LAB FIGURES

Data Security

Last Update: November 21, 2025

Data Handling

Our systems handle various types of data to support our services. For more information about the specific data types we manage, please refer to our Privacy Policy.

Encryption at Rest

All data on our network is encrypted at rest to prevent unauthorized access.

Data stored on AWS is encrypted using the Advanced Encryption Standard (AES-256) which provides robust security.

Any mobile devices (including laptops and mobile phones) accessing our systems are required to have whole disk encryption enabled. This ensures that the entire device's data is encrypted, preventing unauthorized access if the device is lost or stolen.

Data backups are also stored in physically redundant locations to ensure data availability.

Encryption in Transit

Sensitive data transmitted across our network is encrypted using TLS 1.2 and higher, along with strong key and message exchange algorithms. This ensures data is protected when moving between systems and endpoints.

Payment Processing

We use Stripe for all payment processing, ensuring that your transactions are secure and reliable. Stripe is a PCI-DSS Level 1 certified service provider, which is the highest level of certification available in the payments industry. This means that Stripe adheres to stringent security standards to protect your payment information.

For more details on Stripe's security measures, please refer to their Security Policy.

Data Backups

Customer data is backed up daily using snapshot technology. These backups are encrypted with AES-256 and stored in a secondary, geographically separated data center. Backup success is monitored daily, ensuring reliable data recovery if needed.

In addition, our backup systems utilize Amazon S3 and automated daily snapshots that adhere to industry encryption standards.

Audits and Monitoring

We regularly monitor system logs and audit reports, and we review all access attempts to our resources to ensure compliance with security standards and to detect any unauthorized access.

Access Control

Access to sensitive data is restricted based on roles and responsibilities. We enforce multi-factor authentication (MFA) for all users with access to our systems and review permissions periodically to ensure access remains appropriate.

Employee Training

We participate in regular security training to ensure best practices in data handling and system security. Training covers data protection, threat detection, and secure coding practices, ensuring we stay ahead of emerging security challenges.