REELOOP

Data Processing Addendum

to the Reeloop Terms of Service - GDPR Article 28 processor terms for business (team) customers

Processor	APP STUDIO SASU, operating Reeloop
SIREN / RCS	917 474 207 - R.C.S. Marseille
Registered office	BT B, 18 Boulevard Reynaud de Trets, 13010 Marseille, France
VAT	FR06917474207
Version	2.0 - 13 August 2026

Contents

This Data Processing Addendum (the “DPA”) is entered into between **APP STUDIO SASU**, a societe par actions simplifiee unipersonnelle registered with the Marseille Trade and Companies Register under number 917 474 207, with its registered office at BT B, 18 Boulevard Reynaud de Trets, 13010 Marseille, France (“APP STUDIO”, the “Processor”, or “Reeloop”), and the customer identified in the signature block (the “Controller” or “Customer”), each a “Party” and together the “Parties”.

This DPA forms part of, and is incorporated into, the Reeloop Terms of Service and any order or subscription between the Parties (together, the “Agreement”) under which the Processor provides the Reeloop AI video-generation service (the “Service”). It applies where the Controller is a business or team customer and the Processor processes personal data on the Controller's behalf in the course of providing the Service.

1. Definitions

Capitalised terms not defined here have the meaning given in the Agreement.

- “GDPR” means Regulation (EU) 2016/679 and, where applicable, the UK GDPR as retained in UK law.
- “Personal Data”, “Processing”, “Controller”, “Processor”, “Data Subject” and “Personal Data Breach” have the meanings given in the GDPR.
- “Customer Data” means the Personal Data that the Controller submits to, or collects through, the Service and that the Processor processes on the Controller's behalf, including prompts, scripts, product URLs, reference media, voice samples, connected social-account tokens and generated output.
- “Sub-processor” means a third party engaged by the Processor to process Customer Data in connection with the Service.
- “SCCs” means the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries (Commission Implementing Decision (EU) 2021/914), as updated or replaced.

2. Scope, roles and subject matter

2.1 The Controller is the controller of the Customer Data; the Processor processes that data solely as a processor on the Controller's documented instructions, namely to provide, secure, maintain and improve the Service as described in the Agreement and this DPA (including Annex I).

2.2 For the avoidance of doubt, the Processor is an independent controller of the account, billing and usage data it collects to operate its own business (user accounts, payment records, security and error logs, consent-gated product analytics). That data is governed by the Reeloop Privacy Policy and is outside the scope of this DPA.

2.3 The subject matter, duration, nature and purpose of the processing, and the categories of data subjects and personal data, are set out in Annex I.

2.4 The Controller warrants that it has a lawful basis for the processing, that its instructions comply with applicable law, and that it has obtained all consents and given all notices needed for the Processor to process the Customer Data as instructed - in particular for any voice-clone, avatar or likeness reference media the Controller uploads.

3. Duration

This DPA takes effect on the date of last signature and continues for as long as the Processor processes Customer Data under the Agreement, unless terminated earlier in accordance with Section 15. The processing itself runs for the term of the Controller's subscription, subject to the retention and deletion schedule in Section 13 and Annex I.

4. Nature and purpose of processing

4.1 The Processor processes Customer Data only to: (a) generate, assemble, store and deliver AI-generated video and audio content as instructed by the Controller; (b) publish that content to third-party platforms at the Controller's instruction; (c) host, back up and secure the data; and (d) provide support.

4.2 The Processor does not sell Customer Data, does not use it for advertising, and does not use it to train a general-purpose AI model. Content generated for a customer is used only to operate and provide the Service to that customer.

4.3 Publishing to a social platform (TikTok, YouTube, Instagram) is a documented instruction from the Controller. Once posted, the content is public on that platform and governed by that platform's own terms; those platforms act as recipients, not as sub-processors of the Processor.

5. Processor obligations

The Processor shall:

- process Customer Data only on the Controller's documented instructions, including with regard to international transfers, unless required to do otherwise by EU or Member State law (in which case it will inform the Controller first, unless that law prohibits it);
- ensure that persons authorised to process Customer Data are bound by confidentiality (Section 6);
- implement the technical and organisational measures in Annex III and keep them at least as protective throughout the term;
- engage Sub-processors only in accordance with Section 8;
- assist the Controller with data subject requests and with its own compliance obligations as set out in Sections 10 and 12;
- notify the Controller of a Personal Data Breach in accordance with Section 11; and
- delete or return Customer Data at termination in accordance with Section 13.

If the Processor believes an instruction infringes the GDPR, it will inform the Controller without undue delay.

6. Confidentiality

The Processor ensures that all employees, contractors and Sub-processors who access Customer Data are subject to confidentiality obligations at least as protective as those in the Agreement, whether by contract or statutory duty, and that access is limited to those who need it to provide the Service.

7. Security of processing

7.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, the Processor implements the technical and organisational measures described in Annex III, designed to ensure a level of security appropriate to the risk.

7.2 The Controller is responsible for its own use of the Service, including securing its own credentials, managing its team members' access, and deciding what data to submit. The Controller acknowledges that no method of transmission or storage is completely secure.

8. Sub-processors

8.1 The Controller gives a general authorisation for the Processor to engage the Sub-processors listed in Annex II. The Processor keeps an up-to-date list in its Privacy Policy and in Annex II.

8.2 The Processor will give the Controller reasonable advance notice (for example by email or in-product notice) before adding or replacing a Sub-processor. The Controller may object on reasonable data-protection grounds within 14 days; the Parties will then work in good faith to resolve the objection. If it cannot be resolved, the Controller's sole remedy is to stop using the affected feature and terminate the affected order.

8.3 The Processor flows down data-protection obligations to each Sub-processor that are no less protective than this DPA, and remains fully liable to the Controller for the Sub-processor's performance.

9. International transfers

9.1 Some Sub-processors are located outside the EEA/UK, notably in the United States. Where Customer Data is transferred to a third country, the Processor ensures the transfer is covered by an approved safeguard - the EU-U.S. Data Privacy Framework where the recipient is certified, or the SCCs - as provided by each Sub-processor.

9.2 Where SCCs apply, they are incorporated by reference, with the Controller as data exporter and the Processor (or the relevant Sub-processor) as data importer, and the details in Annexes I to III completing the SCC annexes.

10. Data subject rights and assistance

10.1 Taking into account the nature of the processing, the Processor will reasonably assist the Controller, by appropriate technical and organisational measures, in responding to data subject requests to exercise their rights (access, rectification, erasure, restriction, portability, objection).

10.2 The Service provides self-serve tools for the most common actions (account deletion, content deletion, data deletion instructions, disconnecting social accounts). For anything else, the Controller may contact the Processor at support@reeloop.ai. The Processor may charge a reasonable fee for assistance that goes beyond the self-serve tools and its baseline obligations.

10.3 The Processor will also provide reasonable assistance with any data protection impact assessment or prior consultation the Controller is required to carry out, to the extent the request relates to the Service.

11. Personal data breach notification

11.1 The Processor will notify the Controller without undue delay, and in any event within 72 hours, after becoming aware of a Personal Data Breach affecting Customer Data.

11.2 The notification will describe, so far as then known: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed to address and mitigate it. The Processor will keep the Controller informed as more information becomes available. The Controller is responsible for any notification it must make to a supervisory authority or to data subjects.

12. Audits and information

12.1 The Processor will make available to the Controller the information reasonably necessary to demonstrate compliance with this DPA (including the public Privacy Policy, the security page at reeloop.ai/security and the measures in Annex III).

12.2 Where that information is not sufficient, the Controller may carry out an audit, at its own cost, at most once per year, on reasonable prior written notice and subject to confidentiality. The Processor may satisfy the audit through a current third-party certification, pen-test summary or written responses instead of an on-site inspection where that reasonably addresses the Controller's concern.

13. Deletion and return at termination

13.1 On termination of the Agreement or at the Controller's earlier written instruction, the Processor will, at the Controller's choice, delete or return the Customer Data, unless EU or Member State law requires it to keep limited records (for example billing records retained for the statutory tax and accounting period).

13.2 The operational retention schedule that applies during the term is set out in Annex I. The Controller can delete content and its account at any time from within the Service.

14. Liability

Each Party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement. Nothing in this DPA limits liability that cannot be limited under applicable law, including a Party's liability to data

subjects under GDPR Article 82.

15. Term and termination

This DPA takes effect on the date of last signature and ends automatically when the Agreement terminates, except for the obligations that by their nature survive (confidentiality, deletion/return, liability). Termination of the Agreement terminates this DPA.

16. Governing law and jurisdiction

This DPA is governed by French law. Any dispute is subject to the exclusive jurisdiction of the courts of Marseille, France, unless mandatory data-protection law provides otherwise. If any provision of this DPA conflicts with the Agreement on a data-protection matter, this DPA prevails.

Annex I - Details of the processing

Item	Detail
Subject matter	Provision of the Reeloop AI video-generation service to the Controller: script generation, AI video/image/voice generation, assembly, storage, optional publishing, hosting, security and support.
Duration	For the term of the Controller's subscription, subject to the retention and deletion schedule in this Annex and Section 13.
Nature and purpose	Processing of prompts, scripts, product URLs, reference media, voice samples and connected-account tokens to generate, assemble, store and deliver video and audio content, and to publish it at the Controller's instruction. No sale, no advertising use, no training of a general-purpose model.
Categories of data subjects	The Controller's authorised users; individuals appearing in or providing reference media (voice, likeness) uploaded by the Controller; individuals identifiable in generated content.
Categories of personal data	Account identifiers (name, email); user-submitted prompts, scripts and product URLs; reference images, voice samples and avatar/likeness media; connected social-account OAuth tokens; generated video/audio output; support correspondence. The Processor never receives or stores full payment-card numbers (handled by Stripe).
Special categories	Not intended. The Controller must not submit special-category data (GDPR Art. 9) except where it has a valid legal basis and has instructed the Processor accordingly. Voice-clone and likeness media are processed only with the consent the Controller is responsible for obtaining.
Retention during term	Studio tool outputs: deleted after 30 days. Source voiceover and transcript for a finished video: deleted 7 days after render. Failed generations: purged after 14 days. Connected-account OAuth tokens: until disconnect or account deletion. Voice-clone samples and avatar/actor reference media: until the feature or account is deleted. Finished videos: until deleted by the customer or on account deletion.
Frequency	Continuous, for the duration of the subscription.

Annex II - Authorised sub-processors

The Processor engages the following Sub-processors. This list mirrors the public Privacy Policy; the Processor will give notice before adding or replacing a Sub-processor (Section 8.2).

Sub-processor	Function	Location
Supabase	Authentication, database and file storage	USA (EU hosting available)
Vercel	Application hosting and delivery	USA / global edge
Sentry	Error tracking and diagnostics	USA
Anthropic	Script writing (AI language model)	USA
ByteDance / BytePlus (Seedance)	AI video scene generation	Singapore / global
Kling	AI video scene generation	China / global
OpenAI	Catalog-voice text-to-speech, Whisper transcription/captions, content moderation	USA
ElevenLabs	Voice cloning and cloned-voice text-to-speech	USA
Tavus	Video-avatar face replicas (when created by the customer)	USA
fal.ai	Image generation and lip-sync	USA
json2video	Assembly of scenes, audio and captions into the final video	USA
Pexels	Stock-footage clips (no personal data sent; only a topic-derived search query)	USA
Resend	Transactional email (welcome, video-ready, billing, reconnect notices)	USA

Not sub-processors for Customer Data: Stripe (payments), PostHog (product analytics) and Meta (advertising measurement) act for the Processor's own controller-side purposes - billing records and consent-gated analytics - and do not process Customer Data on the Controller's behalf. They are covered in the Privacy Policy, not in this Annex.

Publishing recipients (not sub-processors): TikTok (Content Posting API), Google/YouTube (Data API) and Meta (Instagram Graph API) receive content only at the Controller's publishing instruction and act as independent recipients.

Annex III - Technical and organisational measures

The Processor maintains the following measures, described in more detail on the public security page (reeloop.ai/security).

Domain	Measure
Encryption in transit	TLS on all connections to the Service and to sub-processors.
Encryption at rest	Encryption at rest provided by the hosting and database infrastructure (Supabase, Vercel).
Access control	Authentication via Supabase Auth; row-level security scoping data to the account/organisation; least-privilege access for staff.
Application security	Server-side validation, security headers and a content-security policy; API keys for programmatic access with rotation and expiry support; idempotency and webhook-delivery controls on the public API.
Secrets management	Provider credentials and OAuth tokens stored encrypted; no secrets in source control.
Logging and monitoring	Error tracking (Sentry) and operational logging to detect and diagnose faults and abuse.
Resilience	Managed, redundant hosting and database infrastructure with provider backups.
Data minimisation and retention	Automated daily deletion job enforcing the retention schedule in Annex I; only the minimum data is shared with each sub-processor.
Organisational	Confidentiality obligations for all personnel; single-operator scope (SASU) limiting internal access; documented incident-response handled by the operator.

Signatures

IN WITNESS WHEREOF, the Parties have executed this Data Processing Addendum as of the date of the last signature below.

PROCESSOR		**CONTROLLER**	
Entity:	APP STUDIO SASU BT B, 18 Boulevard Reynaud de Trets 13010 Marseille, France SIREN 917 474 207	Entity:	_____ _____
Signed by (name):	_____	Signed by (name):	_____
Title:	_____	Title:	_____
Signature:	_____	Signature:	_____
Date:	_____	Date:	_____