SECURITY & TRUST

How we protect your *customers*, and your *brand*.

Last updated: 3 June 2026 · virtuemirage.com.au/security

Virtue Mirage processes biometric data — your customers' faces and bodies. We take that seriously. This document is the plain-English version of how we keep that data safe, what infrastructure sits underneath, and what we're working on next. Our full Privacy Policy at virtuemirage.com.au/privacy covers the legal detail.

The six principles

Everything we do flows from these. They're not aspirations — they're enforced in code.

Photos are deleted within seconds.
Within seconds of generating a Digital Twin, the uploaded photos are deleted from our servers. We never had them past that point. Code-enforced — not a policy promise.

Identity is one-way hashed.
Customer identity is stored as a SHA-256 hash of the email. A leaked database snapshot leaks hashes, not emails. Reverse-engineering an email from the hash is mathematically infeasible.

Brands are isolated from each other.
Every brand's customer data lives in its own dedicated partition. Brand A cannot see a single byte of Brand B's customers or vice versa — enforced at the data layer, not just by application code.

We never train AI models on your data.
We use Google Vertex AI under a B2B contract that prohibits training on customer data. We do not retain prompts, photos, or generated images for model improvement. Ever.

Customers can be forgotten.
One email or one click removes every trace of a customer from our systems and every brand on the network within 7 days. GDPR, CCPA, and Australian Privacy Act compliant.

Infrastructure is enterprise-grade.
We run on Google Cloud — ISO 27001, SOC 1/2/3, HIPAA-eligible, FedRAMP-authorized. Data is encrypted at rest with AES-256 and in transit with TLS 1.3 by default.

The photo-deletion guarantee, in detail

When a customer creates their Digital Twin, they upload one or two reference photos. Those photos hit our backend long enough to feed the AI generation pipeline — typically 30 to 90 seconds — and the originals are then irreversibly removed from Google Cloud Storage. The only thing we keep is the AI-generated Digital Twin (which doesn't contain the original photo data) and the customer's measurements.

Guest "Quick Try-On" photos — for shoppers who haven't created an account — are auto-deleted from storage within one hour. This is enforced by a Google Cloud Storage lifecycle rule, not a cron job. Storage itself removes them; no human or service can extend that window.

How your data is protected, layer by layer

LAYER	PROTECTION	STATUS
In transit	TLS 1.3 enforced by Google Cloud Run. HTTP auto-redirected to HTTPS.	**Live**
At rest	AES-256 encryption on all stored data — Google-managed keys (Firestore, GCS).	**Live**
Identity	Email addresses stored as one-way SHA-256 hashes. Plaintext email only on the master record for transactional contact.	**Live**
Tenant isolation	Per-brand Firestore subcollections. Cross-tenant access requires explicit code path; every one is audited.	**Live**
Brand auth	Shopify OAuth + HMAC validation on every webhook. No rogue domain can push or pull data.	**Live**
Admin auth	Firebase Auth + Google SSO + email allowlist. Admin role changes require code deploy.	**Live**
Self-serve links	JWT-signed HS256, 24-hour expiry. Production secrets fail loud on misconfiguration.	**Live**
Audit trail	Every measurement edit, admin action, and customer deletion records who, when, source, prior value.	**Live**
Rate limiting	Per-IP throttling on enumeration-prone and token-burning endpoints. Returns 429 + Retry-After.	**Live**
Log scrubbing	Emails, JWTs, and bearer tokens stripped from server logs before reaching Cloud Logging.	**Live**
Quick Try-On expiry	Guest photos auto-delete from storage after 1 hour via GCS lifecycle policy.	**Live**
Biometric lock	Digital Twin cannot be replaced for 3, 6, or 12 months (brand-configured). Prevents identity laundering.	**Live**
GDPR webhooks	Shopify customers/redact, customers/data_request, shop/redact installed and verified.	**Live**
Edge WAF + DDoS	Google Cloud Armor in front of the API for IP reputation + sustained-attack protection.	**Roadmap — Q3 2026**
Pen test	Independent security review by a recognised pen-test firm. Report shared on request under NDA.	**Roadmap — Q3 2026**
SOC 2 Type 2	Independent audit of our security controls over a 12-month observation window.	**Roadmap — 12 months**
CMEK	Enterprise customers can supply their own KMS key for our data at rest.	**Available — Enterprise**

What we don't do

- **We don't sell your customers' data.** Not in aggregate, not anonymised, not in any form. Our revenue is your subscription. Period.
- **We don't share data across brands without consent.** The cross-brand network is opt-in (default-on, customer-revocable), and a brand never sees data from another brand.
- **We don't train AI models on your customers' photos or your products.** Our Vertex AI contract prohibits it. We pay for inference; we do not contribute training data.
- **We don't store original uploaded photos.** They're deleted within seconds of avatar generation. Quick Try-On photos auto-expire in one hour.
- **We don't use cookies for tracking.** Only functional cookies for session continuity. No advertising IDs.
- **We don't retain data after deletion.** A "Forget me" request removes the record from every brand on the network within 7 days.

Infrastructure & vendors

We build on the same infrastructure used by Spotify, Twitter, and Shopify themselves. Every layer beneath us is certified to enterprise standards.

VENDOR	PURPOSE	CERTIFICATIONS
Google Cloud	Hosting (Cloud Run), DB (Firestore), Storage (GCS), AI (Vertex AI)	SOC 1/2/3, ISO 27001/27017/27018, HIPAA, FedRAMP High, PCI DSS
Stripe	Payment processing — we never see card data	PCI DSS Level 1, SOC 1/2
Shopify	Customer auth, app distribution, billing	PCI DSS Level 1, SOC 2
Google Workspace	Transactional email (SMTP)	SOC 1/2/3, ISO 27001, FedRAMP

Full sub-processor list at virtuemirage.com.au/subprocessors.

Compliance

- **GDPR (EU)** — Lawful basis documented per processing activity. Data subject rights honoured. Article 27 representative pending market entry threshold.
- **UK GDPR** — Same as EU. UK representative on appointment if required.
- **Australian Privacy Act + APPs** — Explicit consent for biometric data. Notifiable Data Breach scheme compliance.
- **CCPA / CPRA (California)** — Right-to-know, right-to-delete, no sale of personal information.
- **Shopify App Store** — Mandatory GDPR webhooks installed and verified. Reviewed for App Store guidelines.

Where we are honest about the roadmap

We're an early-stage company. We've put serious engineering into security from day one, but we're not pretending we have every enterprise badge yet. Here's what's coming:

MILESTONE	TRIGGER	TIMELINE
Cloud Armor (edge WAF + DDoS)	Migration to HTTPS LB with serverless NEG	Q3 2026
Independent pen test	Before 50-brand scale or first enterprise close	Q3 2026
SOC 2 Type 2 audit	100-brand milestone or first enterprise requirement	12 mo from trigger
Customer-managed encryption keys	Enterprise contract	On request
Bug bounty program	Post 100-brand scale	2027
EU/UK Article 27 representative	Crossing GDPR Article 27(2) threshold	On signal

Responsible disclosure

Found a security issue? Email **hello@virtuemirage.com.au** with the subject "Security disclosure". We acknowledge within 24 hours, triage within 72, and credit responsible reporters in our changelog if you'd like.

Please do not publicly disclose until we have shipped a fix. We will not pursue legal action against good-faith researchers.