

Data Processing Agreement

Version 1.0 · Last updated: 2026-10-03 ·

About this agreement

Where we store and process personal data on your behalf, for example recordings of your streams that show or name other people, you are the controller and we are your processor under Article 28 GDPR. This page is the data processing agreement for that processing. It forms part of our [Terms of Service](#) and applies from the moment you accept them; there is nothing further to sign or click. It does not cover personal data we process as a controller for our own purposes, such as your account and billing data, which our [Privacy Policy](#) describes.

The agreement is the Standard Contractual Clauses between controllers and processors adopted by the European Commission (Commission Implementing Decision (EU) 2021/915 of 4 June 2021), reproduced below in their published wording with the options chosen, and Annexes I to IV completed for NONSTOPVOD. Where the clauses offer options, only the chosen one is shown: Regulation (EU) 2016/679 applies, and the processor has the controller's general written authorisation for sub-processors with 30 days' notice of changes (Clause 7.7(a)).

Standard Contractual Clauses

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- (b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.
- (c) These Clauses apply to the processing of personal data as specified in Annex II.

- (d) Annexes I to IV are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

- (a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- (b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.
- (c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 (optional docking clause) is not used.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1. Instructions

- (a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
- (b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

- (a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
- (b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process

the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- (c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
- (d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

- (a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

- (b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
- (d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
- (e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

- (a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- (b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

- (a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
- (b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions
- (c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
 - (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
 - (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
 - (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
 - (4) the obligations in Article 32 of Regulation (EU) 2016/679.
- (d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- (a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- (b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:
 - (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (2) the likely consequences of the personal data breach;
 - (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- (c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

- (a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
- (b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - (2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
 - (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
- (d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing

copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

List of parties

Controller

- Name: the customer, being the person or entity that registered the NONSTOPVOD account and accepted the Terms of Service, as recorded in the account.
- Address and contact details: as provided by the controller when registering and in the account settings.
- Signature and accession date: these Clauses are accepted together with the Terms of Service. The time of acceptance and the version accepted are recorded by the processor against the account.

Processor

- Name: Niklas Fitzon, operating NONSTOPVOD.
 - Address: Chamissostraße 2, Berlin, Germany.
 - Contact: hello@nonstopvod.com. No data protection officer has been appointed.
 - Signature and accession date: the processor accepts these Clauses by offering the Terms of Service; the date is the date of the controller's acceptance.
-

ANNEX II

Description of the processing

Categories of data subjects whose personal data is processed

- People who appear, speak or are named in the controller's recorded streams (the controller itself, guests, and anyone else in the picture or audio).
- Viewers or other users of the controller's Twitch channels whose usernames or messages are visible in a recording, or who write in chat while the chat bot is enabled.

- The controller's authorised users (members of its workspace), to the extent their data is processed to provide the Service to the controller.

Categories of personal data processed

- Video, audio and images in the controller's VODs, uploaded files and chosen audio, together with their metadata (title, duration, recording date, size, chapters and categories).
- Twitch account identifiers, login and display names of the controller's channels, and the access tokens and stream keys the controller grants for them.
- Usernames and messages of chat participants, processed only transiently to answer a chat bot command and not stored.
- Email address and role of workspace members the controller invites.

Sensitive data processed (if applicable) and applied restrictions or safeguards

None is collected on purpose. The processor does not review recordings before they are stored or streamed, so a recording may contain data of any kind that the controller chose to record. Such data is covered by the same access restrictions and purpose limitation as all other content (Annex III); the controller is responsible for having a legal basis for recording it.

Nature of the processing

Receiving copies of the controller's own Twitch VODs and uploaded files; storing them byte for byte in cloud object storage; deriving metadata (for example muted ranges and chapters); serving them to the controller and to people the controller shares a playback link with; and republishing them as a continuous broadcast to the replay channel the controller nominated. Video is copied and segmented, not re-encoded, except where an upload is converted to the format the controller chose, where a channel's live media is converted to its current format, and on GPU Studio channels, which composite and re-encode the picture. The title, game and thumbnail of a stream may be shown publicly, without any credential, on the controller's schedule and vote pages and in its Twitch panel; this is metadata only and the recordings themselves are not.

Purpose(s) for which the personal data is processed on behalf of the controller

Providing the NONSTOPVOD archive, playback and replay channel services described in Section 2 of the Terms of Service to the controller.

Duration of the processing

For as long as the controller holds the account, until the data is deleted. The controller can delete individual VODs, a channel or a whole workspace itself in the dashboard, and the stored recordings are removed from storage when it does. Removal after a subscription lapses, and deletion of an account, follow Sections 10 and 13 of the Terms of Service. On termination Clause 10(d) applies: the controller chooses between deletion and return and tells the processor before the account is deleted.

For processing by (sub-)processors, subject matter, nature and duration

As stated for each sub-processor in Annex IV; in each case for the duration of the processing described above.

ANNEX III

Technical and organisational measures including technical and organisational measures to ensure the security of the data

Measures for the protection of data during transmission

- Public web access is served over HTTPS only, with TLS 1.2 and 1.3 and an HSTS header.
- Traffic between the processor's own hosts runs over a WireGuard tunnel. Links between the supervising service and the hosts that run broadcasts additionally use TLS with pinned certificates, and there is no mode that accepts any certificate.
- Archive objects are written to and read from the storage provider over HTTPS.

Measures for user identification and authorisation

- Passwords are stored only as bcrypt hashes. Session tokens are signed, and only a SHA-256 hash of the session identifier is stored, so a session can be revoked at any time.
- Every request to a workspace's data is checked against the caller's membership of that workspace. Billing actions and deleting a workspace are limited to the workspace owner.
- Playback of stored video requires an unguessable, time-limited grant, which the process that reads recordings from storage checks on every request.
- The operator console is separate from the customer application and requires an operator account.

Measures for the protection of data during storage

- Recordings are held in a private bucket at the storage provider, in an EU region, reachable only with the processor's credentials. The read path through the content delivery provider accepts only short-lived tokens, each bound to one object.
- Credentials the controller grants (Twitch tokens, stream keys) are held in the processor's database, are never returned by the API and are protected by access control and the host measures below rather than by column encryption.

Measures for ensuring physical security and system security

- Processing runs on servers rented from a hosting provider; physical security of the data centres is that provider's (Annex IV).
- Servers accept SSH only with keys, forbid root login, run fail2ban and install security updates automatically.
- A firewall limits which hosts may reach the application ports across the tunnel. The public web host holds no database login, storage key or signing secret, and a broadcast process holds no database credential.
- Storage credentials are scoped by the processor at the storage provider.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience

- Every write to storage is checked against the checksum the storage provider returns, and an inconsistent write is not accepted.
- A broadcast keeps running when the supervising service restarts, and the service re-attaches to it afterwards.
- Access to customer data by the processor is limited to what is necessary to operate the Service and to answer support requests.

Measures for ensuring events logging, data minimisation and limited retention

- Server access logs omit the request path on routes that carry credentials.
- There is no advertising, analytics or tracking. Only the data needed to provide the Service is processed.
- A scheduled job deletes expired sessions and playback grants, spent email tokens, and old mail, job and broadcast history after set periods.

Measures for allowing data portability and ensuring erasure

- Recordings are byte-identical copies of the controller's own VODs, which also remain in the controller's own Twitch account for as long as Twitch keeps them. VODs, channels and

workspaces can be deleted by the controller in the dashboard, after a preview of what will be removed, and the stored recordings are deleted from storage as part of that.

Assistance to the controller (Clauses 8 and 9)

- A request from a data subject that reaches the processor is forwarded to the controller and not answered by the processor, which supports the controller with finding, exporting and deleting the data concerned.
 - The processor notifies the controller of a personal data breach concerning data it processes for the controller without undue delay after becoming aware of it, with the information listed in Clause 9.2, by email to the address on the account.
-

ANNEX IV

List of sub-processors

The controller has authorised the use of the following sub-processors (general written authorisation, Clause 7.7(a)). The processor informs the controller of intended changes at least 30 days in advance, by email to the address on the account or by notice on this page.

1. Backblaze, Inc. (storage provider), USA

Object storage of all recordings, uploads, music and brand files, in the EU region eu-central-003. Duration: as long as the data is stored. Backblaze is a US company; transfers rely on the EU-US Data Privacy Framework or the Standard Contractual Clauses.

2. Cloudflare, Inc. (content delivery), USA

Read path in front of the storage bucket: a Cloudflare Worker passes recording segments from the bucket to the processor's own hosts. It stores nothing permanently and holds a read-only key. Duration: for each request. Cloudflare is a US company; transfers rely on the EU-US Data Privacy Framework or the Standard Contractual Clauses.

3. Hetzner Online GmbH (hosting), Germany; servers in Germany and Finland

Servers on which the processor's services run, including the hosts that process and stream recordings, and the database. Duration: as long as the data is processed.

4. Resend, Inc. (email), USA

Delivery of transactional email to the controller and its workspace members (verification, invitations, billing notices). Duration: as long as mail is sent. Resend is a US company; transfers rely on the EU-US Data Privacy Framework or the Standard Contractual Clauses.

