Data Protection Framework v1

Primefleet Digital Hong Kong Limited | Effective April 2026 | Version 1.0

1. Purpose and Scope

This document establishes the first version of SneakersLite's Data Protection Framework. It defines how Primefleet Digital Hong Kong Limited ("SneakersLite") collects, processes, stores, transfers, and protects personal data and client data in the course of delivering AI-powered sneaker authentication services.

This framework applies to all data processed via the SneakersLite platform, API, and website, including data submitted by B2B clients, end consumers accessing authentication services via partner platforms, and visitors to sneakerslite.com.

2. Regulatory Compliance Commitments

SneakersLite operates as a Hong Kong-registered entity with clients and data subjects across multiple APAC jurisdictions. This framework aligns with the following regulatory requirements:

Hong Kong — Personal Data (Privacy) Ordinance (PDPO)

As the primary jurisdiction of registration, SneakersLite fully complies with PDPO requirements including data collection transparency, purpose limitation, data accuracy, data security, openness of policies, and data subject access rights.

China — Personal Information Protection Law (PIPL)

For clients and data subjects in mainland China, SneakersLite aligns data handling practices with PIPL requirements, including lawful basis for processing, cross-border transfer compliance, and data minimisation principles.

China — Data Security Law (DSL)

SneakersLite aligns with DSL requirements governing the classification, protection, and cross-border transfer of data generated or processed in connection with activities in mainland China.

Singapore — Personal Data Protection Act (PDPA)

For clients and data subjects in Singapore, data handling practices align with PDPA requirements including purpose limitation, consent, and data protection obligations.

3. Data Classification Policy

SneakersLite classifies all data into four categories:

Category A — Personal Identifiable Information (PII)

Includes: client contact details, billing information, authorised representative names, email addresses.

Handling: encrypted at rest and in transit, access restricted to authorised personnel, retained only for the duration of the contractual relationship plus applicable statutory periods.

Category B — Client Business Data

Includes: API keys, authentication volume data, cost structures, client lists, commercial terms.

Handling: treated as commercial confidential information per service agreements, not disclosed to third parties, access restricted on a need-to-know basis.

Category C — Authentication Image Data

Includes: sneaker images submitted via API for authentication.

Handling: processed solely for delivering authentication results, used for anonymised model training only with client consent per service agreement, ownership retained by the submitting client, not sold or disclosed to third parties.

Category D — Public Data

Includes: anonymised authentication statistics, aggregated platform metrics, published content.

Handling: no restrictions on access or use.

4. Data Flow Summary

Authentication API Flow

Client submits sneaker images via API → Images received by SneakersLite API Gateway (AWS, APAC region) → Pre-processing and standardisation → Visual feature analysis and tag authentication → Authentication confidence score generated → Result returned to client via API → Images stored temporarily for quality assurance → Anonymised data retained for model training (with consent) → Raw images deleted per retention schedule.

Website Contact Form Flow

Personal data collected via sneakerslite.com contact form → Transmitted via Resend email API → Received by SneakersLite team → Used solely for responding to the enquiry → Not added to marketing lists without explicit consent.

5. Data Retention Schedule

Data Type	Retention Period	Deletion Method
Authentication images (raw)	90 days post-authentication	Secure deletion from AWS S3
Authentication results and confidence scores	Duration of client contract + 1 year	Secure deletion
Client PII (contact, billing)	Duration of contract + 7 years (statutory)	Secure deletion

Data Type	Retention Period	Deletion Method
API call logs	12 months	Automated log rotation
Website enquiry data	24 months	Manual deletion on request
Anonymised training data	Indefinite (no PII retained)	N/A

6. Data Security Measures

Infrastructure

All data is hosted on AWS infrastructure in the APAC region. Components include EC2 (compute), RDS (database), S3 (storage), CloudFront (CDN), Shield (DDoS protection), and ACM (SSL/TLS certificates).

Encryption

All data encrypted at rest using AES-256. All data in transit encrypted using TLS 1.3 minimum.

Access Control

Role-based access control (RBAC) applied to all internal systems. API authentication required for all client-facing endpoints. Access logs maintained and reviewed.

Security Monitoring

Continuous monitoring via AWS CloudWatch. Incident response plan maintained and reviewed quarterly.

API Security

All API endpoints require authenticated requests. Rate limiting applied to prevent abuse. Requests validated for format and integrity before processing.

7. Cross-Border Data Transfer Policy

SneakersLite processes data on behalf of clients in Hong Kong, mainland China, and Singapore. Cross-border data transfers are conducted under the following conditions:

Transfers from mainland China comply with PIPL cross-border transfer requirements including applicable security assessments where required by law. Clients are responsible for ensuring that data submitted to SneakersLite's API has been collected lawfully in their jurisdiction and that cross-border transfer to SneakersLite's Hong Kong infrastructure is permitted under applicable local law. SneakersLite does not transfer client data to jurisdictions outside of its contracted cloud infrastructure providers (AWS APAC) without client consent.

8. Data Subject Rights

SneakersLite respects and supports the exercise of data subject rights under applicable law. Data subjects may request:

- **Access:** A copy of personal data held about them
- **Correction:** Amendment of inaccurate personal data
- **Deletion:** Erasure of personal data where no legal basis for retention exists
- **Objection:** Objection to specific processing activities

Requests should be submitted to: chrisxue@novelship.com. SneakersLite will respond within 30 days of receiving a valid request.

9. Data Breach Notification Procedure

In the event of a confirmed data breach affecting personal data:

1. Internal escalation to CEO within 2 hours of detection
2. Containment measures implemented immediately
3. Scope and impact assessment completed within 24 hours
4. Affected clients notified within 72 hours of confirmed breach
5. Regulatory notification to the Office of the Privacy Commissioner for Personal Data (PCPD) in Hong Kong where required by law
6. Post-incident review completed within 14 days

7. Remediation plan documented and implemented

10. Third-Party Data Processors

Processor	Purpose	Data Processed	Location
Amazon Web Services	Cloud infrastructure	All platform data	APAC
Vercel	Website hosting and deployment	Website traffic data	Global CDN
Sanity.io	Blog content management	Public content only	Global
Resend	Transactional email	Contact form enquiries	Global

11. Data Subject Access Request (DSAR) Procedure

1. Request received via chrisxue@novelship.com
2. Identity of requestor verified within 5 business days
3. Data retrieval completed within 20 business days
4. Response provided in writing within 30 days of verified request
5. Complex requests may be extended by up to 30 additional days with notification to requestor
6. Requests that cannot be fulfilled responded to with explanation

12. Framework Review and Updates

This framework will be reviewed and updated:

- Annually as a minimum
- Following any material change to data processing activities

- Following any regulatory change affecting applicable data protection laws
- Following any data breach or security incident

Document version: 1.0

Effective date: April 2026

Next review date: April 2027

Document owner: Chris Xue, CEO, Primefleet Digital Hong Kong Limited