, and is **HIPAA eligible**. Customers can also use Bedrock in compliance with the **GDPR**, ensuring that our AI infrastructure meets stringent security and privacy requirements.

## 12. Are user inputs and model outputs made available to third-party model providers?

No. Users' inputs and model outputs are not shared with any model providers.

## 13. What AI security measures does LinearB have in place?

We employ **real-time monitoring, secure API access, Multi-Factor Authentication (MFA), and continuous vulnerability scanning** to detect and mitigate risks.