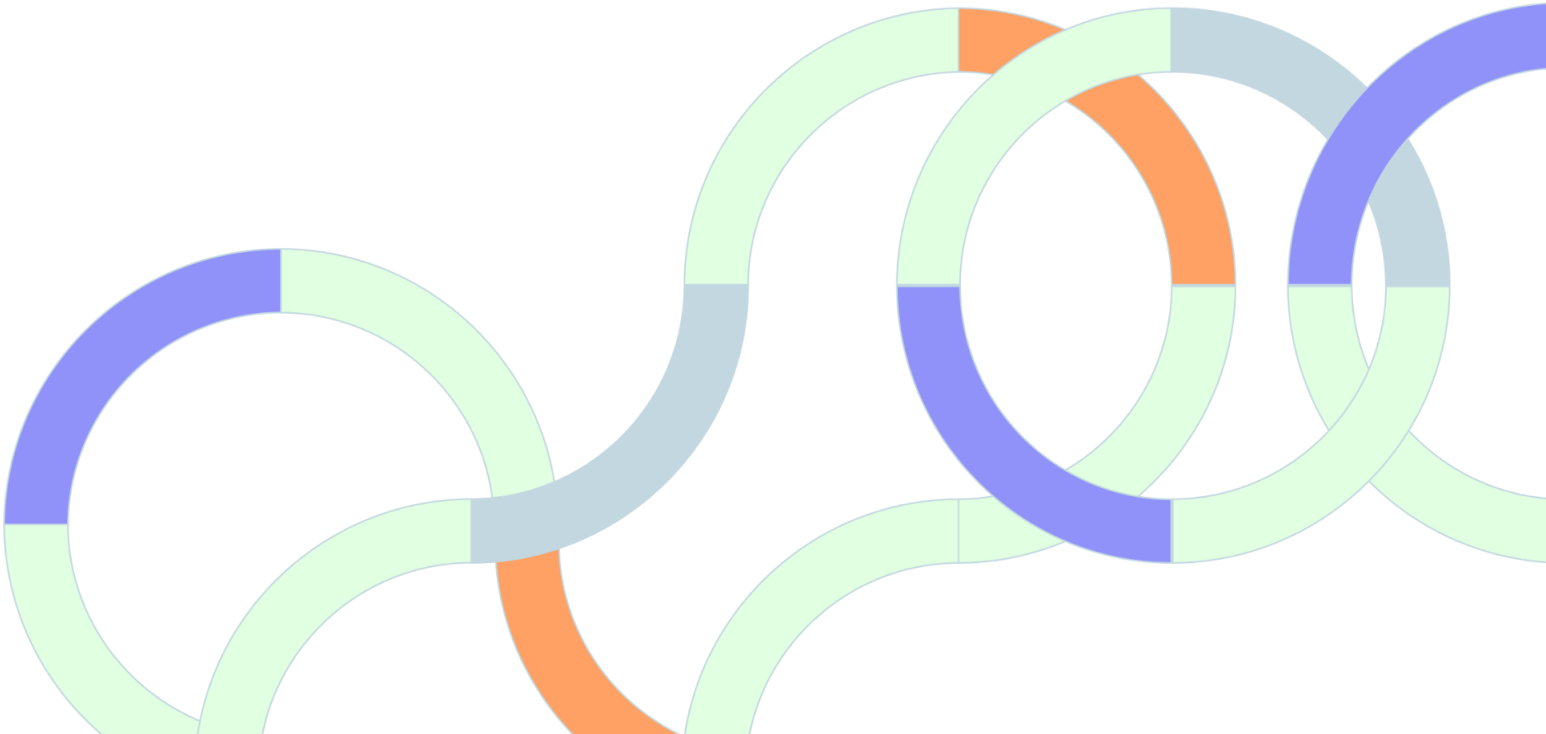
explorium

Security & Privacy - Frequently Asked Questions (FAQ)

Last edited on April 6th, 2025



1. How do you ensure customer data is protected when using AI?

We use a multi-layered security approach, including data encryption (at rest and in transit), role-based access control, and regular security audits to ensure all customer data processed by AI systems is securely handled. Our practices are in line with ISO 27001 and SOC 2 Type 2 standards, ensuring the highest level of data protection.

2. What types of customer data do you collect and how do you ensure it's handled securely?

We only collect the minimal amount of data necessary to provide our services. All data is handled securely through encryption and protected by access controls.

Additionally, we have clear data retention policies to ensure we only keep data as long as needed for legitimate business purposes. For additional information please see the documentation.

3. What security standards does your organization comply with?

We are fully compliant with SOC 2 Type II, ISO 27001, and ISO 27701. Our controls are audited annually by external auditors and aligned with best practices in information security and privacy management.

4. How do you protect customer data?

Customer data is protected using encryption at rest and in transit (AES-256, TLS 1.2+), strict access controls, and data minimization principles.

5. Where is your infrastructure hosted?

We are hosted on AWS US (Amazon Web Services), using its native security services, including AWS Shield, AWS Key Management Service (KMS), and identity management services.

6. Do you monitor your systems for security threats?

Yes, we use centralized logging and real-time monitoring. Alerts are analyzed by our security team and investigated according to our incident response plan.

7. How do you handle access control?

We follow the principle of least privilege. Access to sensitive systems is provisioned only after managerial approval and is subject to periodic reviews. MFA (multi-factor authentication) is enforced for all privileged accounts. In addition we perform user access review at least twice a year.

8. Do employees receive security and privacy training?

Yes. All employees receive mandatory annual security and privacy awareness training, including GDPR fundamentals and data protection best practices. Developers are also trained in secure coding and data handling.

9. How do you ensure privacy compliance (e.g., GDPR, CCPA)?

We have implemented a Privacy Information Management System (PIMS) aligned with ISO 27701. We've implemented policies and processes to ensure compliance and to support data subject rights such as access and erasure.

10. Do you collect and process personal data?

Yes. We process personal data as part of our services, under strict data protection policies. The scope, purpose, and lawful basis for processing are clearly defined and communicated.

11. Can customers request access to or deletion of their data?

Absolutely. We support all data subject rights requests, including access, correction, deletion, and restriction of processing, in accordance with applicable laws such as GDPR and CCPA.

12. What controls are in place for third-party data processors?

All vendors undergo security and privacy assessments before onboarding. We require them to sign Data Processing Agreements (DPAs) and meet our compliance requirements.

13. What happens in the event of a data breach?

Should a data breach occur , we will follow a structured Incident Response Plan, which includes containment, investigation, remediation, and notification. Should personal data be impacted, we will notify the relevant parties in accordance with applicable laws.
We have a dedicated Security & Privacy team that handles all security incidents, ensuring swift and effective resolution in line with our compliance obligations.

14. Where is customer data stored and processed?

Data is stored in AWS data centers located in the US east region. We ensure that data transfers comply with relevant cross-border data protection laws.

15. Do you conduct Data Protection Impact Assessments (DPIAs)?

Yes. DPIAs are conducted for high-risk data processing activities to evaluate potential privacy risks and ensure that appropriate controls are implemented.