YouTrack Cloud for Legal Teams

Data Governance and Compliance Overview

YouTrack

Introduction

JetBrains is committed to providing a high level of security for all services that involve JetBrains hosting its customers' data. We understand that users from the legal industry may be subject to special regulatory or industry requirements to maintain confidentiality when processing sensitive data, and it is important for them to ensure that their data is processed only by services that meet certain high standards. This document describes the data security and privacy measures implemented by JetBrains for the project management tool YouTrack Cloud and how JetBrains meets these standards.

Note: This document applies to YouTrack Cloud instances for which a customer has an active paid subscription (including trial versions). JetBrains may apply different measures for YouTrack Cloud instances used without a paid subscription.

Security measures for legal data storage

Where data is hosted

- **Hosting provider:** YouTrack Cloud instances are hosted by Amazon Web Services (AWS), a trusted and secure infrastructure provider. AWS is a global hosting provider that is regularly audited and holds extensive security certifications including ISO 27001, PCI DSS Level 1 Compliance, SOC2 Certification, and FISMA Moderate Authorization and Accreditation. Users can learn more about AWS security measures and certifications here.
- **Selection of data storage location:** Customers can choose the data center location where their data will be stored from among the following regions: US (Northern California), EU (Ireland), and Asia-Pacific (Singapore).

Encryption

- **Data in transit:** All communication between clients and YouTrack servers are encrypted using up-to-date versions of the TLS protocol. Encryption keys are rotated regularly in accordance with SOC2 and industry best security practices.

- **Data at rest:** Stored data is encrypted using Chacha20 (AEAD) to prevent unauthorized access and ensure confidentiality.

Access controls

- **Role-based access:** Access is strictly enforced based on roles, ensuring only authorized personnel can access sensitive information.
- **Access reviews:** Regular access reviews are carried out in accordance with SOC2 and industry best security practices.
- **Multi-factor authentication (MFA):** MFA adds an additional layer of security to user accounts.
- **Audit logs:** Detailed logs of access and changes are maintained, supporting accountability and traceability.
- **SIEM:** SIEM capabilities are utilized to centrally manage logs and security events.

Isolation of data

- Segregation of data ensures that client information remains isolated from other tenants, protecting against unauthorized cross-access.

Data retention

Backups: Daily backups are retained for seven days, weekly backups for three weeks, and monthly backups for eleven months. Customers can create a backup copy of their database in YouTrack Cloud and download the archive to migrate it to a self-hosted YouTrack Server installation at any time.

Organizational and technical safeguards

Organizational safeguards

- **Dedicated Security team:** The team oversees the implementation and monitoring of security policies.
- **Confidentiality agreements:** All employees and subprocessors with access to sensitive data are bound by confidentiality obligations.

- **Incident management:** JetBrains has robust processes to detect, mitigate, and report data breaches promptly.

Technical safeguards

- **Secure software development life cycle (SSDLC):** JetBrains has appropriate processes to ensure security at all stages of the software development life cycle, including code reviews and approvals, security audits of product features, and security measures during the deployment stage.
- **Regular security audits:** Penetration tests and vulnerability assessments ensure that systems remain secure.

Alignment with technical standards

- **SOC 2 standards:** JetBrains is aligned with the five trust service criteria – security, availability, confidentiality, processing integrity, and privacy.
- **Data minimization and purpose limitation:** Only necessary data is processed, with strict controls on access and usage.

Compliance and contractual commitments

Personal data protection

- JetBrains is a company established in the European Union, and therefore it is directly subject to the strict obligations imposed on data processors by the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).
- YouTrack Cloud Terms of Services incorporate by reference the JetBrains Data Processing Addendum that outlines clear commitments to personal data protection, including confidentiality obligations for employees and subprocessors and notification of data breaches.

Third-party requests

- Requests for access are strictly scrutinized, with a commitment to challenge unlawful or overreaching demands.

Commitment to continuous improvement

JetBrains is committed to maintaining high-security standards for all hosted services, including YouTrack Cloud. We recognize that legal teams must meet strict regulatory and industry requirements for handling sensitive data.

To support this, we conduct regular reviews of security policies and compliance measures and invest in advanced technologies to enhance data protection. This document outlines the security and privacy measures in place to ensure legal teams can confidently manage their workflows in YouTrack Cloud.

References

- JetBrains GDPR and Security Compliance
- Data Processing Addendum (DPA)
- JetBrains Trust Center