

EchoSpan Customer Data & Controls Overview

Overview

EchoSpan is designed to support secure, controlled, and privacy-conscious use of customer data within its 360 feedback platform. Because the platform is often used to collect employee feedback, performance-related comments, and organizational review data, EchoSpan provides customers with a range of privacy, access, retention, and feature-level controls intended to limit unnecessary data exposure and support responsible administration of feedback programs.

This document summarizes the data privacy and customer control features available within EchoSpan's platform. It is intended to help customers, procurement teams, privacy teams, and security reviewers understand how EchoSpan limits the use of customer data, supports customer control, and reduces unnecessary data processing.

Customer Data Ownership

Customer data stored in the EchoSpan system remains the property of the customer. EchoSpan processes customer data only as necessary to provide the services, support authorized users, generate reports, deliver configured review workflows, and provide optional platform features requested or enabled by the customer.

EchoSpan does not:

- Sell customer data
- Share customer data for advertising purposes
- Use customer data to create external benchmarking studies, industry-wide comparisons, or aggregated commercial datasets.

Data is processed only for the purposes associated with providing and supporting the EchoSpan platform.

Types of Data Processed

Depending on the configuration selected by the customer, EchoSpan may process the following types of data:

- Employee or participant names
- Work email addresses
- Organizational or reporting relationships
- Review assignments
- Feedback ratings
- Written comments
- Review status information
- Administrative user information
- Survey or review configuration data
- Generated reports and exports
- Usage and system activity logs

EchoSpan does not require customers to collect sensitive personal data through the platform. Customers are responsible for determining the content of their review programs, including the questions asked and the type of information requested from participants. EchoSpan recommends that customers avoid requesting sensitive personal data unless they have determined that such collection is lawful, necessary, and appropriate for their intended use.

Customer Configuration and Data Minimization

EchoSpan supports customer-controlled configuration of review programs. Customers can limit the data collected by determining which employees participate, what information is uploaded, what questions are asked, what reports are generated, and which administrative users have access.

Customers may configure review projects to use only the data necessary for the intended feedback process. In many cases, the platform can operate using a limited data set consisting primarily of participant names, work email addresses, review assignments, and feedback responses.

Customers can also limit access to optional features, including AI-assisted features, advanced reporting, and administrative functions. This allows customers to align platform usage with their internal privacy and security requirements.

Access Controls

Access to customer data within EchoSpan is controlled through user roles and account permissions. Users may only access the portions of the system made available to them based on their assigned role.

Common access levels include:

- End users, such as feedback providers (raters) or other review participants
- Targets or employees receiving feedback
- Client administrators
- Client sub-administrators
- EchoSpan support or administrative personnel with authorized access

Client administrators control many account-level and project-level settings, including the assignment of users, review workflows, and access for sub-administrators.

Administrative access is intended to be limited to individuals with a legitimate business need. EchoSpan recommends that customers regularly review their administrative and sub-administrative users to ensure access remains appropriate.

Client Sub-Administrator Controls

EchoSpan supports client sub-administrator roles that allow customers to delegate limited administrative access without granting full account control. This helps customers manage internal responsibilities while maintaining appropriate separation of duties.

Sub-administrator access can be enabled, disabled, or modified by authorized customer administrators. EchoSpan's platform can also support periodic reminders for customers to review sub-administrator access.

Authentication and Session Controls

EchoSpan supports secure authentication and session management controls. Depending on account configuration, users may authenticate through standard login credentials or single sign-on.

Default session controls include session timeout after inactivity and account suspension after repeated failed login attempts. These controls are designed to reduce the risk of unauthorized account access.

Single sign-on may be supported for customers that require centralized identity management. Where SSO is configured, authentication is managed through the customer's identity provider and integrated with EchoSpan's access controls.

Encryption

EchoSpan uses encryption to protect customer data in transit and at rest.

Data transmitted between users and the EchoSpan platform is protected using encrypted HTTPS connections. Data stored within EchoSpan's database environment is protected using encryption at rest, including Azure-managed encryption technologies.

Backups and other stored system data are also protected using encryption mechanisms appropriate to the hosting environment.

Data Retention

EchoSpan retains customer data only as necessary to provide the services, support customer accounts, maintain system integrity, and comply with applicable legal or contractual obligations.

Customer data is generally retained for the duration of the customer's active subscription. Upon account expiration or termination, personal data associated with the account is removed in accordance with EchoSpan's standard retention practices, subject to backup retention periods and any applicable legal obligations.

EchoSpan's standard posture is to avoid retaining personal data longer than necessary for the purpose for which it was collected.

Data Deletion

Customers may request deletion of personal data in accordance with applicable law, contractual terms, and platform capabilities. EchoSpan supports deletion and removal processes for personal data stored within customer accounts.

Where an individual data subject submits a request directly to EchoSpan regarding customer-controlled data, EchoSpan may direct the request to the applicable customer unless applicable law requires otherwise. This reflects EchoSpan's role as a processor or service provider acting on behalf of the customer.

Backup copies may persist for a limited period after deletion from active systems, consistent with standard backup and disaster recovery practices. Backup data is protected and retained only for continuity and recovery purposes.

Data Subject Rights Support

EchoSpan assists customers, to the extent reasonably practicable, in responding to data subject requests under applicable privacy laws. These requests may include access, correction, deletion, or other rights recognized under GDPR, CCPA/CPRA, or similar laws.

Because EchoSpan generally acts as a processor or service provider for customer-controlled data, customers remain responsible for determining how to respond to data subject requests. EchoSpan supports the customer's response where the requested data resides within the EchoSpan platform.

No Sale or Sharing of Personal Data

EchoSpan does not sell customer personal data, share customer personal data for cross-context behavioral advertising and will never use customer personal data for unrelated commercial purposes.

Where applicable under CCPA/CPRA, EchoSpan acts as a service provider and processes personal data only for permitted business purposes associated with providing the EchoSpan platform and related services.

No Customer Data Benchmarking

EchoSpan does not use customer data to create aggregated benchmarking databases, industry trend reports, comparative analytics products, or commercial datasets.

Customer feedback data is not pooled with data from other customers for benchmarking or resale.

This is an important distinction for organizations using 360 feedback data, as feedback content may be sensitive, context-specific, and intended solely for internal development or review purposes.

AI Feature Controls

EchoSpan offers optional AI-powered features that may support functions such as feedback writing assistance, comment summarization, report drafting, performance note summarization, or other customer-enabled functionality.

AI features are optional and can be enabled, disabled, or restricted depending on customer preference and account configuration.

Customers that do not wish to use AI-powered features may restrict access to those features at the account level.

How EchoSpan Uses AI Providers

When AI features are enabled, EchoSpan may transmit limited customer-provided text or context to an AI service provider, such as OpenAI, through secure server-side API calls.

The data transmitted is limited to the minimum necessary to provide the requested AI function. For example, if a user asks the platform to improve or summarize a written feedback comment, the relevant text may be transmitted to the AI provider to generate the requested output.

Users do not interact directly with the AI provider. AI functionality is embedded within the EchoSpan platform and remains subject to EchoSpan's authentication, authorization, and session controls.

No AI Model Training on Customer Data

EchoSpan does not permit customer personal data to be used to train publicly available AI models.

Customer data submitted to AI service providers is used only to generate the requested output for the specific customer-authorized function.

EchoSpan does not use customer data to train, fine-tune, or improve public AI models.

AI Data Minimization

EchoSpan's AI implementation is designed around data minimization. Only the content needed to perform the requested AI function is transmitted for processing.

EchoSpan does not send broader customer datasets, account credentials, unrelated employee records, or unnecessary account-level information to AI providers as part of ordinary AI feature use.

Customers should avoid entering sensitive personal data into AI-enabled features unless they have determined such use is appropriate for their organization and permitted under applicable law and policy.

AI Output and Human Review

AI-generated content should be reviewed by users before being accepted, used, or distributed. EchoSpan's AI features are intended to assist users, not replace human judgment.

AI outputs may include summaries, suggested wording, drafted language, or analytical assistance. Customers remain responsible for determining how AI-assisted content is used within their organization.

EchoSpan's AI features are not intended to make automated employment decisions, determine employment eligibility, rank employees for employment action, or replace human review in performance management decisions.

AI Feature Risk Posture

EchoSpan's AI features are assistive and user-directed. They are designed to help users draft, summarize, organize, or improve feedback-related content.

The platform does not use AI to make autonomous employment decisions. It does not independently decide promotions, compensation, terminations, disciplinary actions, hiring outcomes, or other employment determinations.

Because the features are optional, assistive, and subject to customer control, EchoSpan does not view its AI functionality as a high-risk automated decision-making system when used as intended.

Customers should evaluate their own use of AI features based on their internal policies, applicable law, and intended deployment.

AI Customer Controls

Depending on account configuration and subscription features, customers may be able to:

- Disable AI functionality
- Restrict AI access to specific users or roles
- Limit use of AI features to specific workflows
- Control whether AI-generated content is included in reports or summaries
- Review AI-generated content before use
- Apply internal policies governing acceptable AI use

These controls allow customers to align EchoSpan's AI functionality with their organization's privacy, security, and governance requirements.

Subprocessors

EchoSpan uses a limited number of subprocessors to support delivery of the platform. These may include providers for cloud hosting, database infrastructure, payment processing, AI processing, and related operational services.

Subprocessors are used only as necessary to provide, support, secure, or improve the EchoSpan platform.

EchoSpan requires subprocessors to maintain appropriate security and privacy protections consistent with their role and the nature of the data processed.

Current subprocessors are disclosed through EchoSpan's Trust Center or made available upon request.

Customer Data Isolation

EchoSpan is a multi-customer SaaS platform designed to maintain logical separation between customer accounts. Customer users and administrators are restricted to the data associated with their own account and authorized projects.

Role-based access controls, account-level permissions, and application-level data restrictions are used to prevent unauthorized access across customer accounts.

EchoSpan does not make one customer's data available to another customer.

Administrative Access by EchoSpan Personnel

EchoSpan personnel may access customer data only when authorized and only for legitimate business purposes, such as support, troubleshooting, implementation, security review, or maintenance.

Access to production systems and customer data is limited to personnel with appropriate responsibilities and business need.

EchoSpan personnel are subject to confidentiality obligations and internal security policies.

Logging and Monitoring

EchoSpan maintains logs and monitoring processes to support security, availability, troubleshooting, and auditability. Logs may include system activity, authentication events, application events, error reporting, report generation activity, and other operational information.

Logs are protected from unauthorized access and are reviewed or investigated as needed based on alerts, suspected incidents, support requests, or operational requirements.

Incident Response

EchoSpan maintains an incident response process for suspected or confirmed security or privacy incidents. The process includes internal reporting, investigation, containment, remediation, documentation, and customer communication where appropriate.

If EchoSpan becomes aware of a confirmed personal data breach affecting customer data, EchoSpan will notify the affected customer without undue delay and in accordance with applicable contractual and legal obligations.

Customers remain responsible for determining any regulatory or data subject notification obligations applicable to their own organization, unless otherwise required by law.

Customer-Controlled Review Content

EchoSpan provides a configurable platform. Customers control the content of review questions, the scope of review projects, the users invited to participate, the reports generated, and the individuals who receive report access.

Because customers control review design and administration, customers are responsible for ensuring their use of the platform complies with internal policies, employment laws, privacy obligations, and other applicable requirements.

EchoSpan recommends that customers avoid collecting sensitive personal data unless such collection is necessary and properly authorized.

Anonymity and Confidentiality Options

EchoSpan supports review configurations intended to protect feedback confidentiality and limit unnecessary attribution. Depending on the review design and reporting configuration, customers may configure how feedback is presented, aggregated, or attributed.

Anonymity and confidentiality settings should be selected based on the customer's review objectives, internal policies, and privacy requirements.

Because 360 feedback often involves small groups, customers should carefully consider whether comments or ratings could indirectly identify a respondent even where names are not displayed. EchoSpan can support privacy-conscious reporting practices, but customers are responsible for determining the appropriate review design for their organization.

Reporting and Export Controls

EchoSpan provides reporting and export functionality to support customer review workflows. Reports and exports may contain personal data, ratings, written comments, and other feedback-related information.

Access to reports and exports should be limited to authorized customer administrators or other approved recipients.

Customers are responsible for controlling distribution of downloaded reports and exports once they leave the EchoSpan platform.

Data Quality and Integrity

EchoSpan maintains processes and tools designed to support data quality, report accuracy, and system integrity. These may include internal checks, report monitoring, error alerts, and administrative review processes.

Where a data quality issue is identified, EchoSpan investigates and remediates the issue as appropriate and communicates with affected customers when necessary.

Business Continuity and Disaster Recovery

EchoSpan maintains business continuity and disaster recovery processes designed to support availability and data integrity in the event of a disruption.

Backups, monitoring, recovery procedures, and periodic testing support EchoSpan's ability to restore critical services following a significant outage or incident.

Additional information is available in EchoSpan's Business Continuity and Disaster Recovery materials.

Security Documentation and Review

EchoSpan provides standardized security, privacy, and compliance materials through its Trust Center. These materials are designed to support customer due diligence and answer common procurement, legal, and security questions.

Available materials may include:

- Security Overview
- Data Processing Addendum
- Business Continuity and Disaster Recovery Summary
- Subprocessor Summary
- Privacy Policy
- Penetration Testing Summary, where available
- Microsoft Azure Trust Center link
- AI and Data Privacy information

For standard deployments, EchoSpan uses its established documentation and does not typically support extensive customization of legal agreements or completion of large enterprise-specific security frameworks.

Where a customer has specific concerns that are true blockers, EchoSpan is willing to review those concerns individually and determine whether they can be addressed within EchoSpan's standard framework.

Practical Privacy Commitments

EchoSpan's data privacy approach is grounded in the following principles:

- Customer data belongs to the customer.
- Customer data is processed only to provide the services.
- Customer data is not sold.
- Customer data is not used for advertising.
- Customer data is not used for public AI model training.
- Customer data is not used for external benchmarking.
- AI features are optional and controllable.
- Access to customer data is restricted based on role and business need.
- Customer data is protected through encryption, access controls, monitoring, and documented processes.
- Customers retain control over review design, user access, reporting, and data use within their organization.

Contact

For questions about EchoSpan's data privacy controls, security documentation, or Trust Center materials, please contact support@echospan.com.