Data Processing Agreement

Effective date: October 21, 2026

https://genlook.app/dpa/versions/2026-10-21

> This is an archived version. The current version is at https://genlook.app/dpa.

This Data Processing Agreement ("**DPA**") forms part of the Genlook Terms of Service (the "**Agreement**") between:

- **the Customer**: the business that installs or uses a Genlook app, plugin, in-store try-on page or Try-On API key (the "**Service**"); and
- **Parakeet Labs SASU**, operating as Genlook, 4 Rue de la République, 69001 Lyon, France, RCS Lyon, SIREN 105 375 349 ("**Genlook**").

The Customer accepts this DPA by installing a Genlook app or plugin, by accepting the Terms of Service, or by using a Genlook API key. It replaces every earlier version. Earlier versions are listed at genlook.app/dpa/versions.

1. Definitions

- "**Data Protection Laws**" means the GDPR (Regulation (EU) 2016/679), the UK GDPR and UK Data Protection Act 2018, the Swiss Federal Act on Data Protection, the e-Privacy rules that apply to the Service, and US state privacy laws including the California Consumer Privacy Act as amended (the "**CCPA**"), each to the extent it applies.
- "**Customer Personal Data**" means the personal data described in Annex 1 that Genlook processes on behalf of the Customer when providing the Service.
- "**Shopper**" means a visitor or customer of the Customer's online or physical store, and "**End User**" means a person whose data the Customer sends through the Try-On API.
- "**Subprocessor**" means a third party Genlook engages to process Customer Personal Data.
- "**SCCs**" means the standard contractual clauses approved by the European Commission Implementing Decision (EU) 2021/914.
- "Controller", "processor", "personal data", "processing", "data subject", "personal data breach" and "supervisory authority" have the meanings given in the GDPR. "Business", "service provider", "sell" and "share" have the meanings given in the CCPA.

2. Roles

The Customer is the controller of Customer Personal Data and Genlook is its processor. If the Customer itself acts as a processor for another controller (for example an agency or a platform using the Try-On API for its own clients), Genlook acts as the Customer's subprocessor, and the Customer confirms that its controller has authorised the processing described in this DPA.

The Customer is responsible for:

- having a lawful basis for the processing and for its instructions;
- informing its Shoppers and End Users, for example by linking the Genlook shopper privacy policy at genlook.app/privacy/widget, or by using the template in the Genlook privacy policy;
- the settings it chooses in the Service, such as the photo retention window, email collection, marketing integrations, the shopping assistant and live try-on;

- not instructing Genlook to process photos of children, and not sending Genlook special categories of personal data beyond what a try-on photo inherently shows.

3. Instructions

Genlook processes Customer Personal Data only on the Customer's documented instructions, unless EU or Member State law requires otherwise. In that case Genlook informs the Customer of that legal requirement before processing, unless the law prohibits it.

The Customer's instructions are: this DPA, the Agreement, the settings the Customer chooses in the Service, and any further written instruction the parties agree on.

Genlook informs the Customer without undue delay if, in its opinion, an instruction infringes Data Protection Laws, and may suspend the processing concerned until the Customer confirms or changes it.

4. Genlook's own purposes

The Customer authorises Genlook to process Customer Personal Data for the following purposes, and only these, in addition to providing the Service to the Customer:

1. **Security, fraud and abuse prevention across the Service**, including recognising the same device, image or network across different stores and accounts through pseudonymous hashes, so that one actor cannot abuse the Service at many stores.
2. **Billing, metering and accounting**, for example counting the try-ons Genlook ran for the Customer.
3. **Aggregated statistics** that identify no person, used to operate and improve the Service and to publish industry figures. No store is named without its consent.
4. **Compliance with the law**, for example tax records or a lawful request from an authority.

For the cross-store part of purpose 1, and for purposes 3 and 4, Genlook acts as an independent controller, under its own privacy policy, and is responsible for that processing.

Genlook does not use Customer Personal Data to train AI models, does not sell or share it, does not use it for advertising, and does not use photos to identify anyone.

5. Confidentiality

Genlook ensures that every person it authorises to process Customer Personal Data is bound by a duty of confidentiality, contractual or statutory, and accesses the data only as needed to run, support and secure the Service.

6. Security

Genlook implements and maintains the technical and organisational measures described in **Annex 2**, appropriate to the risk of the processing (GDPR Article 32). Genlook may update these measures as long as the overall level of protection does not decrease.

7. Subprocessors

The Customer gives Genlook general authorisation to engage Subprocessors. The current list is in **Annex 3**. Genlook:

- imposes on each Subprocessor, by written contract, data protection obligations that offer at least the same protection as this DPA;
- remains fully liable to the Customer for the performance of its Subprocessors' obligations;

- gives at least **30 days'** notice before adding or replacing a Subprocessor, by email where Genlook holds a contact address for the Customer and in every case by updating Annex 3 and the published list.

The Customer may object to a change, on reasonable data protection grounds, within those 30 days by writing to privacy@genlook.app. The parties will discuss the objection in good faith. If they cannot resolve it, the Customer may stop using the affected part of the Service and terminate the Agreement for it, without penalty.

8. Requests from data subjects

Taking into account the nature of the processing, Genlook assists the Customer in answering requests from Shoppers and End Users exercising their rights (access, rectification, erasure, restriction, portability, objection):

- **Self-service.** Shoppers can delete their photos, results, conversations and try-on history from the try-on widget. On Shopify, Genlook acts on the platform's customer and shop redaction requests. Try-On API customers can delete an End User's photos through the API.
- **Direct requests.** The Customer authorises Genlook to act directly on an erasure request a Shopper makes through the widget or to privacy@genlook.app, and to answer an access request about the Shopper's try-on data. Genlook forwards to the Customer, without undue delay, any other request that concerns the Customer, and does not answer it except to redirect the person.
- **On request.** Genlook provides the Customer with the information it holds about a given Shopper or End User within 10 business days of the Customer's written request.

9. Assistance with security, impact assessments and authorities

Genlook assists the Customer, taking into account the nature of the processing and the information available to it, in meeting its obligations under GDPR Articles 32 to 36: security of processing, breach notification, data protection impact assessments and prior consultation of a supervisory authority. On request, Genlook provides a description of the processing, its risks and the measures in place, to support the Customer's impact assessment.

10. Personal data breaches

Genlook notifies the Customer without undue delay, and in any case within **48 hours**, after becoming aware of a personal data breach affecting Customer Personal Data. The notice includes, as far as available at the time and otherwise as soon as it becomes available:

- the nature of the breach, the categories and approximate number of people and records concerned;
- the likely consequences;
- the measures taken or proposed to address the breach and limit its effects;
- a contact point for more information.

Genlook takes reasonable steps to contain the breach and keeps a record of it. A notice is not an admission of fault.

11. Deletion at the end of the Service

Customer Personal Data follows the retention periods in Annex 1 while the Service runs. When the Customer stops using the Service:

- **Shopify**: Genlook deletes the Customer's shopper data when Shopify sends its shop redaction request, about 48 hours after the last Genlook app is uninstalled.

- **Other channels**: Genlook deletes Customer Personal Data within 30 days of the end of the Agreement or of the Customer's written request.

Before that, the Customer may ask in writing for a copy of the Customer Personal Data Genlook still holds, which Genlook provides in a common machine-readable format. Genlook may keep data it is required to keep by law, and a record of the Service it provided with every Shopper and End User identifier removed, for billing and accounting. Residual copies in backups expire within 30 days.

12. Audits

Genlook makes available to the Customer the information necessary to demonstrate compliance with GDPR Article 28 and this DPA: this DPA and its annexes, answers to a reasonable security questionnaire, and the relevant terms of its Subprocessors. Requests are limited to once per year, except after a personal data breach or when a supervisory authority requires it.

If that information is not enough to demonstrate compliance, the Customer may have Genlook audited, including through inspections, by the Customer or an independent auditor bound by confidentiality, on at least 30 days' written notice, during business hours, at the Customer's cost, and no more than once per year. The audit must not give access to other customers' data or compromise the security of the Service.

13. International transfers

Genlook stores Customer Personal Data in the European Union. Some Subprocessors process it outside the European Economic Area, as indicated in Annex 3. Each such transfer relies on an adequacy decision of the European Commission, including the EU-US Data Privacy Framework where the Subprocessor is certified under it, or on the SCCs in the Subprocessor's data processing terms.

Where the Customer is established outside the European Economic Area in a country without an adequacy decision, and Genlook transfers Customer Personal Data to the Customer, the parties agree to Module 4 (processor to controller) of the SCCs, which is incorporated into this DPA by reference. For the SCCs, the Customer is the data importer, Genlook is the data exporter, the details of Annex 1 to this DPA complete Annex I of the SCCs, and the clauses are governed by French law. For transfers subject to the UK GDPR, the UK International Data Transfer Addendum applies to the SCCs; for transfers subject to Swiss law, references to the GDPR are read as references to the Swiss Federal Act on Data Protection.

14. US state privacy laws

Where the CCPA or a similar US state law applies, the Customer is a business and Genlook is its service provider. Genlook:

- processes Customer Personal Data only for the business purposes described in this DPA, which are the limited and specified purposes for which the Customer discloses it;
- does not sell or share Customer Personal Data;
- does not retain, use or disclose it outside the direct business relationship with the Customer, or for any purpose other than those business purposes, except as the CCPA permits;
- does not combine it with personal information it receives from other sources, except as the CCPA permits, for example to detect security incidents and prevent fraud;
- complies with the CCPA and provides the same level of privacy protection the CCPA requires of businesses;
- notifies the Customer if it can no longer meet these obligations, and allows the Customer to take reasonable and appropriate steps to stop and remediate unauthorised use.

Genlook certifies that it understands and will comply with these restrictions.

15. Liability, precedence and governing law

Each party's liability under this DPA is subject to the limitations in the Agreement, except where Data Protection Laws do not allow them. In case of conflict, the SCCs prevail over this DPA, and this DPA prevails over the Agreement on data protection matters. This DPA is governed by French law and the courts of Lyon, France have jurisdiction, without prejudice to the rights of data subjects under Data Protection Laws.

16. Changes

Genlook publishes this DPA at genlook.app/dpa and keeps every earlier version at genlook.app/dpa/versions. Genlook may update it to reflect changes in the law or in the Service, and notifies the Customer of material changes at least 30 days in advance. Changes required by law or by a supervisory authority apply when the law requires.

Annex 1: Details of processing

Categories of data subjects

- Shoppers who use the try-on or browse an online store where it is installed.
- In-store visitors who use the try-on page opened by a QR code.
- The Customer's customers whose orders the store shares for attribution, including those who never used the try-on.
- End Users of the Customer's own apps and sites, through the Try-On API.
- Shoppers who receive emails the Customer sends through Genlook.

Categories of personal data

- **Photos**: the photo a Shopper or End User provides, and the generated try-on images. Photos usually show the person's face.
- **Live camera video**, during live try-on sessions, streamed and never stored.
- **Pseudonymous identifiers**: a random browser identifier, a session identifier, the cart and checkout attribution reference, and the customer number on the store when the Shopper is logged in. Through the Try-On API: the end-user identifier the Customer chooses to send.
- **Usage data**: pages and products viewed on the store, try-on events, country derived from the IP address, device and browser characteristics.
- **Order data**: order number, amounts, products, billing country, attribution reference and customer number. No name, email or postal address.
- **Email address and marketing choice**, when the Customer enables email collection, and events on emails sent through Genlook (delivered, opened, clicked).
- **Shopping assistant conversations**: messages, replies, products shown and sizing answers (such as height, a body measurement, usual size or fit preference).
- **Consent records**: that the Shopper agreed, when, the wording shown and the settings in force.

- **Security signals**: image fingerprints and photo metadata, a hashed device signal, hashed IP address, and automated safety scores (content category, number of faces detected, apparent age range).
- **Request data** through the Try-On API: hashed IP address, user agent and request metadata.

Special categories of data. None are intended. A photo can incidentally reveal information such as religious dress or a health condition. Genlook does not use photos to infer such information and does not process biometric data to identify anyone: face detection and apparent age estimation produce numbers only, and no facial template, faceprint or embedding is created.

Nature of the processing: collection, storage, AI image generation, real-time video generation, automated safety screening, conversation with an AI assistant, email delivery, analytics and attribution reporting to the Customer, deletion.

Purposes: providing the virtual try-on, live try-on, shopping assistant and store emails; reporting try-on performance and attributed orders to the Customer; keeping the Service secure; and the purposes in Section 4.

Frequency: continuous, while the Service is in use.

Retention

Data	Retention
Photos and generated images	The window the Customer chooses: 1, 3 or 7 days (7 by default). Unprocessed originals: 1 day.
Live camera video	Not stored
Share links	7 days at most
Shopping assistant conversations	13 months after the last message (temporary copy: 30 days)
Usage events	13 months
Orders	1 year; refunds and returns: 3 years
Try-on records and security signals	2 years
Consent records	5 years
Email addresses	Until the Shopper or the Customer asks for deletion, or the Customer leaves the Service

Annex 2: Technical and organisational measures

Access control

- Production access is limited to the founder. The admin console requires single sign-on with multi-factor authentication for an allowlisted account, and every access is written to an audit log before it is answered.
- Database queries from the admin console run through a read-only role that cannot see secrets.
- The Customer cannot access Shopper photos or generated images through the Service.

Encryption and storage

- Encryption in transit (TLS) on every connection, and encryption at rest by the hosting providers (Google Cloud, Render).

- Platform credentials kept in the database are encrypted (AES-256). Other secrets are kept in the hosting provider's environment configuration, never in source code.
- Photos are stored in the European Union and deleted automatically at the end of their retention window. Stored images are reached only through signed links that expire.

Minimisation and separation

- Shoppers are identified by random identifiers. IP addresses are not stored with analytics or security signals; only their hash is kept.
- Production personal data is not copied to development: development uses its own storage bucket and analytics datasets, and the development credentials cannot reach the production bucket.
- Photos are not used to train AI models.

Safety of the Service

- Every photo goes through automated safety screening (inappropriate content, apparent minors), and abusive usage is limited across stores.

Resilience and monitoring

- Managed database backups and hosting with automatic restarts.
- Error and performance monitoring (Sentry) and alerts on failures.

Incident response

- Personal data breaches are assessed, contained, recorded in a breach register and notified as set out in Section 10.

Subprocessors

- Written data protection terms with each Subprocessor (Section 7).

Annex 3: Subprocessors

Last updated: October 21, 2026.

Subprocessor	Purpose	Location
Google Cloud (Cloud Storage, BigQuery)	Photo storage, analytics warehouse	EU
Google Cloud (Vertex AI, Gemini)	AI image generation	Global (Google-managed regions)
RunPod	GPU servers for AI image generation	EU (RunPod, Inc. is a US company)
Comfy Cloud	AI image generation (specialised engine)	United States
Decart	Real-time video try-on (live sessions)	United States
Anthropic	Shopping assistant replies; size recommendation from the photo, only when the Shopper allows it	United States

Resend	Delivery of the emails the Customer sends Shoppers through Genlook	United States
Render	Application, database and ML service hosting	EU (Frankfurt)
Vercel	Hosting of genlook.app, including the in-store try-on page	United States
Cloudflare	Delivery of the widget files (sees IP addresses in transit)	Global
Sentry	Error monitoring	EU (Germany)

The Customer's commerce platform (such as Shopify) and the tools the Customer connects to the Service (such as Klaviyo or Shopify Flow) are not Subprocessors: they act under the Customer's own contracts and instructions.

Genlook: Parakeet Labs SASU, represented by Thibault Mathian, Founder.