VoicePing Enterprise Security Questionnaire

Voice Translation & Virtual Office | Enterprise evaluation

Overview	Guidance
Scope	This questionnaire covers VoicePing Voice Translation and Virtual Office. Assess live and event translation, Meeting Bot, File Transcribe, Meeting Logs, collaboration and Time Tracking according to the features used. Mobile offline translation runs on the device. Dedicated environments and on-premises configurations require individual confirmation.
Basis of answers	The answers describe specifications and policies supported by public documentation. Applicability depends on the plan, features and settings in use. Items requiring further detail are marked 'Confirm individually' and must be confirmed in accordance with the applicable agreement.
Documented	The specification or policy is supported by public documentation.
Conditional	Conditions depend on the plan, feature, configuration or agreement.
Confirm individually	This document alone cannot establish a definitive answer; individual confirmation is required.
Points to assess	The primary cloud infrastructure is in Tokyo, Japan. AI processing, content delivery and notification integrations can involve processing outside Japan. Assess the policy against using customer audio and transcripts for AI model training separately from whether data is sent to external services. Authentication and access restrictions depend on the plan and user role. Confirm the required settings before deployment. Confirm retention and deletion by data type. When using presence history, tracked time or optional image capture, review participant notices and collection and viewing settings.
How to use this PDF	Review the questions by category and confirm the features and agreement that apply to your deployment. Please contact us with any follow-up questions.

Total questions	Documented	Conditional	Confirm individually
114	31	34	49

These counts describe response categories. They are not a security score or a certification of every control.

Products and applicable features

Product / feature	Scope and assessment focus
Live Translation	Transcribes and translates in-person or online speech. Check audio sources and the audience for captions and translated speech.
Event Translation	Distributes captions and translated speech to event listeners. Check listener links or QR codes, optional passwords and event usage terms.
Meeting Bot	Joins supported Zoom, Google Meet and Microsoft Teams calls. Assess host admission, optional calendar connections and record sharing.
File Transcribe	Processes uploaded audio or video into transcripts, translations, subtitles and dubbing where supported. Assess both uploaded files and generated outputs.
Meeting Logs	Reviews and shares conversation records and file-processing results from enabled features. Assess retention, visibility, exports and API or MCP access.
Virtual Office	Combines presence, floors and meeting rooms, calls, translation and shared work tools. Check member and guest access and shared-content audiences.
Time Tracking	Records project time and work memos. Desktop screenshots, webcam snapshots and input activity are optional controls that require separate configuration review.
Offline Translation	Transcribes and translates on a mobile device after models are downloaded. Assess local records, deletion and device handling separately from cloud features.

Assess only the features used in your deployment. Availability, limits and settings depend on the applicable plan and agreement.

Governance and certification

Item	Question	Response	Answer
GOV-01	Are the provider and services clearly identified?	**Documented**	VoicePing Inc. provides Voice Translation and Virtual Office, including transcription and summaries, file processing, collaboration and time tracking. Identify the products, features and plan covered by your agreement.
GOV-02	Does the provider hold an information security certification?	**Documented**	Official documentation states that VoicePing has obtained ISO/IEC 27001:2022 certification. This certification concerns the organization's information security management system.
GOV-03	Can the scope and validity of the certification be confirmed?	**Confirm individually**	The certification scope and current validity require individual confirmation against the latest documentation.
GOV-04	Can third-party assessments be confirmed?	**Confirm individually**	Please contact us individually regarding the status of third-party assessments and the availability of supporting documentation.
GOV-05	Are additional assurance reports or certifications available?	**Confirm individually**	Confirm individually whether a SOC 2 assurance report, PrivacyMark certification or other relevant material is available and current.
GOV-06	Are security policies and management responsibilities defined?	**Confirm individually**	Please contact us individually for details of security policies and management responsibilities.
GOV-07	Are risk assessments and asset management performed?	**Confirm individually**	Details of risk assessment and asset management require individual confirmation for the agreed scope.
GOV-08	Is employee security awareness managed?	**Confirm individually**	Please contact us individually for details of security management relating to employees.
GOV-09	Can the security management evaluation framework be confirmed?	**Confirm individually**	Please contact us individually regarding the framework for evaluating security management and the methods available to confirm it.
GOV-10	Are confidentiality obligations defined for employees and service providers?	**Documented**	Public policies and contractual documents establish confidentiality obligations for people handling personal data and data protection obligations for subprocessors. Customer-specific nondisclosure agreements are subject to confirmation of the applicable plan and contract terms.
GOV-11	Can customer questionnaires, supporting documents and customer audits be accommodated?	**Conditional**	Security questionnaires, document requests, nondisclosure agreements and customer audits are coordinated after confirming the applicable plan and contract terms. Please share any additional questions with us.
GOV-12	Is compliance with all laws and standards guaranteed?	**Confirm individually**	A privacy policy is publicly available. Compliance with industry-specific standards, GDPR, healthcare requirements and financial-sector requirements must be assessed individually according to the regions and data involved. Certification alone does not establish compliance with every law or industry standard.
GOV-13	Can the applicability of information security controls be confirmed?	**Confirm individually**	Please contact us individually regarding the scope of applicable controls and the availability of detailed documentation.
GOV-14	Can supplier and service-provider management be confirmed?	**Confirm individually**	Please contact us individually for details of supplier and service-provider selection and management.

Data protection and privacy

Item	Question	Response	Answer
DAT-01	What types of data are processed?	**Documented**	Depending on the features used, data includes account details, audio or video, transcripts, translations, summaries, shared content and IP or device information. Virtual Office can also involve presence and history, work memos and time, and optional images or input activity. Collection depends on enabled features and settings; see USE-14 for optional capture.
DAT-02	Are the purposes and roles for processing customer data clear?	**Documented**	Customer content is processed according to the customer's instructions. Account administration, billing, support and security operations have separately defined purposes. See the privacy policy for details, including maintenance and legal compliance.
DAT-03	Which cloud infrastructure and primary storage locations are used?	**Documented**	The primary cloud infrastructure uses the AWS and GCP Tokyo regions in Japan. Cloudflare is used for content delivery. The responsibilities of the cloud providers and VoicePing must be distinguished. See DAT-04 for overseas processing and OPS-04 for backup scope and storage locations.
DAT-04	Does processing or subcontracting occur outside Japan?	**Conditional**	Content delivery, AI processing and notification integrations involve processing outside Japan. The Data handling and external processing table identifies providers, purposes and data types. Requirements for processing exclusively in Japan or prohibiting overseas access need individual agreement.
DAT-05	Is data encrypted in transit?	**Documented**	The official specifications state that application, audio and video communications use TLS 1.3 and enforce HTTPS. Communication conditions for files sent separately by the customer and for external integration services require separate confirmation.
DAT-06	Is stored data encrypted?	**Documented**	The public DPA specifies AES-256 encryption for databases and file storage, and the privacy policy describes AES-256 encryption for audio. Configuration evidence for individual storage destinations can be confirmed as needed. See INF-12 for key management and BYOK/CMK requirements.
DAT-07	Is data separated between customer organizations?	**Documented**	The design logically separates each organization's data within the database. This answer does not guarantee a dedicated database or physical separation as a standard feature.
DAT-08	How long is audio retained?	**Conditional**	Public documentation states that audio is retained for up to three months depending on plan and settings, then deleted. Do not apply this period to every other data type. Discuss longer retention in advance and obtain required data before expiry.
DAT-09	How long are meeting records and summaries retained?	**Confirm individually**	The meeting-record guide states up to one year for paid self-service plans, with Enterprise retention governed by contract terms. The privacy policy states retention during the contract period. The applicable agreement and actual settings require confirmation; this questionnaire does not provide a blanket guarantee of one-year or unlimited retention.
DAT-10	How long are video recordings retained?	**Conditional**	The pricing and retention guide states that meeting recordings are deleted after one month. Confirm the applicable feature and plan; uploaded videos, generated subtitles or dubbing, and time-tracking images require their own retention assessment.
DAT-11	How are retention and identifier deletion handled for each log type?	**Confirm individually**	The pricing guide lists 18 months for event, online-presence and work logs on paid plans; the privacy policy describes access-log retention as the minimum necessary period. Confirm actual retention and deletion scope, including captured images. The published policy calls for deletion or anonymization of personal identifiers within 30 days of a valid deletion request.
DAT-12	Is all data automatically deleted when the contract ends?	**Conditional**	The public policy describes retaining data after the contract ends until an authorized person deletes it or requests deletion, and deletion within 30 days of a valid request. Statutory retention obligations are exceptions. Contract termination and data deletion require separate actions. See USE-09 for customer offboarding actions and DAT-13 for backup deletion scope.
DAT-13	Can complete deletion, including backups, be confirmed?	**Confirm individually**	Backup retention, replication destinations, propagation of deletion, legal retention and the scope of deletion certificates require individual confirmation. Deletion through the user interface alone does not guarantee immediate physical erasure of every copy.

Data protection and privacy			
Item	**Question**	**Response**	**Answer**
DAT-14	Can disclosure, correction or deletion of data be requested?	**Documented**	Public procedures and contact channels are available for requests to access, correct, suspend use of or erase data, subject to identity verification. The requester's authority, request scope and statutory exceptions are checked when handling the request.
DAT-15	Is disposal and reuse of media and equipment managed?	**Confirm individually**	Controls for disposal and reuse of media and equipment require individual confirmation for the agreed scope.
DAT-16	Are there controls for sharing company documents externally?	**Confirm individually**	Please contact us individually for details of controls governing external sharing of company documents.

Identity and access management

Item	Question	Response	Answer
IAM-01	Are users managed through individual accounts?	**Documented**	Users are generally managed with one account per user. Caption listeners using a URL or QR code and Virtual Office guests using its web app are distinct participation modes. See USE-04 for feature-specific access.
IAM-02	Is two-step authentication supported?	**Conditional**	Paid plans can enable email-token two-step authentication for all workspace users. Sign-in through Google or Apple accounts has exceptions where email verification is not required. Confirm the strength of these alternative authentication paths and their interaction with SSO before deployment.
IAM-03	Is single sign-on available?	**Conditional**	SSO configuration procedures for Microsoft Entra ID and HENNGE One are publicly documented for Enterprise plans. Confirm the applicable plan, identity-provider configuration and domains.
IAM-04	Can SSO be enforced and alternative sign-in controlled?	**Conditional**	The official Entra ID guide states that members must use SSO when it is enabled, while owners and managers can also sign in without SSO. Confirm protection of these administrator exceptions, behavior with other identity providers and access during an identity-provider outage before deployment.
IAM-05	Can access be restricted by source IP address?	**Conditional**	IP Restriction is available on paid plans. The official guide states that it applies to managers and members, with an exception for the owner. Confirm owner protection, guest and API access paths, and permitted IP/CIDR ranges before deployment.
IAM-06	Are permissions checked by role after authentication?	**Documented**	The design applies authorization according to roles, workspaces and sharing settings in addition to authenticating the user. Permissions differ for owners, managers, members and external guests. Workspace deletion and billing administration require the owner role. See DAT-07 for separation between organizations and IAM-08 for group and feature access settings.
IAM-07	Can members be added, removed and assigned different roles?	**Documented**	Owners and managers can manage member additions, removals and role changes. Removing the current owner requires transferring ownership first.
IAM-08	Can access be configured by group and feature?	**Documented**	Access to groups, floors, projects and features such as translation and the virtual office can be configured for individual members. Assign the minimum permissions required for the customer's organizational structure.
IAM-09	Can meeting and file-processing records be shared with the intended audience?	**Conditional**	Meeting Logs provide viewing permissions and sharing settings. Check who can view records from each source, including Meeting Bot, Virtual Office and file processing. Review floor participation and record sharing separately. See USE-04 for participation routes and USE-07 for downloaded copies.
IAM-10	Are session IDs and cookies protected?	**Documented**	The published specifications describe hard-to-predict session IDs managed in cookies using Secure and HttpOnly attributes. The design does not embed session IDs in URLs.
IAM-11	Can session expiration and revocation be managed?	**Confirm individually**	Session revocation is described in the documentation. Actual settings for absolute timeouts, inactivity timeouts, per-device revocation and SSO-linked revocation require individual confirmation. Persistent sign-in and expiration when a browser closes must be distinguished.
IAM-12	What password strength and storage mechanisms are used?	**Confirm individually**	Users can change their passwords. Current requirements for length, complexity, hashing and reuse restrictions must be confirmed against current technical evidence. Contact us before deployment if specific authentication requirements apply.
IAM-13	Are unauthorized sign-in attempts restricted?	**Confirm individually**	Sign-in attempt limits, lockout conditions, unlocking methods, CAPTCHA coverage and rate-limit thresholds require individual confirmation. Product-user authentication and privileged access by operations personnel must be assessed separately.
IAM-14	Are automated provisioning and inactive-account suspension supported?	**Confirm individually**	Support for SCIM, identity-provider-linked deletion and automatic suspension of inactive accounts requires individual confirmation. Standard member-management features alone do not guarantee automated integration.
IAM-15	Can customers review their accounts and access rights?	**Documented**	The administration interface shows members and roles and can export a member list as CSV. The customer should manage removals after role changes or departures and conduct periodic access reviews.

Identity and access management			
Item	**Question**	**Response**	**Answer**
IAM-16	Is privileged access by operations personnel restricted?	**Confirm individually**	The permission scope, authentication, approval and activity records for operations personnel require individual confirmation.
IAM-17	Are employee account creation, changes and access reviews managed?	**Confirm individually**	Please contact us individually regarding employee account creation, changes and access-right reviews.
IAM-18	Are access rights revoked and issued equipment returned on departure?	**Confirm individually**	Please contact us individually regarding access revocation and return of issued equipment when an employee leaves.

Infrastructure, devices and monitoring

Item	Question	Response	Answer
INF-02	Is network access controlled?	**Documented**	Official documentation describes source-IP restrictions for servers and databases using AWS Security Groups. Disclosure of detailed network diagrams and permitted paths is coordinated individually.
INF-03	Is continuous threat detection performed?	**Documented**	Public documentation describes continuous detection of suspicious activity using AWS GuardDuty. Threat detection and real-time antivirus scanning of files are distinct controls.
INF-04	Is a WAF applied to every publicly accessible service?	**Confirm individually**	WAF coverage by domain and API, rules, exceptions and log operations require individual confirmation. Use of a CDN or DDoS protection alone does not guarantee WAF coverage for every access path.
INF-05	Is DDoS protection implemented?	**Conditional**	Public documentation states that Cloudflare is used for content delivery and DDoS protection. Covered paths, contracted services and guarantees regarding attack scale require individual confirmation.
INF-06	What is the scope of antivirus and EDR protection?	**Confirm individually**	The coverage and implementation status of antivirus and endpoint detection and response require individual confirmation.
INF-07	Is system operation monitored?	**Documented**	The published specifications describe process and system-state monitoring through CloudWatch or custom alerts, with notifications when a process or system stops. Automated monitoring does not guarantee a staffed support desk operating around the clock.
INF-08	Can administrators view and export activity history?	**Conditional**	Event Log shows the actor, action, timestamp and source IP address. Records can be filtered by period, member and category and exported as CSV or PDF. Confirm viewing permissions and plan conditions. See DAT-11 for retention and INF-14 for continuous SIEM forwarding, WORM storage and tamper protection.
INF-10	Are employee devices and software managed?	**Confirm individually**	Please contact us individually regarding the policies and scope for managing employee devices and software.
INF-11	Is physical security managed?	**Confirm individually**	Physical safeguards at offices and data centers require individual confirmation for the agreed scope.
INF-12	Are keys and secrets managed?	**Confirm individually**	Key and secret management methods, including support for customer-managed keys, require individual confirmation according to the customer's requirements.
INF-13	Are unattended screens and information on desks protected?	**Confirm individually**	Please contact us individually regarding employee screen locking and protection of information on desks.
INF-14	Are logs protected against tampering and unauthorized deletion?	**Confirm individually**	Log tamper protection, prevention of unauthorized deletion, storage methods and integration with external monitoring systems require individual confirmation.
INF-15	Is there a system clock synchronization policy?	**Confirm individually**	Please contact us individually regarding the scope and management of clock synchronization.

Application security and development

Item	Question	Response	Answer
APP-01	What controls address SQL injection?	**Documented**	Official documentation describes database operations using an ORM and placeholders, together with restricted database permissions. The scope, dates and results of security assessments are confirmed separately.
APP-02	Is operating-system command injection prevented?	**Documented**	The published design generally avoids launching a shell and performs necessary processing through verified libraries. Validation of exceptional paths requires individual technical evidence.
APP-03	What controls address directory traversal?	**Documented**	The design does not provide direct access to files on the web server and uses measures such as randomized filenames. Individual upload and download APIs can be checked when needed.
APP-04	What controls address cross-site scripting?	**Documented**	Published XSS safeguards include frontend libraries and explicit character-encoding settings. CSP coverage and current configuration values require individual confirmation. See IAM-10 for cookie protection attributes such as HttpOnly.
APP-05	What controls address cross-site request forgery?	**Conditional**	Public documentation describes access control using POST, Referer checks and notifications for important actions. POST or notifications alone should not be treated as sufficient protection; the scope of token validation, Origin checks and other controls must be confirmed.
APP-06	Is HTTP header injection prevented?	**Documented**	Public documentation describes using APIs for header output. Handling of input values and test evidence for response-splitting protection require individual confirmation.
APP-07	Is email header injection prevented?	**Confirm individually**	The current coverage of email header validation and newline handling requires individual confirmation.
APP-08	What controls address clickjacking?	**Documented**	The published design sends X-Frame-Options headers. Features requiring embedding, exceptions and the scope of CSP frame-ancestors require individual confirmation.
APP-09	How is memory-corruption risk addressed?	**Conditional**	The official specifications describe using Node.js and other technologies. Properties of the runtime alone do not establish that native code or dependencies are free from vulnerabilities. See APP-16 for dependency vulnerability checks and update procedures.
APP-11	Are development and change management established?	**Confirm individually**	Please contact us individually for development and change-management details, identifying the products and scope to be reviewed.
APP-12	Are third-party vulnerability assessments performed?	**Confirm individually**	The scope, timing and response status of assessments by external specialists require individual confirmation.
APP-13	Are development, test and production environments separated?	**Confirm individually**	Separation of development, test and production environments requires individual confirmation for the relevant configuration.
APP-14	Is personal information in test data protected?	**Confirm individually**	Please contact us individually regarding the permitted use of test data and measures for protecting personal information.
APP-15	Is code reviewed by another person?	**Confirm individually**	Please contact us individually regarding code-review methods and coverage.
APP-16	Are vulnerability information and fixes managed?	**Conditional**	Official documentation describes checking dependencies for vulnerabilities and updating them. Response deadlines by severity and the status of individual cases can be confirmed according to the customer's requirements.
APP-17	Can security testing during development be confirmed?	**Confirm individually**	Please contact us individually regarding the scope of security testing during development and the methods available to confirm it.

Availability, continuity and incident response			
Item	**Question**	**Response**	**Answer**
OPS-01	What are the service operating hours?	**Documented**	Public documentation describes service availability in principle 24 hours a day, 365 days a year. Conditions apply for planned maintenance, outages and individual agreements.
OPS-02	What availability level is stated in the SLA?	**Conditional**	Official documentation states availability of at least 99.9%. The calculation method, planned downtime, exclusions, compensation and refunds must be checked in the applicable agreement.
OPS-03	Can availability for a recent period be confirmed?	**Confirm individually**	Current availability results must be confirmed for a defined measurement period and method. Cumulative results with an unspecified period should not be used as measurements for the most recent 12 months.
OPS-04	Are backups taken?	**Confirm individually**	Backup scope, frequency, storage locations and retention periods require individual confirmation.
OPS-05	Can business continuity arrangements be confirmed?	**Confirm individually**	Please contact us individually regarding business continuity arrangements and the documentation available for confirmation.
OPS-06	Can RTO, RPO and recovery capability be guaranteed?	**Confirm individually**	Recovery time objectives (RTO) and recovery point objectives (RPO) require individual confirmation according to the required service scope and contract terms.
OPS-07	Are maintenance and specification changes communicated?	**Conditional**	Public documentation describes communications about maintenance and specification changes. Individual implementation dates and notification conditions must be confirmed under the applicable service agreement.
OPS-08	What channels are available for outage reports and support?	**Documented**	The published contact channels are email, in-app chat and inquiry forms. Confirm business hours and emergency contact conditions. Typical response guidance should not be treated as a fixed response-time SLA.
OPS-09	Are incident response procedures in place?	**Confirm individually**	Please contact us individually regarding the incident response framework and its scope.
OPS-10	Can security events be discussed individually?	**Confirm individually**	Information about security events is handled individually after confirming the relevant period and disclosure scope.
OPS-11	Are targets defined for notifying customers of outages?	**Confirm individually**	Notification recipients, communication methods and notification deadlines during an outage require individual confirmation under the applicable agreement.
OPS-12	Are incident evidence preservation and response records defined?	**Confirm individually**	Please contact us individually regarding evidence preservation and record handling during incident response.

AI and external integrations			
Item	**Question**	**Response**	**Answer**
AI-01	Are customer audio, transcripts and similar content used for AI training?	**Documented**	Public policy states that customer audio, transcripts and similar data are not used to train or develop AI models. Whether external services are used and whether data is used for model training must be assessed separately.
AI-02	What data is sent to external AI services, and where is it processed?	**Conditional**	Public documentation describes using OpenAI for meeting summaries and text analysis, with processing in the United States. Confirm the current model, transmitted data and processing destination for the features and processing involved.
AI-03	How long do external AI services retain data?	**Conditional**	Public policy describes a zero data retention configuration for the OpenAI API used by VoicePing. This does not automatically apply to AI services independently connected by the customer or to consumer services. Evidence of the current configuration requires individual confirmation.
AI-04	Is the accuracy of AI output guaranteed?	**Conditional**	Customers should check AI-generated translations, transcripts, summaries, subtitles and dubbing against the original audio, video or conversation record before important decisions or external use. These outputs require human review; this questionnaire does not promise 100% accuracy.
AI-05	Can AI features be disabled or models fixed?	**Confirm individually**	Requirements for AI-summary availability, centralized administrator controls, model pinning, change notifications and prompt retention require individual confirmation. Individual feature settings and enforcement of an organization-wide policy must be distinguished.
AI-06	Can external AI clients or APIs access Meeting Logs?	**Conditional**	External access is available through MCP-compatible AI clients and API keys, with connections managed by administrators. Customers should also evaluate retention, model-training use and access rights at the connected service.
AI-07	Can API and MCP permissions be limited?	**Documented**	Separate scopes distinguish searching the meeting-record list, reading record content and reading AI summaries. Allowed-IP restrictions can be configured for API keys. Assign only the minimum scopes required for each purpose.
AI-08	Can external connections be disabled, deleted and audited?	**Documented**	MCP connections and API keys can be disabled, re-enabled and deleted. Issuance, approval, disabling and similar actions are recorded in the event log. Disable keys suspected of exposure and also review data stored by the connected service.
AI-09	Can the content and destinations of integration notifications be managed?	**Conditional**	Notification text and meeting summaries are transmitted according to the enabled notification integrations. Customers should check destinations, public channels and transmitted content. See the Data handling and external processing table for the processing countries and purposes of Slack, Discord and Chatwork.
AI-10	Is the EU DPA ready to be executed?	**Confirm individually**	The availability of an EU DPA for execution, the representative and data-transfer terms require individual confirmation against the latest version. This document does not establish execution of a DPA or GDPR compliance.

Deployment and customer responsibilities

Item	Question	Response	Answer
USE-01	Can mobile devices process data offline?	**Conditional**	Offline Transcript on iOS and Android transcribes and translates audio on the device after the model has been downloaded in advance. This is a different processing method from cloud features and web-meeting bots.
USE-02	Can offline records be deleted?	**Documented**	The guide states that offline records can be viewed and deleted from the history on the device used. Device loss, operating-system backups and restrictions on taking devices or data off-site also require customer device management.
USE-03	Are PC and server features also fully offline?	**Confirm individually**	Standard cloud features must be distinguished from mobile offline features. Requirements for PC use on closed networks, dedicated environments and on-premises configurations need confirmation. Mobile offline support does not establish offline support for every product.
USE-04	Can caption listeners and Virtual Office guests be managed appropriately?	**Conditional**	Caption listeners view content through a URL or QR code. Virtual Office guests join an enabled guest web app through an invitation link. Review each route separately: recipients, available password controls, identity checks and plan eligibility. Check event terms when distributing captions outside your organization.
USE-05	Who manages notices and permissions for recording and transcription?	**Conditional**	Customers should confirm permissions, participant notices and any necessary consent for recording or transcription in meetings, events and Virtual Office, and for processing uploaded files. Assess applicable law, organizational rules and information classification for the intended use.
USE-06	Can confidential or sensitive information be used?	**Confirm individually**	Suitability must be assessed by confirming the data types, processing purposes, legal basis, destinations and storage conditions. This answer does not permit highly confidential information to be submitted without conditions.
USE-07	Can data be protected after export?	**Conditional**	Downloaded records and recordings, subtitles or dubbing, shared materials and time reports fall under the customer's storage, access and retention controls. Changing access inside VoicePing does not recall copies already obtained.
USE-08	Which settings should be checked before deployment?	**Conditional**	Confirm the features, plan and actual settings for Voice Translation and Virtual Office. Review authentication in IAM, record sharing in IAM-09, external access in AI-06 through AI-08, retention in DAT-08 through DAT-11, and feature-specific considerations in USE-10 through USE-15. Confirm required entitlements, administrators and settings before rollout.
USE-09	What data-return and access-termination actions are needed at offboarding?	**Conditional**	Customers should separately manage retrieval of required data, disabling external connections (AI-08), removal of unnecessary accounts (IAM-07), contract termination and data deletion requests (DAT-12). Contract termination, revocation of access rights and erasure of personal data are separate states.
USE-10	Are Meeting Bot admission and calendar connections controlled?	**Conditional**	Meeting Bot joins supported web meetings as a visible participant and is subject to host admission. Google Calendar or Outlook connections are configured when used. Customers should review target meetings, connected accounts and permissions, recording notices and the audience for resulting records.
USE-11	Are uploaded files and generated media managed?	**Conditional**	File Transcribe processes uploaded audio or video into transcripts, translations and supported subtitle or dubbing outputs, with results available in Meeting Logs. Check upload rights, sharing and downloads, supported formats and features, and the applicable retention and deletion conditions.
USE-12	Are Virtual Office presence and presence history distinguished?	**Conditional**	Virtual Office displays availability and work memos. When Online Log is enabled, presence history can be reviewed; it is distinct from project time tracking. Confirm notices to affected users, necessary displays and history, intended viewers and retention.

Deployment and customer responsibilities			
Item	**Question**	**Response**	**Answer**
USE-13	Is the audience for shared work content checked?	**Conditional**	Floors and meeting rooms support screen sharing, a collaborative editor and a whiteboard. Screen sharing can cover a desktop or a selected window. Review participants, guests and shared material, including information that could appear through notifications or other windows.
USE-14	Can optional time-tracking capture and viewing permissions be configured?	**Conditional**	Time tracking, desktop screenshots, webcam snapshots and input activity have separate member-level settings. Owners and managers can review team logs; members can view their own. Confirm selected capture types, intervals and blur, user notices, viewing permissions and retention. Running the timer requires the desktop app.
USE-15	Is use of remote desktop control managed?	**Conditional**	The collaboration guide describes requesting remote control of a shared screen and ending remote control from the sharing side. Customers should govern permitted use, the other participant, target device or screen, and ending the session. Confirm detailed restrictions and recording requirements individually.

Data handling and external processing

Provider / destination	Purpose	Location	Example data	Points to confirm
AWS	Cloud infrastructure, storage and monitoring	Japan (Tokyo)	Customer content, account and operational information	Used as infrastructure. Confirm backup replication destinations separately.
GCP	Databases and static hosting	Japan (Tokyo)	Database information and static content	Used as infrastructure. Confirm the configuration of the relevant service.
Cloudflare	Content delivery and DDoS protection	Global	IP addresses, request information and cached content	Processing is not limited exclusively to Japan.
OpenAI	Meeting summaries and text analysis	United States	Transcripts and text	Applies to the relevant AI features. This is not a complete list of providers for all speech-recognition processing.
Slack / Discord	Notifications such as meeting summaries	United States	Notification content and meeting summaries	Depends on the notification integrations enabled.
Chatwork	Notifications such as meeting summaries	Japan	Notification content and meeting summaries	Depends on the notification integrations enabled.
Customer-connected AI and customer systems	Data retrieval through API / MCP	Depends on the connected service	Meeting records and AI summaries within authorized scopes	The customer checks the connected service's terms, retention, model-training use and permissions.
Customer-connected meeting / calendar services	Meeting Bot admission and calendar connections	Provider and account settings	Meeting links, event details, in-call audio or video	Zoom, Google Meet, Microsoft Teams, Google Calendar or Outlook as used. Check permissions and the external service's retention.
Mobile device (offline)	On-device transcription and translation	On the device in use	Offline audio and text	The model must be downloaded in advance. Device management is the customer's responsibility.

Processing destinations vary by enabled feature. This table includes cloud providers, customer-connected external services and offline devices; it is not solely a subprocessor list. Confirm the data types, locations, retention, deletion and agreements for each feature.

Public references

All editions use the same public sources, in Japanese or English as published. Review dates indicate when the sources were checked.

Document	URL	Reviewed	Subject
Official security specifications	https://manual.voiceping.net/ja/security	2026-09-08	Public specifications for encryption, authentication, access control and monitoring.
Privacy policy	https://manual.voiceping.net/ja/privacy-policy	2026-09-08	Processing purposes, service providers, storage locations, retention and deletion.
Public GDPR DPA	https://manual.voiceping.net/en/gdpr-dpa	2026-09-08	Personal-data processing and international-transfer terms. Check the latest version when applying it.
Member types and permissions	https://manual.voiceping.net/ja/member-roles	2026-09-08	Workspace roles and permissions.
Member management	https://manual.voiceping.net/ja/member-management	2026-09-08	Member administration and list exports.
Microsoft Entra ID SSO	https://manual.voiceping.net/ja/sso-entra-id	2026-09-08	SSO configuration using Microsoft Entra ID.
HENNGE One SSO	https://manual.voiceping.net/ja/sso-hennge-one	2026-09-08	SSO configuration using HENNGE One.
IP Restriction	https://manual.voiceping.net/ja/ip-whitelist	2026-09-08	Restrictions on source IP addresses.
Event Log	https://manual.voiceping.net/ja/event-log	2026-09-08	Viewing, filtering and exporting activity history.
Meeting records and AI summaries	https://manual.voiceping.net/ja/meeting-minutes	2026-09-08	Meeting records, sharing and AI summaries.
Mobile offline translation	https://manual.voiceping.net/ja/mobile-offline-translation	2026-09-08	On-device mobile processing and history management.
External access	https://manual.voiceping.net/ja/external-access	2026-09-08	Management of API and MCP connections.
Pricing plans and data storage	https://manual.voiceping.net/ja/pricing	2026-09-08	Plan and data-storage guidance.
VoicePing official website	https://voiceping.net/	2026-09-08	Service and enterprise-feature information.
Member invitations and two-step authentication	https://manual.voiceping.net/ja/invite-members	2026-09-08	Member invitation and email-authentication procedures.
Virtual Office product guide	https://voiceping.net/en/products/virtual-office/	2026-09-08	Presence, collaboration, floors and guest participation.
Time Tracking product guide	https://voiceping.net/en/products/time-tracking/	2026-09-08	Tracked time, optional capture, viewing roles and exports.
Meeting Bot product guide	https://voiceping.net/en/products/meeting-bot/	2026-09-08	Meeting admission, calendar connections and records.
File Transcribe product guide	https://voiceping.net/en/products/video-translation/	2026-09-08	Uploads, translation, subtitles, dubbing and exports.
Time-tracking management	https://manual.voiceping.net/ja/time-tracking-management	2026-09-08	Member-level capture, intervals and blur.
External guests in a floor	https://manual.voiceping.net/ja/guest-invitation	2026-09-08	Guest web app and invitation links.
Collaboration tools	https://manual.voiceping.net/ja/collaboration-tools	2026-09-08	Screen sharing, editor, whiteboard and remote control.