Data Processing Agreement

Last updated: September 28, 2026

This Data Processing Agreement (the **“DPA”**) forms part of, and is an addendum to, the Tutorial AI Terms of Service or any other master subscription or services agreement (the **“Agreement”**) between the customer (**“Customer”**) and **VideoScripter Kft.** (**“VideoScripter”**, “we”, “us”), the provider of the Tutorial AI service (the **“Service”**). It reflects the parties’ agreement with regard to the processing of Personal Data by VideoScripter as a processor on behalf of Customer as a controller.

By accepting the Agreement, or by accessing or using the Service, Customer accepts this DPA on behalf of itself and, to the extent required, its affiliates. In the event of any conflict between this DPA and the Agreement on the subject of the processing of Personal Data, this DPA prevails.

> **Parties.** Processor: VideoScripter Kft., Káplár utca 11–13, 1024 Budapest, Hungary. Data-protection contact: legal@tutorial.ai. Controller: the Customer identified in the Agreement.

How to sign this DPA

This DPA applies as part of the Agreement and does not need to be signed. If your organization requires a signed copy:

1. Download the PDF of this DPA.
2. Complete and sign the Customer block on the signature page.
3. Email the signed PDF to legal@tutorial.ai.

VideoScripter will countersign and return a fully executed copy.

1. Definitions

Capitalized terms not defined here have the meaning given in the Agreement. **“Data Protection Law”** means all laws applicable to the processing of Personal Data under the Agreement, including the EU General Data Protection Regulation 2016/679 (**“GDPR”**) and any implementing or successor legislation. **“Personal Data”**, **“processing”**, **“controller”**, **“processor”**, **“data subject”** and **“personal data breach”** have the meanings given in the GDPR. **“Customer Personal Data”** means Personal Data processed by VideoScripter on behalf of Customer under the Agreement, as

described in Annex 1. **"Sub-processor"** means any processor engaged by VideoScripter to process Customer Personal Data.

2. Roles and scope

For Customer Personal Data, Customer is the controller and VideoScripter is the processor. VideoScripter will process Customer Personal Data only as necessary to provide the Service and as set out in Annex 1. Customer is responsible for the accuracy and lawfulness of Customer Personal Data and for having an appropriate legal basis for the processing, and warrants that its instructions comply with Data Protection Law.

3. Processing on documented instructions

VideoScripter will process Customer Personal Data only on Customer's documented instructions, including as set out in the Agreement, this DPA and Customer's configuration and use of the Service, unless required to process by applicable law (in which case VideoScripter will, where legally permitted, inform Customer of that requirement). VideoScripter will inform Customer if, in its opinion, an instruction infringes Data Protection Law. VideoScripter does not sell Customer Personal Data and does not use it for any purpose other than providing and maintaining the Service.

4. Artificial intelligence

The Service uses third-party AI models (listed on our Sub-processors page) to generate scripts and narration, transcribe audio, recognize on-screen activity, and synthesize and translate speech. VideoScripter does not use Customer Personal Data to train AI models, and requires its AI Sub-processors not to train their models on Customer Personal Data. The AI does not make automated decisions producing legal or similarly significant effects concerning any natural person.

5. Confidentiality

VideoScripter ensures that personnel authorized to process Customer Personal Data are bound by appropriate confidentiality obligations and are granted access on a least-privilege, need-to-know basis.

6. Security measures

VideoScripter implements and maintains appropriate technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, as required by Article 32 GDPR. Those measures are described in Annex 2 and may be updated from time to time, provided the overall level of protection is not materially reduced.

7. Sub-processing

Customer grants VideoScripter general authorization to engage Sub-processors to process Customer Personal Data. A current list of Sub-processors, including their locations and processing activities, is available on VideoScripter's Sub-processors page, which includes a mechanism to subscribe to notifications of new Sub-processors. VideoScripter imposes on each Sub-processor data-protection obligations no less protective than those in this DPA and remains liable for the acts and omissions of its Sub-processors. If Customer has subscribed to notifications, VideoScripter will notify Customer before authorizing a new Sub-processor; Customer may reasonably object on data-protection grounds within thirty (30) days of that notice, and VideoScripter will use commercially reasonable efforts to address the objection. If it cannot do so within a reasonable period, Customer may terminate the affected part of the Service.

8. Assistance to Customer

Taking into account the nature of the processing, VideoScripter will assist Customer by appropriate technical and organizational measures, insofar as possible, in fulfilling Customer's obligations to respond to data subject requests to exercise their rights under the GDPR. VideoScripter will also provide reasonable assistance to Customer with data protection impact assessments and prior consultations with supervisory authorities, taking into account the information available to VideoScripter.

9. Personal data breach

VideoScripter will notify Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data, and will provide Customer with information reasonably required to enable Customer to meet its own notification

obligations under Article 33 GDPR (including within the 72-hour timeframe where applicable). VideoScripter may provide this information in phases as it becomes available. Notification of a breach is not an acknowledgement of fault or liability. Except as required by Data Protection Law, these obligations do not apply to incidents caused by Customer or its authorized users.

10. International transfers

Customer content is stored and processed in the European Economic Area (the **"EEA"**). Billing and support data are processed by Stripe and Intercom in the United States under the European Commission's Standard Contractual Clauses — see our Sub-processors page. VideoScripter will not otherwise transfer Customer Personal Data outside the EEA unless it has taken measures necessary to ensure the transfer is compliant with Data Protection Law, such as an adequacy decision or the European Commission's Standard Contractual Clauses, which are incorporated by reference where applicable and prevail over this DPA in the event of conflict.

11. Return and deletion

Upon termination or expiry of the Agreement, VideoScripter will, after ninety (90) days, securely delete Customer Personal Data, unless Customer has notified VideoScripter before the end of that 90-day period that it requires the return of Customer Personal Data, and subject to any longer retention required by applicable law. Customer can export generated videos from the Service during this period. Residual copies in routine backups are deleted in accordance with VideoScripter's backup rotation and remain protected by this DPA until deleted.

12. Audits

VideoScripter will make available to Customer the information necessary to demonstrate compliance with Article 28 GDPR, primarily in the form of the security documentation, third-party certifications and audit reports it makes available. VideoScripter will also allow for and contribute to audits, including inspections, conducted by Customer or an independent auditor mandated by Customer, but only to the extent required under Data Protection Law and where the Agreement does not already provide equivalent audit rights. Any on-site audit is subject to the parties first

agreeing the scope, timing and duration, takes place no more than once per year (except following a personal data breach or where required by a supervisory authority), and Customer reimburses VideoScripter for time expended at its then-current rates. The parties will treat all audit information confidentially.

13. Liability and precedence

Each party's liability under this DPA is subject to the limitations and exclusions of liability set out in the Agreement. This DPA is without prejudice to the rights and obligations of the parties under the Agreement, which continue in full force. In the event of conflict, the order of precedence is: (1) the Standard Contractual Clauses (where applicable), (2) this DPA, (3) the Agreement.

14. Term and governing law

This DPA takes effect on the date the Agreement is entered into and remains in force for as long as VideoScripter processes Customer Personal Data. This DPA is governed by the laws of Hungary. The courts of Budapest have exclusive jurisdiction, except where the Standard Contractual Clauses require otherwise.

[Signature page follows]

Signatures

The parties' authorized signatories have executed this DPA.

On behalf of Customer

Full legal name

Address

Signatory name

Position

Signature

Date

On behalf of VideoScripter Kft.

Full legal name

Address

Signatory name

Position

Signature

Date

Annex 1 — Details of the processing

Subject matter	Provision of the Tutorial AI service (AI-assisted creation of screen-recording–based video tutorials, narration, transcripts, translation and documentation).
Duration	For the term of the Agreement, plus the return/deletion period in clause 11.
Nature and purpose	Hosting and processing of Customer-supplied screen recordings and optional audio to generate scripts, AI narration (text-to-speech), transcripts, translations and written documentation, and to host and share the resulting videos. No automated decision-making concerning natural persons.
Categories of data subjects	Customer's authorized users (e.g. creators and administrators) and any individuals whose image or voice appears in Customer-uploaded recordings.
Categories of personal data	Account and authentication data (name, e-mail address, password stored as an Argon2id hash); activity logs (username, timestamp, endpoint IP address, mouse position and typing duration — *no keystrokes, typed text or clipboard content are captured*); and any personal data contained in Customer-uploaded screen recordings (on-screen images, optional audio/voice) and the transcripts and narration derived from them.
Special categories	None intended. The Service is not designed for special-category data; Customer must not upload such data unless separately agreed in writing.

Annex 2 — Technical and organizational measures

- **Data location.** Customer content is hosted on Google Cloud in the EEA, in Belgium with disaster recovery in the Netherlands.
- **Encryption.** TLS 1.2 or higher in transit and AES-256 at rest. Passwords are hashed with Argon2id.

- **Access control.** Role-based access in the application, with organization-level mandatory two-factor authentication and Google Workspace SSO. Production access is limited to a small number of named senior engineers using phishing-resistant two-factor authentication, and all access is logged.
- **Data minimization.** Only click-region still images and sentence-level narration text are sent to AI sub-processors; the full video never leaves the platform. Domain names and e-mail addresses are anonymized before transmission.
- **Backup and recovery.** Daily backups to isolated storage, with deleted files and prior versions recoverable for 30 days and a documented, regularly tested recovery procedure.
- **Secure development.** Reviewed, pull-request–based changes, automated testing and dependency scanning, and prioritized remediation of vulnerabilities.
- **Logging, monitoring and incident response.** Application and cloud audit logs, continuous monitoring and alerting, and a documented incident-response process.
- **Certification.** ISO/IEC 27001 certification is in progress.

More detailed security documentation, including our completed security questionnaire, is available to customers on request, subject to confidentiality, at legal@tutorial.ai.