



Data Processing Addendum

Effective 5 September 2026. Last updated 9 October 2026.

This Data Processing Addendum ("Addendum") applies where an organisation uses the Chui Service and is, in respect of personal data contained in User Content, a controller within the meaning of applicable data protection law. It is incorporated into our [Terms of Use](#) by clause 3.5 of those Terms and is accepted with them. There is nothing to sign and nothing to negotiate. A Customer that wants a countersigned record for its files may use [the copy signed by us](#) and complete its own part of the signature page; doing so changes nothing in this text.

It does not apply to an individual who uses the Service for personal purposes. An individual account is not a controller relationship and is governed by the Terms of Use and the [Privacy Policy](#) alone.

1. Parties, scope and precedence

1.1 The parties are the organisation identified by the account or accounts to which this Addendum applies ("Customer", the controller) and **Generative Chaos LLC**, 5900 Balcones Drive #33409, Austin, TX 78731, United States ("Chui", "we", "us", the processor).

1.2 This Addendum governs our processing of Customer Personal Data on the Customer's behalf. It takes effect when the Customer, or a person authorised to bind the Customer under clause 3.4 of the Terms, accepts the Terms, and it remains in force for as long as we process Customer Personal Data.

1.3 Where this Addendum and the Terms of Use conflict on a matter of data protection, this Addendum prevails. In every other respect the Terms govern.

1.4 We do not offer a separately negotiated agreement and we do not sign a customer's own template. This is the whole of what is on offer, on the same terms to everyone.

2. Definitions

"Applicable Data Protection Law" means Regulation (EU) 2016/679 (the "GDPR"), the UK GDPR together with the Data Protection Act 2018, the Swiss Federal Act on Data Protection, and any other data protection or privacy law applicable to our processing of Customer Personal Data.

"Authorised User" means an individual to whom the Customer has made the Service available, whether by creating an account for them, paying for one, administering one, or admitting one through a domain or directory the Customer controls.

"Customer Personal Data" means personal data contained in User Content, and personal data in the account records of Authorised Users, that we process on the Customer's behalf in providing the Service.

"Sub-processor" means a third party engaged by us to process Customer Personal Data. It is the same set of companies the Privacy Policy calls Providers.

"Voiceprint" has the meaning given in clause 3.3 of the Terms of Use.

"controller", "processor", "personal data", "processing", "data subject", "personal data breach" and **"supervisory authority"** have the meanings given in the GDPR.

Capitalised terms not defined here have the meaning given in the Terms of Use or the Privacy Policy.

3. Roles

3.1 We are the processor of Customer Personal Data. The Customer is the controller. The Customer determines the purposes for which meetings are recorded, who is recorded, what is kept and for how long; we process it to provide the Service to the Customer and, unless the Customer switches it off, to improve the Service as clause 3.4 describes, and for no purpose of our own.

3.2 We are the controller of Usage Data. Technical, operational, diagnostic and event data generated by use of the Service is processed by us as controller, for the purposes and on the legal bases set out in the Privacy Policy. It does not include User Content.

3.3 We are not a joint controller and we do not determine the purposes of the Customer's recordings.

3.4 Improving the Service. Unless it is switched off, the Customer instructs us, as part of the instructions in clause 4.1, to process Customer Personal Data also in order to operate, develop, evaluate, test and improve the Service the Customer uses, including by review and automated analysis, as paragraph 3(h) of the Privacy Policy describes. The instruction does not extend to developing any other product or service of ours. An administrator of the Customer may switch that processing off for every Authorised User of the Customer, which withdraws the instruction, and no Authorised User can then switch it back on; each Authorised User may also switch it off for their own account in Settings → Privacy. While it is off for an Authorised User, nothing recorded through their account is processed for that purpose; switching it off does not affect processing carried out before. It never extends to a Voiceprint, and it gives no Sub-processor any right to use Customer Personal Data to train, fine-tune or otherwise develop its own models.

4. Our obligations

4.1 Documented instructions. We will process Customer Personal Data only on the Customer's documented instructions, including as regards transfers to a third country. The Terms of Use, the Privacy Policy, this Addendum and the Customer's use of the features of the Service constitute those instructions in their entirety. If we are required by law to process otherwise, we will inform the Customer before doing so unless that law prohibits it. If we consider an instruction to infringe Applicable Data Protection Law, we will inform the Customer without undue delay.

4.2 Confidentiality. Every person we authorise to process Customer Personal Data is bound by an obligation of confidentiality that survives the end of their engagement.

4.3 Security. We will implement and maintain the technical and organisational measures set out in Annex 2, which are our measures under Article 32 of the GDPR. We may change a measure provided the level of security is not reduced.

4.4 Sub-processors. The Customer gives a general written authorisation for us to engage Sub-processors. The current list is published at chui.io/subprocessors and is part of this Addendum. Each Sub-processor is engaged under a written contract imposing obligations no less protective than those in this Addendum, and we remain liable to the Customer for its performance. We will give reasonable advance notice of the addition or replacement of a Sub-processor, and in any case before it begins to process Customer data, by updating that page and, where the Customer has given us an address for the purpose, by writing to it. The Customer may object on reasonable grounds relating to data protection before the change takes effect; where we cannot accommodate the objection, the Customer may terminate the affected part of the Service and receive a refund of the unused portion of any amount paid for it.

4.5 Data subject requests. The Service allows an Authorised User to delete a recording and an account from within the application, which is how most requests are satisfied without our involvement. Where a data subject applies to us directly — including a person who was recorded and holds no account — we deal with the request as section 6 of the Privacy Policy describes, and we will inform the Customer where the recording is held in an account the Customer administers. We will not otherwise decide a request on the Customer's behalf. Taking account of the nature of the processing, we will assist the Customer by appropriate technical and organisational measures, insofar as this is possible, in fulfilling its obligation to respond to requests under Chapter III of the GDPR.

4.6 Assistance with Articles 32 to 36. Taking into account the nature of processing and the information available to us, we will assist the Customer in ensuring compliance with its obligations as to security, breach notification, data protection impact assessment and prior consultation.

4.7 Personal data breach. We will notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data, and will provide the information reasonably available to us to enable the Customer to meet its own notification obligations. A notification is not an admission of fault.

4.8 Deletion and return. What is deleted from within the application leaves the Service at once and is erased within fourteen days. On the ending of the Service, and at the Customer's choice, we will delete or return Customer Personal Data and delete existing copies within fourteen days, and from routine backups within thirty days after that, unless

the law requires us to keep it. The Service's export facilities are the means of return. **The Customer may also set a retention period for audio:** an administrator of the Customer's company in the Service may choose a number of days after which the audio of the meetings of every Authorised User who is then a member of the company is deleted — from our storage and from the Authorised Users' devices — while the transcripts, summaries, notes and attached files are kept until they are deleted. Until a period is chosen, audio is kept for as long as the meeting is.

4.9 Information and audits. We will make available to the Customer the information necessary to demonstrate compliance with Article 28 of the GDPR. The Customer may audit that compliance, or appoint an independent auditor to do so, on not less than thirty days' written notice, not more than once in any twelve-month period unless a personal data breach or a supervisory authority requires otherwise, during business hours, at the Customer's cost, subject to confidentiality, and in a manner that does not disrupt the Service or expose the data of any other customer.

5. The Customer's obligations

5.1 Lawful basis and notice. The Customer warrants that it has a lawful basis for the processing it instructs, that it has given the notices and obtained the consents required of a controller, and that its instructions comply with Applicable Data Protection Law.

5.2 Recording. Clauses 3.1 to 3.4 of the Terms of Use apply to the Customer: where an account is administered by an organisation, that organisation is the party responsible for having a lawful basis and, where required, the consent of every participant in every recording made through it. We have no means of determining who is present in a meeting or whether they have agreed, and we make no assessment of the lawfulness of any recording.

5.3 Voiceprints and special categories. A Voiceprint is a special category of personal data under Article 9 of the GDPR. The Service creates one only for an Authorised User who has switched on "Own-voice recognition" for their own voice (paragraph 6.4(f) of the Privacy Policy), on the basis of that person's own explicit consent, which the Service records together with the wording they were shown and any withdrawal. Nobody — the Customer, an administrator or another Authorised User — can give that consent for

somebody else. A Voiceprint is compared only in that Authorised User's own recordings and in recordings made by the Customer's other accounts to which they were invited, and never outside the Customer; every other voice in a recording is measured for that comparison only and discarded at once. An administrator of the Customer may switch the setting off for every Authorised User, and never on; doing so deletes every Voiceprint of the Customer's accounts at once. A Voiceprint is deleted when its owner switches the setting off, when an administrator of the Customer forbids it, when it has not been used for a year and when that Authorised User's account is deleted; it belongs to that Authorised User and not to any recording, so deleting a recording in which they spoke does not delete it. Voices are still separated within a single recording whatever the setting, which creates no Voiceprint. The Customer is responsible for informing the participants in its recordings that voices of people who switched the setting on may be recognised. A recording may also contain special categories of personal data because a participant said something, and the Customer is responsible for that processing on the same footing. The Service does not require special categories of personal data in order to function.

5.4 Access within the Customer. The Customer decides which of its Authorised Users may see which recordings, and is responsible for administering that.

6. International transfers

6.1 We are established in the United States and Customer Personal Data is processed in the United States and in the European Union. Where the Customer's company in the Service was created from the European Union, the European Economic Area, the United Kingdom or Switzerland, Customer Personal Data is stored in the European Union, with the exceptions, and the means of correcting a wrongly detected region, set out in section 15 of the Privacy Policy.

6.2 Standard Contractual Clauses. Where the transfer of Customer Personal Data from the European Economic Area to us would otherwise be prohibited, the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914, Module Two (controller to processor), are incorporated into this Addendum by reference and are deemed executed by the parties on the date this Addendum takes effect, with the Customer as data exporter and Chui as data importer. The following applies to them: the

optional docking clause in Clause 7 does not apply; Clause 9 Option 2 (general written authorisation) applies with the period of notice in clause 4.4 above; the optional redress clause in Clause 11(a) does not apply; the governing law under Clause 17 is the law of Ireland; the forum under Clause 18(b) is the courts of Ireland; Annex I is Annex 1 of this Addendum; Annex II is Annex 2 of this Addendum; and Annex III is the list at chui.io/subprocessors.

6.3 United Kingdom. Where the UK GDPR applies, the International Data Transfer Addendum issued by the Information Commissioner under section 119A of the Data Protection Act 2018 (the "UK Addendum") is incorporated and deemed executed, with the Standard Contractual Clauses above as its Approved EU SCCs, the parties and annex information as set out here, and neither party entitled to terminate under its Section 19.

6.4 Switzerland. Where the Swiss Federal Act on Data Protection applies, references in the Standard Contractual Clauses to the GDPR are read as references to that Act, the competent authority is the Federal Data Protection and Information Commissioner, and the term "member state" does not deprive a data subject in Switzerland of the right to sue in their place of habitual residence.

7. Liability, changes and law

7.1 Liability. Our liability under this Addendum is subject to section 10 of the Terms of Use. Nothing in this clause limits the liability of either party to a data subject under Applicable Data Protection Law or under the Standard Contractual Clauses.

7.2 Changes. We may amend this Addendum. Where an amendment materially affects the Customer's rights we will give not less than thirty days' notice before it takes effect, in the same way as section 13.3 of the Terms of Use requires. Where an amendment is required by law or by a supervisory authority, it takes effect on the date the law requires.

7.3 Governing law. This Addendum is governed by the law stated in section 11 of the Terms of Use, save that the Standard Contractual Clauses and the UK Addendum are governed by the law each of them specifies.

7.4 Survival. Clauses 4.2, 4.8, 4.9 and 7.1 survive the ending of the Service.

Annex 1 — description of the processing

ELEMENT	DESCRIPTION
Subject matter	The provision of the Service to the Customer under the Terms of Use
Duration	For as long as the Customer uses the Service, and thereafter for the deletion periods in clause 4.8; audio no longer than the retention period the Customer chooses under clause 4.8, where it chooses one
Nature and purpose	Recording a meeting from a device in an Authorised User's possession; storing it; transcribing it; separating and labelling speakers; producing titles, summaries and search results; answering an Authorised User's own questions, by a language model that reads, through the Service's own tools, what that user may open — meetings, people, calendar, attachments, workspaces, and the user's account, company and billing details (an administrator may switch this off for the Customer's accounts); sending notifications; providing support — in each case to provide the Service to the Customer. Recognising the voice of an Authorised User who has switched on "Own-voice recognition" for their own voice (clause 5.3). Improving the Service on the Customer's instruction, unless switched off (clause 3.4)
Frequency	Continuous, for as long as the Customer uses the Service
Categories of data subjects	Authorised Users, and the other people present in the meetings they record — most of whom have no account with us
Types of personal data	Audio recordings of speech; transcripts, summaries, titles, speaker labels and notes derived from them; names spoken in a meeting or typed by an Authorised User; files attached to a meeting and their names; the list of people an Authorised User keeps and the short note kept about each; calendar events of a connected calendar, with invitees' names and addresses; questions an Authorised User asks the Service and the answers to them; the Voiceprint of each Authorised User who has switched on "Own-voice recognition" for their own voice, and of nobody else; account identifiers and email addresses; what a third-party account an Authorised User connects — a calendar, for instance — hands us, limited to what the connection requires; device, application and event data

ELEMENT	DESCRIPTION
Special categories	Not required by the Service. A recording may nevertheless contain them because a participant said something. A Voiceprint is one, held only for the Authorised User whose voice it is and on that person's own explicit consent. Clause 5.3 governs
Transfers to Sub-processors	For the purposes and to the categories of recipient listed at chui.io/subprocessors , for the duration of this Addendum
Competent supervisory authority	The supervisory authority of the European Economic Area state in which the Customer is established, or as otherwise determined under Clause 13 of the Standard Contractual Clauses
Data exporter	The Customer, acting as controller. Contact: the address it has given us
Data importer	Generative Chaos LLC, 5900 Balcones Drive #33409, Austin, TX 78731, United States, acting as processor. Contact: privacy@chui.io
Data importer's representative in the Union	Data Protection Representative Limited ("DataRep"), 77 Camden Street Lower, Dublin D02 XE80, Ireland

Annex 2 — technical and organisational measures

These are the measures in place at the date above. We may change a measure provided the level of security is not reduced.

- **Encryption.** Customer Personal Data is encrypted in transit and at rest.
- **Access to audio.** Audio is served only through short-lived signed links, not from public addresses. A link expires and is scoped to a single recording, and when a recording is deleted its audio is destroyed, so no link to it can serve anything afterwards.
- **Authentication.** Sign-in is provided through third-party identity providers. We do not hold a password for any Authorised User.

- **Sessions.** A session is bound to a device, is visible to the Authorised User in the application, and can be revoked there.
- **Access control within Chui.** Access to production systems is limited to the personnel who operate the Service, under the confidentiality obligation in clause 4.2, and for the purposes set out in section 3 of the Privacy Policy.
- **Segregation.** Every recording is held against the account that created it. A request for it is authorised against that account; a signed link is issued only to a request that was already authorised.
- **Sub-processor constraint.** No Provider is permitted to use User Content to train, fine-tune or otherwise develop its own models. This is a term of our contract with each of them, not a preference.
- **Analytics.** Product analytics receive Usage Data only, and no User Content.
- **Deletion.** Deletion from within the application erases, within fourteen days, the audio, transcript, summary, notes and attached files. A Voiceprint is kept per person, not per recording: it may have been learned in part from a recording that is deleted, and it is not deleted with that recording. It belongs to the Authorised User whose voice it is, and is deleted when that person switches off "Own-voice recognition", when an administrator of the Customer forbids it, when it has not been used for a year, and when that person's account is deleted (clause 5.3). Deletion of an account removes the Service Data associated with it within fourteen days, and from routine backups within thirty days after that.
- **Resilience.** Data is held on cloud infrastructure that maintains redundant copies across facilities. The infrastructure provider is named in the list at chui.io/subprocessors.
- **Availability of the record.** The Service measures and reports the proportion of elapsed time actually captured in a recording, so that an incomplete recording is visible as one rather than silently short.

No method of transmission or storage is entirely secure, and we do not warrant absolute security.

Annex 3 — Sub-processors

The current list, with the category and the country of establishment of each, is published at chui.io/subprocessors and forms part of this Addendum. Clause 4.4 governs how it changes.

Questions about this Addendum: privacy@chui.io

Generative Chaos LLC, 5900 Balcones Drive #33409, Austin, TX 78731, United States

Signatures

This Addendum binds on acceptance of the Terms of Use (clause 1.2) and needs no signature to take effect. This copy is provided signed by Chui for a Customer that wishes to hold a countersigned record. Completing it does not change the text above.

**For Generative Chaos LLC ("Chui",
processor)**

Signature:



Name:

Emil Ivov Petrov

Title:

Manager

Date:

9 October 2026

5900 Balcones Drive #33409, Austin, TX
78731, United States

For the Customer (controller)

Signature:

Name:

Title:

Date:

Company name:

Address: