

FantaScript Privacy Policy

Effective date: 6 June 2026 | Version 1.1 | Public repository version

IMPORTANT CUSTOMER AND PARTICIPANT NOTICE: FantaScript processes speech, audio, video, files, captions, transcripts, translations, summaries, metadata and related content through cloud infrastructure. By starting, joining, enabling, uploading, streaming, importing or submitting any session or content to FantaScript, the customer, organizer, administrator, host or user represents and warrants that all speakers, attendees, viewers, employees, contractors, guests and other participants have received legally sufficient notice and that all required consents, permissions, lawful bases and approvals have been obtained before any recording, monitoring, capture, cloud transmission, transcription, translation, captioning, speech-to-text, text-to-speech, speech-to-speech, storage, sharing, export or other processing occurs.

STRONG DISCLAIMER: FantaScript does not decide whether a meeting, call, event, recording, transcript, translation, caption, summary, export, publication or downstream use is lawful. Customers and users are solely responsible for complying with recording, wiretapping, surveillance, workplace monitoring, telecoms, ePrivacy, data protection, employment, accessibility, consumer, education, health, financial, confidentiality, intellectual-property, AI, biometric, children and sector-specific laws that apply to their use. To the maximum extent permitted by law, FantaScript disclaims liability for claims, fines, damages, complaints, investigations or disputes arising from customer or user failure to give notice, obtain consent, establish a lawful basis, restrict sensitive data, configure retention, verify output accuracy, or comply with applicable laws.

1. Scope

This Privacy Policy explains how FantaScript ("FantaScript", "we", "us" or "our") collects, uses, discloses, transfers, stores and protects personal data when individuals access or use FantaScript websites, landing pages, web applications, desktop applications, mobile applications, browser-based tools, APIs, integrations, admin consoles, support channels and related services (collectively, the "Services").

This Policy applies to customers, account owners, administrators, event organizers, meeting hosts, speakers, attendees, viewers, participants, end users, visitors and other individuals whose personal data may be processed through the Services. It does not replace any signed customer agreement, data processing agreement, order form or product-specific privacy notice.

2. What FantaScript Does

FantaScript is a cloud-based transcription, captioning, translation and speech-intelligence platform. The Services may provide live subtitles, live captions, speech-to-text, transcript generation, translation, multilingual outputs, speech-to-speech or text-to-speech features, speaker labels, timestamps, summaries, action items, highlights, notes, analytics, exports and related AI-assisted functionality.

Because the Services are cloud based, speech, audio, video, files, text and metadata may be transmitted from websites, browsers, desktop software, mobile applications, devices, microphones, meeting tools, conferencing systems or integrations to FantaScript systems and third-party cloud infrastructure for processing, storage, security, delivery, support and service operations.

3. Key Definitions

- **Customer** means the organization or person that creates or controls a FantaScript account, session, event, workspace, project, integration or subscription.
- **Customer Content** means audio, speech, video, files, chats, captions, transcripts, translations, summaries, speaker labels, timestamps, session content, exports and other materials submitted to or generated through the Services at the direction of a customer or user.
- **Participant** means any individual whose voice, image, words, personal data or other content may be captured, transmitted, transcribed, translated, summarized, displayed, stored, exported or otherwise processed through the Services.
- **Personal data** or **personal information** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to an individual, subject to applicable law.

4. GDPR and Similar Privacy Roles

For Customer Content, FantaScript generally acts as a processor, service provider or contractor that processes personal data on behalf of the customer, organizer, employer, institution, event owner or account administrator that determines the purposes and means of processing. The customer generally acts as controller, business or equivalent responsible party for Customer Content.

FantaScript may act as an independent controller for account registration, billing administration, customer relationship management, security, fraud prevention, abuse prevention, website analytics, service communications, legal compliance, business records, support, product administration and aggregated or de-identified operational data used to maintain and improve the Services. FantaScript may be both a controller and a processor depending on the processing activity.

Where GDPR, UK GDPR, Swiss FADP or similar laws apply, customers are responsible for entering into any required data processing agreement, documenting processing instructions, selecting appropriate settings, providing notices, obtaining consents, establishing lawful bases, conducting data protection impact assessments where required, managing data subject requests relating to Customer Content, and confirming that use of the Services is lawful for their jurisdiction and context.

5. Mandatory Customer, Host and User Responsibilities

The customer, host, organizer, administrator or user who initiates, configures or controls a session is solely responsible for:

- Giving clear and timely notice that speech, audio, video, screen content, files, chats or other content may be recorded, captured, transmitted to cloud infrastructure, transcribed, translated, captioned, summarized, stored, reviewed, downloaded, exported, shared or otherwise processed.
- Obtaining all required consents, permissions and approvals from every participant before recording, monitoring, capturing, transmitting, transcribing, translating, captioning, summarizing, storing or sharing content.
- Identifying and documenting a valid lawful basis under GDPR and other applicable laws, including explicit consent or another valid authorization where special-category or sensitive data may be processed.
- Complying with all recording, wiretap, two-party consent, ePrivacy, telecoms, employment, workplace monitoring, accessibility, education, health, financial, professional secrecy and sector-specific laws.
- Ensuring participants can access required notices before or at the start of a session and that any objections, withdrawals, opt-outs or restricted-processing requests are handled properly.
- Configuring retention, access, export, sharing and deletion settings in a lawful, proportionate and secure manner.
- Preventing unauthorized use of the Services for unlawful surveillance, discrimination, harassment, profiling, disciplinary action, publication, evidence gathering or other harmful or unlawful purposes.
- Ensuring that FantaScript is not used to process confidential, privileged, regulated, children, biometric, health, criminal, financial or highly sensitive information unless the customer has all required legal authority and safeguards.

FantaScript is not responsible for providing customer-specific recording notices, obtaining participant consent, deciding whether a lawful basis exists, monitoring local recording laws, validating customer content, or approving downstream use of outputs.

6. Categories of Data We May Process

6.1 Account, customer and administrative data

We may process names, usernames, email addresses, organization names, roles, login credentials or authentication identifiers, workspace settings, subscription or plan information, support requests, communications, account preferences, audit information and related business records.

6.2 Customer Content and session data

Depending on configuration and use, we may process live or recorded speech, audio, video, screen content, uploaded files, chat content, captions, transcripts, translations, summaries, speaker labels, timestamps, event names, meeting titles, agenda details, attendee lists, language selections, exports, action items and related outputs.

6.3 Device, usage, log and technical data

We may process IP addresses, device identifiers, operating system, browser type, application version, crash logs, diagnostic data, microphone or device status, performance data, access logs, authentication logs, feature usage, error reports, cookie identifiers, analytics events, security logs and approximate location derived from IP address.

6.4 Payment and billing data

If paid Services are offered, billing, tax, invoice, plan and transaction-related information may be processed by FantaScript or by independent third-party payment processors. This Policy does not copy, incorporate or replace any third-party payment provider rules, checkout terms, refund terms, merchant terms or payment-platform privacy policies. Third-party payment processors are responsible for their own platforms, terms, security, compliance and privacy practices, and customers should review those separate terms before completing any payment. FantaScript should not receive or store full payment-card details unless expressly stated by the relevant payment flow.

7. Sensitive Data and Special Categories

Speech and transcripts may unintentionally reveal sensitive or special-category information, including health information, disability, religion, political opinions, trade-union membership, sexual orientation, racial or ethnic origin, biometric or voice-related identifiers, criminal allegations, financial information, confidential business information, privileged communications, children data or other regulated information. FantaScript does not require customers to submit such data, and customers must not submit or capture it unless they have a valid legal basis, required notices, explicit consent where needed, appropriate safeguards, and contractual authority to do so.

FantaScript is not responsible for detecting, classifying, redacting or preventing sensitive information contained in Customer Content unless a specific written agreement states otherwise. Customers remain responsible for minimizing sensitive data, limiting access, applying retention controls, reviewing outputs and complying with sector-specific duties.

8. Purposes of Processing

FantaScript may process personal data to:

- Provide, operate, secure, maintain, troubleshoot and improve the Services.
- Transmit, ingest, process, transcribe, translate, caption, summarize, display, store, export, delete and deliver Customer Content according to customer settings and instructions.
- Authenticate users, manage accounts, administer workspaces, enforce permissions and provide customer support.
- Monitor performance, prevent abuse, investigate errors, detect security threats, protect rights and comply with legal obligations.
- Generate operational analytics, service quality measurements, aggregated or de-identified data and product improvements where permitted by law and applicable agreements.
- Send administrative notices, service updates, security alerts and customer communications.

FantaScript does not sell Customer Content. FantaScript does not use Customer Content for advertising targeting based on the content of private sessions unless expressly permitted by a customer agreement or applicable consent.

9. Legal Bases Where FantaScript Acts as Controller

Where FantaScript acts as controller under GDPR or similar laws, legal bases may include performance of a contract, legitimate interests in providing and securing the Services, compliance with legal obligations, consent where required, and protection of vital interests or public-interest grounds in limited cases. Where FantaScript acts as processor for Customer Content, the customer determines the legal basis and provides processing instructions.

10. Cloud Infrastructure, EU and US Data Centers

FantaScript may use cloud hosting, storage, networking, speech processing, translation, AI, backup, monitoring, security, support and content-delivery infrastructure located in the European Union, the United States, or both. Data may be routed through, processed in, stored in, backed up in, accessed from, or supported from EU and/or US data centers depending on product configuration, availability, latency, security, failover, customer location, feature use, subprocessors and operational needs.

Unless FantaScript signs a separate written data-residency commitment, FantaScript does not guarantee that Customer Content or metadata will remain in any specific country, region or data center. Customers that require EU-only, US-only, sovereign, on-premises or other restricted processing must obtain a written agreement from FantaScript before using the Services for such content.

Customers must inform participants that their speech, audio, transcripts, translations, summaries, files and related personal data may be transmitted to, processed in, stored in, or accessed from cloud infrastructure in the EU and/or the United States. Customers must not use the Services where such transmission or processing is prohibited by law, contract, policy, confidentiality duty, professional obligation or participant restriction.

11. International Transfers

Personal data may be transferred to, processed in, stored in or accessed from countries other than the country where it was collected, including transfers between the EEA/UK/Switzerland and the United States. Where GDPR, UK GDPR, Swiss FADP or similar laws require safeguards for international transfers, FantaScript will rely on appropriate transfer mechanisms as applicable, such as adequacy decisions, the EU-US Data Privacy Framework for certified recipients, UK extension or Swiss-US frameworks where applicable, Standard Contractual Clauses, International Data Transfer Agreements, supplementary measures, customer instructions, derogations or other lawful mechanisms.

Customers are responsible for determining whether their intended use of the Services, including any cross-border transfer of Customer Content, is lawful for their participants, sector and jurisdiction. FantaScript may update hosting regions, subprocessors or transfer mechanisms from time to time to maintain service availability, security and compliance.

12. Subprocessors and Third-Party Services

FantaScript may disclose or provide access to personal data to service providers, contractors, subprocessors and partners that help operate the Services, including cloud hosting, compute, storage, networking, content delivery, speech recognition, translation, AI processing, text-to-speech, monitoring, analytics, logging, security, authentication, email, customer support, backup, billing, tax, legal, accounting and professional advisory providers.

Subprocessors are authorized to process personal data only as needed to provide contracted services, comply with law, protect systems, support security, or fulfil documented customer instructions. Customers that require a list of subprocessors, prior notice of changes, objections or specific transfer terms should use the applicable data processing agreement or written enterprise contract.

13. Data Sharing and Disclosures

FantaScript may disclose personal data:

- At the direction of the customer or user, including to participants, administrators, collaborators, integrations, export destinations or recipients selected by the customer.
- To subprocessors and service providers supporting the Services.
- To comply with law, legal process, regulator requests, court orders, subpoenas or governmental demands.
- To enforce agreements, protect the Services, prevent abuse, detect fraud, investigate security incidents or protect rights, safety and property.
- In connection with a merger, acquisition, financing, restructuring, bankruptcy, asset sale or corporate transaction.
- With consent or as otherwise permitted by applicable law.

14. Accuracy, AI and Output Disclaimers

Transcripts, captions, translations, summaries, speaker labels, action items, analytics and other outputs may be incomplete, delayed, inaccurate, mistranslated, misattributed, biased or unsuitable for legal, medical, financial, official, accessibility, employment, compliance or evidentiary purposes. Customers and users must independently review, correct and validate outputs before relying on them or sharing them externally.

FantaScript does not provide certified translations, court transcripts, legal advice, medical advice, financial advice, official records, accessibility compliance guarantees or employment decision tools unless explicitly agreed in writing. Outputs should not be used as the sole basis for decisions that produce legal, employment, financial, health, educational, disciplinary or similarly significant effects on individuals.

15. Retention, Deletion and Backups

FantaScript retains personal data for as long as reasonably necessary to provide the Services, comply with customer settings and instructions, maintain records, resolve disputes, enforce agreements, prevent abuse, protect security, comply with law, maintain backups and satisfy legitimate business needs. Retention periods may vary by plan, feature, customer setting, contract and data type.

Customers are responsible for configuring retention settings, deleting content they no longer need, managing exported copies and instructing FantaScript where processor deletion is required. Deletion from active systems may not immediately delete data from encrypted backups, logs, audit records or legally preserved records. Backup deletion follows reasonable technical cycles, and FantaScript may retain limited information where necessary for legal, accounting, fraud prevention, security, abuse prevention or dispute purposes.

16. Security

FantaScript uses administrative, technical and organizational measures designed to protect personal data against unauthorized access, loss, misuse, alteration and disclosure. Measures may include encryption in transit, access controls, authentication, logging, monitoring, backup, segmentation, vendor review, confidentiality obligations, least-privilege practices, incident response and security testing.

No internet, cloud, AI, speech-processing, storage or electronic communication system is completely secure. Customers and users are responsible for securing accounts, using strong passwords or single sign-on where available, limiting administrator privileges, protecting devices, controlling exports, restricting sharing, verifying recipients and promptly notifying FantaScript of suspected compromise.

17. Data Subject Rights

Depending on jurisdiction, individuals may have rights to access, correct, delete, restrict, object to processing, withdraw consent, request portability, complain to a supervisory authority, or limit certain uses of personal data. For Customer Content, participants should contact the customer, host, organizer, employer, institution or account administrator that controlled the session because that party generally determines the purposes and means of processing.

Where FantaScript acts as processor, FantaScript will assist the customer as required by applicable data processing terms and law. Where FantaScript acts as controller, individuals may contact FantaScript through the privacy channels published on FantaScript properties or in customer agreements. FantaScript may verify identity and may deny or limit requests where permitted by law, including where retention is required for legal, security, accounting, abuse prevention or dispute purposes.

18. Cookies, Analytics and Similar Technologies

FantaScript websites and web applications may use cookies, pixels, local storage, SDKs and similar technologies for necessary functionality, authentication, security, preferences, analytics, performance, diagnostics and, where enabled, marketing. Users can manage cookies through browser settings and any cookie controls provided. Disabling certain technologies may affect functionality.

19. Desktop and Mobile Application Permissions

Desktop and mobile applications may request permissions such as microphone access, audio capture, camera access, screen capture, file access, notifications, local storage, speech input, network access, accessibility permissions and integration permissions. Permissions depend on device, operating system, product configuration and features used. Users should grant only permissions they are authorized to grant and may adjust permissions through device, browser or operating-system settings. Disabling permissions may prevent transcription, translation, captions or related features from working.

20. Children and Minors

The Services are not intended for use by children unless used under the lawful responsibility and authorization of a parent, guardian, school, educational institution or other authorized organization. Customers must comply with children privacy laws, parental-consent requirements, school records laws and age-specific safeguards where applicable. FantaScript does not knowingly collect children personal data as an independent controller without appropriate authorization.

21. Confidentiality, Access, Sharing and Exports

Customers are responsible for determining whether content is confidential, privileged, proprietary or restricted and for controlling who can access, view, download, export, publish or share transcripts, translations, summaries, recordings and other outputs. Once content is exported, downloaded, copied, emailed, posted to another platform, connected to an integration or shared outside FantaScript, FantaScript may not be able to control, retrieve or delete those copies.

22. Customer Content Ownership and Limited License

As between FantaScript and the customer, Customer Content remains owned by the customer or its licensors, subject to the customer agreement and applicable law. Customers grant FantaScript a limited license and instruction to host, transmit, process, reproduce, display, transform, transcribe, translate, caption, summarize, store, secure, support, maintain, delete and otherwise use Customer Content as necessary to provide the Services, comply with law, protect the Services and enforce agreements.

23. Prohibited and Restricted Uses

Customers and users must not use the Services to violate law; record without required notice or consent; capture private conversations unlawfully; process content without authorization; conduct unlawful surveillance; identify or authenticate

individuals biometrically without authorization; harass, discriminate or retaliate; infringe intellectual-property or confidentiality rights; expose secrets without authority; process regulated data without safeguards; violate export-control or sanctions laws; or attempt to reverse engineer, overload, scrape, abuse, disrupt or compromise the Services.

24. Limitation of Liability and Customer Indemnity Notice

To the maximum extent permitted by law, FantaScript is not liable for claims, fines, penalties, damages, losses, complaints, investigations, regulatory actions, participant disputes or third-party demands arising from customer or user decisions about what to record, capture, upload, transmit, transcribe, translate, caption, summarize, retain, export, disclose, publish or rely on. Customers and users are solely responsible for legality, transparency, necessity, proportionality, consent, lawful basis, participant notice, access control, retention, deletion, accuracy review and downstream use of Customer Content and outputs.

Where allowed by applicable agreement and law, customers should indemnify, defend and hold FantaScript harmless from claims arising out of Customer Content, participant notices and consents, customer instructions, unlawful recordings, regulatory violations, employment or monitoring disputes, unauthorized sharing, sensitive-data processing, data-residency requirements not agreed in writing, and downstream reliance on or publication of outputs. The exact indemnity terms, if any, must be stated in the applicable customer agreement.

25. Relationship to Terms, DPA and Payment Provider Terms

This Policy should be read with the applicable Terms of Service, customer agreement, data processing agreement, order form, product documentation, cookie notice and security documentation. If there is a conflict, the signed customer agreement or data processing agreement controls to the extent permitted by law.

This Policy does not reproduce, incorporate or adopt the rules of any third-party marketplace, payment platform, checkout provider or payment processor. Payment providers, app stores and other third-party platforms may have their own privacy notices, payment terms, refund rules, merchant obligations and dispute processes, and those separate documents govern the third-party platform relationship.

26. Complaints and Supervisory Authorities

Individuals in the European Economic Area, United Kingdom, Switzerland and other jurisdictions may have the right to lodge a complaint with a competent data protection authority. For Customer Content, individuals should first contact the customer, host, organizer, employer, institution or account administrator that controlled the session. For processing where FantaScript acts as controller, individuals may contact FantaScript through the privacy contact channels made available on FantaScript properties or in customer agreements.

27. Changes to this Policy

FantaScript may update this Policy from time to time to reflect changes to the Services, law, subprocessors, infrastructure, transfer mechanisms, security practices or business operations. The updated version will be indicated by an updated effective date. Continued use of the Services after an update means the Services will be subject to the updated Policy, subject to applicable law and contractual terms.

28. Contact

For privacy questions regarding FantaScript-controlled processing, use the contact channels made available on www.fantascript.com, in your FantaScript account, or in your customer agreement. For Customer Content, participants should first contact the customer, host, organizer, employer, institution or account administrator that controlled the session.