# INFORMATION SECURITY FAQS

A comprehensive guide to our security frameworks and protocols




trint

# CONTENTS

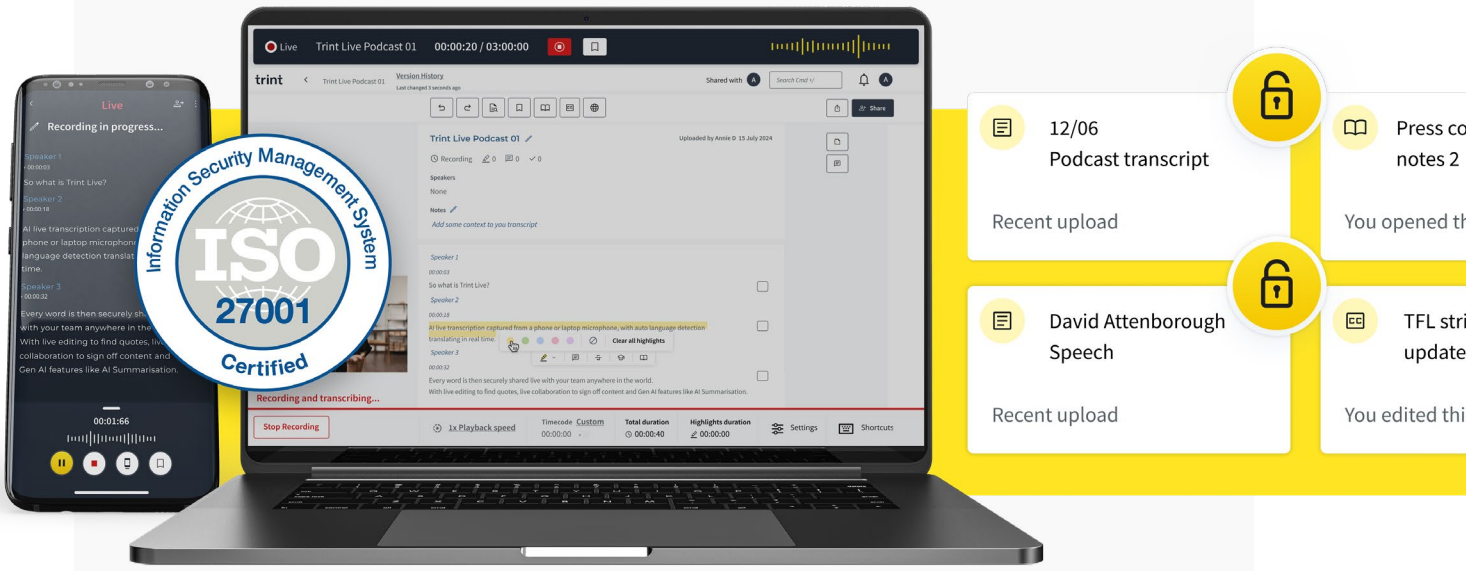

Data privacy 3

Data processing 6

Access control 9

Audit and security reviews 12

Artificial Intelligence 14

# DATA PRIVACY



**Does Trint encrypt all data? If keys are used, who holds the keys?**

Data is encrypted in transit using TLS 1.3 or later, and at rest using AES 256. Keys are stored and managed by AWS, but are controlled by Trint.

**Does Trint have backup, storage and restoration procedures? How long are backups retained? And are the backups encrypted?**

Our cloud database takes incremental snapshots enabling us to continuously back up customer data and allow point in time recovery for one week. Daily, weekly and monthly snapshots are taken and held for up to one year. Snapshots are duplicated offsite from the DaaS provider for business continuity purposes.

Database recovery tests occur once per quarter.

Customer content is stored in AWS S3 with version control enabled. The data is replicated over at least three of the Availability Zones in the region. AWS states a durability of 99.999999999%, and availability of 99.99% over a given year. No additional backup is made of this data.

All data at rest is encrypted with AES 256.

**Can any third party access customer content and, if so, how?**

Trint uses third parties to provide the service:

Trint services run inside Amazon AWS, with Trint customer content stored in encrypted AWS S3 buckets.

Trint uses a cloud-based database within the MongoDB Atlas service to store customer transcriptions in encoded documents with full encryption at rest and in transit.

UploadCare is used for file transfer services; when files are uploaded via the Trint app they will go directly from the User to Trint. However, uploaded media may pass via UploadCare if transferring directly from a cloud storage provider (e.g. Dropbox or Google Drive).

For a complete list of Trint sub-processors, please see **here.**

**Will customer data be permanently erased from the solution, including any backup storage, when this data is deleted or the service ended?**

A monthly secure deletion request can be arranged via your Customer Success Manager at Trint. As the client, your content will be removed from AWS S3, and data will be removed from the database.

Database backups may retain content metadata (filename, excerpt, media type, duration, file size) for up to a year.

Trint can check the database and S3 for the files that were removed and validate that they are missing. We can also search the secure deletion log with the status of each file that has been queued for deletion.

**Is verification provided that data has been securely deleted?**

Yes, via your Trint Customer Success Manager.

**Are third party vulnerability assessments conducted on the applications processing customer data? What is the frequency of these assessments?**

A thorough vulnerability assessment is performed once a year by a well-established software security auditing company. In addition, we continuously run a Vulnerability Program Disclosure via a security testing platform. A summary of this report can be provided under NDA.

**Is "Enforced TLS" the default standard for outgoing Trint emails?**

Trint does not transmit our customers' data via email.

TLS is enforced as default, while our email domain is configured with DMARC.

**Is an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) deployed and monitoring all traffic?**

We use AWS Guard Duty for anomaly detection and alerting, and AWS WAF for request filtering and rate limiting.

# DATA PROCESSING

12/06
Podcast transcript

Recent upload

David Attenborough
Speech

Recent upload

David Attenborough
Speech

Recent upload

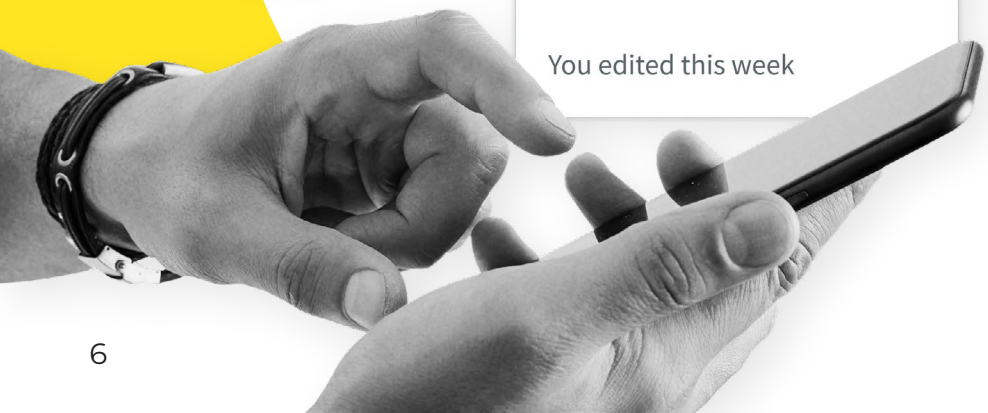
Press conference
notes 2

You opened this week

TFL strike coverage
updated

You edited this week

Information Security Management System
ISO
27001
Certified



**Is any sensitive personal data being processed?**

Trint does not process sensitive information as a Data Controller.

Customers may upload media that contains sensitive personal information that Trint processes as a Data Processor on behalf of the customer. Trint has no visibility or control over this data. Trint does not access customer content without the prior written consent of the customer unless required by local law. Customers will be notified prior to execution of such a request.

**With regards to sub-contractors that hold customer data, how does Trint ensure that they meet the required information security standards?**

All of Trint's suppliers are subject to a Vendor Security Assessment process as per our ISO approved Information Security Management System (ISMS). Vendors are required to meet or exceed Trint's own security standards for the type of data processed.

For more details, ask a member of the Trint team.

**How does Trint comply with cross-border data transfer requirements**

Trint is GDPR compliant and asserts Standard Contractual Clauses in our enterprise contracts.

For data transfer and storage, Trint uses HTTPS (using TLS 1.3+) for secure data upload, export and transfer.

**Why does Trint need to collect personal data or sensitive personal data?**

This is for the provision of user accounts.

**Has Trint provided a Privacy Notice?**

Trint has a platform privacy policy that can be viewed here and a website and marketing policy that can be viewed here. If you have any questions, please contact a member of the Trint team.

**What access do Trint developers have and what training do they receive to ensure security standards?**

Trint is designed and built with security in mind. Trint uses the principle of least privilege. Our Developers are required to undertake OWASP and other security training on an annual basis.

**What is Trint's retention policy for data processing?**

Trint keeps all client content for the lifetime of the contract and deletes it within 6 months of contract end. Other personal data may be retained longer for auditing. Secure deletion can be arranged at contract termination or once per month upon request. All data is stored in the cloud and securely destroyed at end-of-life.

**Where is the data stored?**

Data is stored in AWS systems comprising the Trint Platform, specifically in AWS data centers located in either the EU/Dublin or US/Virginia, depending on the tenant. Data is spread over multiple availability zones for resilience.

**Does Trint have the ability to promptly delete or provide information on a specific individual on instruction from the customer?**

Administrators appointed by the customer can view activity and remove users from the organization within the admin dashboard.

Secure deletion of customer content and user accounts can be performed by Trint upon request once per month.

**How is the data transferred?**

In all cases, data is transferred over a TLS v1.3+ encrypted connection.

# ACCESS CONTROL



**What is the process for mutual authentication on sending API commands?**

An API key will be generated by the customer, which is used to authenticate the calling user.

The server is authenticated by use of a TLS v1.3+ connection and the certificate obtained during the connection.

**Does the service allow for a login federated IDM infrastructure? Does your service support SAML or ADFS for Single Sign-On (SSO)?**

SAML based SSO integrations are possible.

**Does Trint log and audit staff's privileged access and activities?**

Yes. All access and changes in the platform are logged using AWS CloudTrail.

**How is customer data kept logically and/or physically separated from other users' data?**

Data stored is kept in per user file system containers. Processing of data occurs in single use container instances that are destroyed upon completion.

**Is there multi-factor authentication (MFA) implemented for user access?**

Trint does not currently provide MFA. It is recommended that enterprise customers enable an SSO integration allowing them to enforce their own security standards for authentication and authorization.

**What happens if an access violation is identified?**

For access violations identified, customers can provide the documented process for remediation that is followed. Our Information Security Incident Response Procedure would be followed.

**Is remote access allowed for employees, contractors and / or agents?**

Trint Engineers can access the cloud environment, with access policy based on the least privilege principle.

**What levels of user access are available? What reports are available?**

The fine-grained controls within our Workspaces include:

- **Add Workspace members**
- **Archive Workspace**
- **Can access Workspaces**
- **Comment on Trints**
- **Create folders**
- **Edit folders**
- **Edit Trints**
- **Edit Workspace members**
- **Edit Workspaces**
- **Remove Workspace members**
- **Share transcripts with the public**
- **Share transcripts with users outside the Workspace**
- **Upload to Workspace**

Predefined roles and custom roles comprised of these are available.

Usage reports are available upon request or via the admin dashboard (exportable as CSV).

**How are the accounts with the highest level of privilege authenticated and managed?**

Access to the AWS root account is restricted. All access to the platform is controlled using time-limited credentials authorized by Google Workspace SSO and group membership, which in turn relies on Multi-factor authentication.

**Will any form of remote access technology be required and, if so, what? Does this include two factor authentication?**

The customer's users access the platform using a web browser, desktop app, mobile app or via the API where an automated process is integrated. Trint can also be accessed on mobile or a desktop app now too.

# AUDIT & SECURITY REVIEWS



**What scanning and testing processes, if any, does Trint perform, and at what frequency? How does Trint resolve issues identified through such testing?**

Penetration testing is currently performed annually by a third party - currently CyberArmed. The last test was performed in June 2025. The report is available under NDA (though a limited executive summary is available on request without an NDA required). Trint runs a Vulnerability Disclosure Program for the responsible disclosure of issues identified outside of penetration testing.

**Do you (or a third party) conduct internal audits regularly?**

Our internal audit program conducts targeted annual assessments of key information security controls.

**Has Trint undergone an independent review of information security (example: ISO 27001, SOC 2 Type 2, PCI, etc)?**

Trint holds ISO 27001 certification which is audited by an external team annually. Please reach out to a Trint team member if you need a copy of this certificate.

**Do Trint (or a third party) conduct external audits regularly?**

External audits of Trint's ISO 27001 ISMS are performed annually.

**Have all relevant statutory, regulatory, contractual requirements (including: intellectual property rights, protection of records, protection of personally identifiable information and cryptographic controls), and your approach to meet these requirements, been explicitly identified, documented and kept up to date for the customer?**

As part of our ISO ISMS, Trint reviews all legal, regulatory and contractual requirements relevant to our business operations.

**Is your ISMA (i.e. control objectives, controls, policies, processes and procedures for information security) reviewed and inspected for compliance, independently at planned intervals, or when significant changes to the security implementation occurs?**

We conduct both internal and external audits on an annual basis.

**Has an internal audit group performed a formal information security assessment of your environment?**

Yes. Our internal audit team has performed a formal information security assessment as required under our ISO 27001 audit program.

# ARTIFICIAL INTELLIGENCE



### What data is used for features powered by AI at Trint?

Trint securely stores and processes data you provide us to enhance your workflow. While we use media content and metadata to support AI-powered transcription and other features, your data is not used to train or improve our AI models.

To learn more about how Trint processes your information, please see Trint's Privacy Policy.

### Does Trint use OpenAI or external AI models?

Trint does not use OpenAI or other third-party AI models [for external processing]. We develop and deploy all AI features in-house within Trint's secure infrastructure, meaning no customer data is shared externally for AI processing. [Third party incorporated]

### How does Trint optimise AI usage?

All AI processes are run exclusively within Trint's infrastructure. This setup allows us to provide consistent, reliable services without compromising data security or sharing customer data outside our platform.

### What safeguards does Trint have in place for AI usage?

Trint implements several safeguards for responsible AI usage:

- **No training on your data:** We do not use your data to train or improve Trint's AI models.
- **Data deletion:** Your data is not stored whilst being processed by our ephemeral systems and any content created is encrypted and securely stored.
- **AI content transparency:** Our platform clearly indicates when content is AI-generated and when it has been reviewed and verified by a human.

### Your responsibilities as a user when using AI-powered tools?

While Trint provides a range of AI tools to assist you in verification and cross-checking. We recommend verifying all AI outputs before making any decisions, taking actions, or relying on it for critical decisions. Where appropriate, let others know when you're using or presenting AI-generated content and whether it has been reviewed, cross checked and verified.

### Active Session Responsibility

When using Live features or real-time transcription, you are responsible for managing active sessions. This includes starting and stopping recordings as required and reviewing the captured content to ensure it aligns with your intent. Failure to end a recording promptly may capture unintended conversations, which could lead to sensitive content being transcribed and shared. Trint is not liable for any issues arising from users' failure to manage session controls.

### What features are powered by AI?

Trint's AI supports multiple features, including:

- **Automated transcription** of audio and video content.
- **Enhanced editing and summarisation** tools.

- **Speech alignment**, enabling accurate transcript generation.
- **AI Assistant**, helping you realise efficiencies in your workflow.

These features are designed to improve productivity while ensuring a high level of data security.

### What data does Trint's AI Assistant have access to?

As a user, you will only be able to ask questions about files that your user has valid access to:

The content of files will only ever be securely and temporarily accessed at the point you ask a question relating to a file, until a response is generated.

Any questions you ask or generated responses are treated with the same high level of data protection that we already follow for the media content itself.

For more information on this, please see Trint's Terms and Conditions here and the Platform Privacy Policy here.

### How does Trint address AI bias?

Trint strives to ensure that our AI serves everyone equally, regardless of accent, dialect, age, gender or location. Our training models are designed with diverse data exposure to reduce AI bias, and we continuously monitor AI performance to uphold this standard.

At Trint, we believe that working in diverse teams is critical in us thinking and doing better. It also means we have a broader mindset in working with and understanding each other. It's the same for AI and ML. Therefore, we ensure our training models are exposed to a different variety of voices and this is critical for reducing AI bias. With the Autonomous Speech Recognition (ASR) Trint currently uses, self-supervised learning was introduced into its training. More data is now used efficiently and the results have been extraordinary at reducing AI Bias.

### Who owns the IP in the AI and the output?

All content and data uploaded by users, including outputs generated by Trint's AI features, remain the intellectual property of the user, subject to any applicable fees and terms in our agreement with you. Trint retains ownership of its proprietary AI models, algorithms, and associated technology used to generate these outputs. Using the Trint Platform does not grant users any rights, title, or interest in Trint's underlying AI technology or IP.

trint

If you have any questions regarding this guide, please contact your Trint representative or email us at support@trint.com.