

ReimagineHome AI by Styldod Inc.

ReimagineHome: Room Visualizer
Shopify App - Security, Privacy & Data Protection Policy
Shopify App Store Distribution | August 2026

Document ID	REIH-APP-001
Version	v1.0
Effective Date	August 2026
Document Owner	Senior Leadership / Engineering Leadership
Applies To	ReimagineHome: Room Visualizer Shopify App, merchants, shoppers, and authorized personnel

1. Purpose and Scope

This document defines the security, privacy, and data protection framework for the ReimagineHome: Room Visualizer app (the "App") distributed through the Shopify App Store. It is a standalone document covering all Shopify-specific requirements.

This policy addresses the requirements of Shopify Privacy Requirements, Shopify Protected Customer Data Requirements, Shopify Privacy Law Compliance (mandatory webhooks), the Shopify Partner Program Agreement, Shopify API Terms of Use, GDPR, UK GDPR, CCPA/CPRA, and other applicable privacy laws.

2. App Overview

ReimagineHome: Room Visualizer (the "App") is operated by Styldod Inc. ("Styldod", "we", "us"), which offers the App under its ReimagineHome AI brand. In this policy, "ReimagineHome AI" refers to Styldod Inc. The App lets a Shopify merchant add an AI-powered space visualizer to their online store. A shopper opens the widget from a product page button, uploads a photo of their space, selects products from the merchant's catalog (at most one product per furniture category), and generates an AI-powered visualization showing how those products would look in their space. The shopper can compare before and after views and add selected products to the merchant's Shopify cart to proceed to the merchant's own Shopify checkout.

The App consists of three deployable components: a Shopify admin app (React Router 7 on Vercel) for merchant onboarding, settings, and billing; a theme app extension that injects the widget on the storefront; and an embed backend (Express on AWS Lambda) that handles sessions, image processing, AI generation, and WebSocket communication.

3. Roles and Responsibilities

Party	Role
Shopify merchant	Controller of shopper personal data. Responsible for the end-user relationship, privacy notice on their storefront, consent where required, and instructing ReimagineHome AI regarding data subject requests.
ReimagineHome AI by Styldod Inc.	Processor of shopper personal data on behalf of the merchant. Controller of merchant account data (shop name, email, domain) required for app installation, billing, and support.
Shopify Inc.	Platform provider. Governs the Shopify Partner Program Agreement, API Terms of Use, and mandatory compliance webhook requirements.
Shoppers	Data subjects whose space photo and product selections are processed through the App.

4. Data Collection

4.1 Data Collected from Merchants

The following data is collected from merchants during app installation and use:

Data Element	Source and Purpose
Shop name, contact email, shop domains	Fetches via Shopify Admin GraphQL (ReihShopDomains query) during provisioning. Used for app installation, billing, and support.
Support form submissions (organization name, email, message)	Submitted by the merchant through the in-app support form. Sent to embed backend POST /v1/public/contact.
Shopify Storefront API access token	Created via storefrontAccessTokenCreate mutation during provisioning. Used to read the merchant's product catalog for the visualizer. Stored encrypted; marked select: false in default database reads; revoked on uninstall.
Shopify offline session data	Stored in Vercel Postgres via Prisma. Contains access token, refresh token, shop, scope, and session state. Deleted on app/uninstalled webhook.
Shop Install record	Created during provisioning to track the merchant's installation: shop identifier, subscription reference, credit usage, and onboarding state. Used for app operation and billing. Deletion is covered in Section 7.

4.2 Shopify API Scopes

The App requests only the following Shopify API scopes, which are the minimum necessary for its functionality:

Scope	How Used
read_products	Admin GraphQL queries: collections, product count, catalog product query for onboarding and catalog management.
read_themes	Read the main theme and templates/product.json to detect whether the product block is present.
unauthenticated_read_product_listings	Enables the Storefront API access token to read product listings for the storefront widget catalog.
unauthenticated_read_product_tags	Enables the Storefront API to read product tags for category classification in the visualizer.

4.3 Shopify Protected Customer Data Position

The App does not request read_customers, read_orders, or any other customer or order API scope. The App does not access Shopify Protected Customer Data at Level 1 or Level 2. The App does not access customer names, email addresses, phone numbers, mailing addresses, order details, shipping information, payment information, gift cards, or checkout data through Shopify APIs.

4.4 Data Collected from Shoppers

The following data is collected from shoppers who use the visualizer on the merchant's storefront:

Data Element	How Collected and Purpose
Space and property photos	Uploaded by the shopper through the widget. Client-side validation: max 25MB, longest edge downscaled to 1600px. Uploaded to S3 via a presigned URL. Used solely to generate the AI visualization.
Product selections	Selected by the shopper in the widget UI (at most one product per furniture category). Used to generate the visualization and for cart handoff.

4.5 Data Not Collected from Shoppers

- Names, email addresses, or phone numbers.
- Mailing, shipping, or billing addresses.
- Payment information, credit card details, or financial data.
- Shopify customer account details or login credentials.
- Order history, purchase history, or transaction details.
- Government-issued identification.
- Advertising cookies, marketing cookies, Google Analytics, or tracking pixels.
- We don't use IP addresses, device identifiers, or similar technical data for advertising, profiling, or cross-site tracking. Our hosting and infrastructure providers may log IP addresses and basic technical information in access logs for security, abuse prevention, and operations.

4.6 Cookies and Local Storage

The App uses no advertising or marketing cookies, no Google Analytics, and no tracking pixels.

Name / Type	Purpose and Duration
Shopify admin session cookie	Keeps merchants logged into the embedded admin app. Duration: session.
Google Fonts (third-party resource)	Loads widget fonts on the storefront. Google receives the shopper's IP address and basic technical information (such as browser type) with each request to deliver the font and operate its service, not for our advertising or profiling.

5. Legal Basis for Processing

Legal Basis (GDPR)	Application
Art. 6(1)(b) - Performance of a contract	Providing the App to the merchant; generating visualizations requested by shoppers through the merchant's store.
Art. 6(1)(f) - Legitimate interests	Security, abuse prevention, troubleshooting, and service integrity.
Art. 6(1)(a) - Consent	Where specifically required by applicable law.

For shopper data, ReimagineHome AI acts as the merchant's processor and relies on the merchant's legal basis. The merchant is responsible for any required privacy notice or consent mechanism on their storefront.

6. Purpose Limitation and Data Minimization

Data is processed only for the following purposes:

- Install and operate the App for the merchant.
- Generate AI-powered space visualizations requested by shoppers.
- Direct shoppers to the merchant's Shopify cart with selected products.
- Respond to merchant support requests.
- Maintain service security, prevent misuse, monitor performance, and troubleshoot issues.
- Meet Shopify platform requirements and applicable legal obligations.

The App collects only the minimum data required. API scopes are limited to the minimum necessary. The App does not request access to customer or order data.

ReimagineHome AI does not sell personal information. ReimagineHome AI does not share personal information for cross-context behavioural advertising.

7. Data Retention and Deletion

7.1 Retention Schedule

Data Category	Retention Period
Uploaded space photos, generated images	48 hours
Visualizer session and workflow data (anonymous usage counts, product selections, generation totals - no shopper identifiers)	Retained while the app is installed; deleted on shop/redact

Merchant account, app configuration, and Shopify access data	Retained while the app is installed. Operational data is deleted or anonymized after uninstall when the <code>shop/redact</code> request is processed. Shop id , Credit usage , Billing and subscription records are retained as required for legal, accounting, and fraud-prevention purposes.
--	---

7.2 Uninstall Behaviour (Current Implementation)

When a merchant uninstalls the App, the following occurs:

1. When a merchant uninstalls the App, Shopify sends the `app/uninstalled` webhook. The App deletes the shop's Prisma session records, calls `markShopUninstalled`, marks the installation as inactive, and triggers the embed backend's uninstall process, which sets the installation status to uninstalled and the associated organization status to revoked. The installation record is soft-deleted rather than permanently removed. Uploaded photos and generated images are deleted automatically on the 48-hour schedule in Section 7.1, independently of uninstall. Anonymous visualizer session and workflow data (usage counts only, with no shopper identifiers) is retained until the `shop/redact` request is processed, at which point it is deleted.
2. Approximately 48 hours after uninstall, Shopify sends the `shop/redact` webhook. The App processes the redaction request, scrubs the operational fields associated with the shop, and calls the embed backend's redaction process. The stored Storefront API access token is deleted, and shop-related backend sessions, media, conversation records, generations, and associated S3 objects are purged, while the `ReihShopInstall` row(the shop identifier, the subscription reference, credit usage totals, and a flag indicating whether free credits were previously consumed) is retained only where needed for required billing records.
3. After redaction, the App retains only limited information required for billing, accounting, fraud prevention, and compliance. This may include the shop identifier, subscription reference, and whether free credits were previously used. It does not retain customer contact details, shop content, access credentials, uploaded photos, or generated images.

8. Shopify Mandatory Compliance Webhooks

The App subscribes to all three mandatory Shopify compliance webhooks. Every request is verified using HMAC-SHA256 signature validation before processing; invalid signatures are rejected with `401 Unauthorized`. Verified requests are logged with shop domain, topic, and timestamp.

8.1 customers/data_request

The App does not collect, receive, or store any Shopify customer identifier. Visualizer sessions are anonymous - no customer ID, name, email, or order reference is passed to or retained by the App at any point, including at cart handoff. The App requests no customer or order scopes (Section 4.3).

A `customers/data_request` payload therefore contains no identifier matchable against App data, and there is no responsive data to export. The handler verifies HMAC, logs the event, and returns `200`.

8.2 customers/redact

For the same reason, the App holds no data linkable to an identified Shopify customer and there is no responsive data to delete. The handler verifies HMAC, logs the event, and returns 200.

Uploaded photos and generated images are deleted on the 48-hour schedule in Section 7.1, independently of this webhook. Any remaining anonymous session records are deleted on shop/redact.

8.3 shop/redact

Sent approximately 48 hours after uninstall. Unlike the customer webhooks, the App does hold responsive data. On a verified request, the App:

1. Deletes the merchant's stored Storefront API access token from both databases.
2. Calls the embed backend redaction endpoint, which deletes all visualizer sessions, media records, and generation records scoped to the merchant's organization ID, together with the corresponding objects in S3.
3. Scrubs merchant operational fields from the `ReihShopInstall` record - contact email, shop domains, widget configuration, catalog collection handles, publishable key, and onboarding state.

Shopify offline session records, including access and refresh tokens, are deleted earlier in the lifecycle on receipt of the `app/uninstalled` webhook (Section 7.2). Data segregation by organization ID (Section 12) is what makes each shop's content addressable and deletable as a unit across both the database and object storage.

Data retained after redaction. The `ReihShopInstall` row is retained in redacted form and holds only: the shop identifier, the subscription reference, credit usage totals, and a flag indicating whether free credits were previously consumed. This is retained under GDPR Art. 6(1)(c) and Art. 6(1)(f) for accounting, tax, and fraud-prevention purposes, and is deleted after 7 years. No merchant contact details, access credentials, shop content, uploaded photos, or generated images are retained.

Redaction completes within 30 days of receipt.

9. Data Subject Rights

9.1 Rights Under GDPR / UK GDPR

- Right of access - request a copy of personal data held.
- Right to rectification - request correction of inaccurate data.
- Right to erasure - request deletion of personal data.
- Right to restriction - request restriction of processing.
- Right to data portability - receive data in a structured, machine-readable format.
- Right to object - object to processing based on legitimate interests.
- Right to withdraw consent - where processing is based on consent.

-
- Right to complain - lodge a complaint with a supervisory authority.

9.2 Rights Under CCPA / CPRA

- Right to know - what personal information is collected, used, disclosed, or sold.
- Right to delete - request deletion of personal information.
- Right to correct - request correction of inaccurate information.
- Right to opt out of sale or sharing - ReimagineHome AI does not sell or share personal information.
- Right to limit use of sensitive personal information.
- Right to non-discrimination for exercising rights.

9.3 How to Exercise Rights

Merchants: email support@reimaginehome.ai. Response within 30 days (GDPR) or 45 days (CCPA), extendable where permitted.

Shoppers: contact the merchant (the store where the visualizer was used), since the merchant acts as controller. ReimagineHome AI assists merchants with verified requests as their processor.

ReimagineHome AI supports the Shopify mandatory compliance webhooks (customers/data_request, customers/redact, shop/redact) as the technical mechanism for processing data subject requests routed through the Shopify platform.

10. Subprocessors and Data Sharing

ReimagineHome AI uses Vercel to host the merchant App and to store Shopify sessions and App settings in **Vercel Postgres**; **Amazon Web Services (AWS)** to operate the visualizer backend, store and deliver uploaded room photos and generated images, and manage generation requests; and **MongoDB Atlas** to store visualizer sessions, media records, generation records, shop installation details, and subscription information. Visualization requests are processed through the **ReimagineHome AI backend**, which receives uploaded room photos, selected product images, and visualization instructions solely to generate the requested result. When generating a visualization, uploaded room photos, selected product images, and text instructions are sent to our AI infrastructure and trusted AI providers (such as OpenRouter, Vercel AI Gateway, Blackforest Labs, OpenAI and Google APIs) solely to generate the requested visualization. These providers receive only the information needed to provide this service (including normal connection data like IP address) and aren't used by us for advertising or cross-site tracking. ReimagineHome AI does not sell personal information or share it for cross-context behavioural advertising. Information may be disclosed where required by law. ReimagineHome AI does not use shopper photos or generated images to train its own models. Our cloud and infrastructure providers may retain their own service logs in accordance with their published policies.

11. International Data Transfers

ReimagineHome AI is based in the United States and processes data primarily in the US. Infrastructure evidence from the codebase indicates AWS region us-west-2 (Oregon) for Lambda, S3, SQS, and API Gateway, Vercel and MongoDB Atlas.

If a merchant or shopper is located in the EEA, UK, or Switzerland, their data may be transferred to the United States. Where required, transfers rely on safeguards including EU Standard Contractual Clauses (SCCs), the UK International Data Transfer Addendum, and equivalent mechanisms.

12. Security Controls

ReimagineHome AI applies layered security controls across encryption, authentication, access management, and input validation for the ReimagineHome: Room Visualizer app. All browser and API traffic is encrypted in transit using HTTPS/TLS, and our storage layers - Vercel Postgres, MongoDB Atlas, and Amazon S3 - rely on cloud-provider managed encryption at rest. Sensitive application-level credentials, including Shopify Storefront API tokens and third-party AI provider keys, are encrypted at rest and held in restricted database fields that are excluded from ordinary application reads. Authentication is enforced at every trust boundary: Shopify admin sessions are validated through App Bridge session tokens using Shopify's official libraries; all incoming Shopify webhooks, including the mandatory compliance webhooks, are verified by HMAC signature before any processing occurs, with invalid signatures rejected; storefront widget requests are authenticated with a per-merchant publishable key and accepted only from domains the merchant has registered as allowed origins; and internal service-to-service calls between the Shopify app and the embed backend require a shared bearer credential. The app requests only the Shopify API scopes it needs to function - notably, it does not request access to customer or order data - and the merchant's product catalog is read live from the Storefront API at request time rather than copied into our systems. Development, staging, and production run as fully separate environments with distinct URLs, databases, and API credentials, with all configuration supplied through environment variables rather than hardcoded values. The embed backend is deployed as a serverless service behind an API gateway with no direct server access, and production infrastructure access is limited to authorized ReimagineHome AI personnel on a least-privilege basis. Uploaded content is validated on both sides of the boundary, with client-side MIME type checks, a 25MB file size limit, and image downscaling, alongside server-side session validation, and request validation before any generation is queued. Data is segregated by organization throughout, so that each merchant's sessions, media, generations, and stored objects are addressable and deletable as a unit - the mechanism that allows a [shop/redact](#) request to remove a shop's shopper content across both the database and object storage.

13. Consent, Opt-Out, and Automated Decisions

13.1 Consent

The merchant (controller) is responsible for obtaining any consent required under applicable law before shoppers use the visualizer. ReimagineHome AI processes shopper data only on the basis of the merchant's instructions and the shopper's voluntary use of the visualizer.

13.2 Data Sale and Sharing

ReimagineHome AI does not sell personal information. ReimagineHome AI does not share personal information for cross-context behavioural advertising. No opt-out mechanism for sale or sharing is required for the App's current data practices.

13.3 Automated Decision-Making

The App uses AI solely to generate space visualizations based on shopper-uploaded photos and product selections. The AI generates a visual output only. The App does not make legal or similarly significant automated decisions about individuals. It does not determine housing eligibility, credit approval, pricing, employment, legal rights, or access to essential services.

14. Children's Privacy

The App is not directed to children and is not designed for anyone under 18. ReimagineHome AI does not knowingly collect information from children. Contact support@reimaginehome.ai if you believe a child's data has been collected.

15. Merchant Obligations

Merchants using the App are responsible for:

- Providing a privacy notice on their storefront covering the use of the App.
- Obtaining any consent required under applicable law.
- Responding to data subject requests from shoppers in their capacity as controller.
- Instructing ReimagineHome AI where assistance with data subject requests is required.
- Complying with the Shopify Partner Program Agreement, Shopify API Terms of Use, and applicable laws.

16. Shopify Protected Customer Data - Compliance Matrix

The following maps each Shopify requirement to how the App addresses it:

Shopify Requirement	How Addressed
L1-1: Minimum data only	Only 4 functional scopes.No customer/order scopes. See Section 4.
L1-2: Inform merchants what data you process	This policy and the App Store privacy policy. See Sections 4-6.
L1-3: Limit processing to stated purposes	Section 6 - purpose limitation.
L1-4: Respect customer consent	Section 13.1 - merchant responsible for consent.
L1-5: Respect opt-out of data sale/sharing	Section 13.2 - no data sale or sharing.
L1-6: Automated decision opt-out	Section 13.3 - no automated decisions with legal effects.

L1-7: Data protection agreements	This policy. DPA available on request.
L1-8: Apply retention periods	Section 7 - retention schedule by data category.
L2-9: Encrypt backups	S3 and MongoDB Atlas managed encryption covers backups.
L2-11: Data loss prevention	Storefront tokens excluded from default reads. No local storage of customer data. Restricted infrastructure access.
L2-13: Strong passwords	Required for all staff accounts.
L2-14: Access logs	Application and server logging with restricted access.
L2-15: Incident response policy	Security incidents are handled through an established incident response process.
L2-10 - Encrypt data in transit	All browser, API, and service-to-service traffic uses HTTPS/TLS. Storefront widget calls, Shopify webhooks, and internal Shopify app → embed backend calls are all TLS-encrypted. See Section 12.

17. Policy Changes

ReimagineHome AI may update this policy. When changes are material, the privacy policy's "Last updated" date will be updated and merchants will be notified through the App or by email.

18. Contact

ReimagineHome AI by Styldod Inc.

Email: support@reimaginehome.ai

Address: 3500 South Dupont Highway, Dover, Kent, Delaware 19901, USA.