

SCALEON ERP — Personal Information Protection Standard

Document ID	Version	Effective date	Next review	Owner / Approver
SCL-PIPS-001	1.0	October 14, 2026	Annually, or after an incident or material change	Gabriel Molina Teramoto, Founder — Security & Privacy Owner / DPO

Organization: SCALEON ERP (scaleonerp.com.br) — legal entity NICOLAS GOMES LIMA, CNPJ 59.770.797/0001-59, Brazil. **DPO (Encarregado) contact:** privacidade@scaleonerp.com.br. **Privacy Policy:** <https://scaleonerp.com.br/privacidade>

Relationship to other documents: this Standard is SCALEON's internal personal data protection policy under the LGPD. It complements the *Information Security & Data Protection Program v1.1* (published at <https://scaleonerp.com.br/security>), whose controls it references. Annex A maps every questionnaire answer to its evidence.

1. Purpose, scope and legal basis

Defines how SCALEON collects, uses, stores, shares and deletes personal information in the SCALEON ERP, a multi-tenant SaaS for order, inventory, production and fulfillment management used by TikTok Shop sellers in Brazil. Applies to all personal data received through the TikTok Shop Open API or uploaded by sellers, and to all staff, contractors, systems and sub-processors. Implements the Brazilian General Data Protection Law (LGPD — Law 13.709/2018), ANPD regulations and the TikTok Shop Developer Terms.

2. Roles

- For TikTok Shop buyer data, the seller is the **controller** and SCALEON is the **processor (operador)**, acting only on the seller's documented instructions and within the scopes the seller authorizes (LGPD Art. 39).
- For seller user account data (name, e-mail, login), SCALEON is the controller.
- Security & Privacy Owner / DPO:** the Founder — accountable for this Standard, handles requests from data subjects, sellers, TikTok Shop and the ANPD (LGPD Art. 41).
- Lead Developer:** implements and operates technical controls. **All staff and contractors:** follow this Standard and report incidents immediately.

3. Personal data inventory and purpose limitation

Category	Data	Purpose	Classification
Buyer order data (TikTok Shop API)	Buyer name, shipping address, phone, order details	Fulfillment: picking, packing, shipping labels, tracking	Confidential – Personal
Seller user data	Name, e-mail, role, credentials (hashed), access logs	Account management, authentication, audit	Confidential – Personal
Workshop contacts (production)	Contact names, phones, addresses (not buyers)	Production freight (Lalamove)	Confidential – Personal
Secrets	App secret, OAuth tokens, DB credentials, API keys	Integration and system operation	Confidential – Secrets

- Minimization:** only the TikTok Shop API scopes needed for orders, products, inventory and fulfillment are requested.
- Purpose limitation:** data is used only to serve the authorizing seller. It is never sold, rented, used for advertising or profiling, shared with other sellers, or used to contact buyers outside TikTok Shop.
- Customer data is not exported to personal devices or spreadsheets unless strictly necessary, and such files are deleted after use. Development environments never use production customer data.

4. Security of personal data

Personal data is protected by the controls of the Security Program v1.1, summarized here:

- **Encryption:** TLS 1.2+ for all traffic (browser, database, TikTok Shop API, sub-processors). TikTok Shop tokens encrypted by the application with AES-256-GCM; database, files and secrets use provider-managed encryption at rest. RSA-1024 or weaker is prohibited. (Program §6)
- **Access control:** least privilege; only the Founder and Lead Developer have production access, with individual named accounts and MFA; RBAC and tenant isolation (every record scoped by seller tenant ID); access reviewed at least every 6 months and revoked within 24 hours on departure or role change. (Program §5)
- **Daily baseline:** mandatory MFA on admin accounts, 12+ character passwords in a password manager, no shared accounts, screen lock after max 5 minutes, clean desk / clear screen; awareness training at onboarding and annually. (Program §4)
- **Endpoints:** anti-malware (Microsoft Defender or equivalent), automatic updates and disk encryption, checked quarterly. (Program §3)
- **Network:** fully managed cloud, HTTPS only, provider firewall and DDoS protection, segregated Production / Preview / Development. (Program §2)
- **Vulnerabilities:** Dependabot, npm audit and secret scanning; critical/high fixed within 7 days, medium within 30 days. (Program §8)

5. Data location and sub-processors

Sub-processor	Purpose	Personal data	Location
Neon	Managed PostgreSQL (primary data store)	Orders, buyer shipping data	Brazil (São Paulo)
Vercel	Hosting, serverless runtime, logs	All application data in transit	United States
Vercel Blob	File storage and backups	Shipping labels, attachments, backups	Per Blob store region
Labelary	ZPL label rendering	Label content incl. buyer data	United States
Resend	Transactional e-mail	Recipient name / e-mail	United States
Inngest	Background jobs	Job identifiers and metadata	United States
GitHub Actions	Weekly backup job	None stored	United States
Lalamove	Production freight	Workshop contacts (not buyers)	Brazil

Personal data is stored primarily in Brazil; application processing and some files occur in the United States. International transfers rely on LGPD Art. 33 safeguards (sub-processors' data processing terms and standard contractual clauses). Sub-processors are used only under data processing terms with security obligations equivalent to this Standard; changes to this list are reflected in this Standard and the Privacy Policy.

6. Data subject rights and requests from sellers or TikTok Shop

- SCALEON assists sellers and TikTok Shop to access, correct, delete or provide personal data upon request of data subjects (LGPD Art. 18).
- Requests are received at privacidade@scaleonerp.com.br or through the TikTok Shop partner channel, logged, verified and fulfilled **within 15 days**, or sooner when TikTok Shop or the law requires.
- Requests a buyer sends directly to SCALEON are forwarded to the responsible seller (controller), and SCALEON executes the seller's or TikTok Shop's instructions.

7. Retention and deletion

Data	Retention
Shipping label PDFs	Automatically deleted after 10 days
Printed tracking-code records	Kept 30 days
Database backups	Last 4 weekly + 1 monthly, kept up to 12 months, then expire

Data	Retention
Other seller data	While the seller account is active, or as required by law, and never longer than the TikTok Shop Developer Terms allow
TikTok Shop tokens on de-authorization / contract end	Deleted immediately
All seller marketplace data at contract end or on request (incl. de-authorization)	Permanently deleted from database and file storage within 30 days; deletion logged and confirmed to the requester

8. Incident response and breach notification

- Steps: Report (immediately) → Triage and incident record (within 4 hours) → Contain → Notify → Recover → Post-incident review (within 10 business days).
- TikTok Shop (Partner Center ticket and partner@tiktokshop.com) and affected sellers are notified **without undue delay and within 24 hours** of confirming a suspected or identified breach, describing the incident, data and tenants involved, containment and a contact point.
- The ANPD and data subjects are notified when required by LGPD Art. 48. Incidents are recorded, and an incident tabletop exercise is performed at least annually.

9. Governance and review

- Staff and contractors are bound by confidentiality obligations and receive data protection guidance at onboarding and at least annually.
- This Standard is reviewed at least annually and whenever processing, sub-processors, law or TikTok Shop requirements change; versions are kept with their change history.
- Non-compliance leads to access revocation and contractual or disciplinary measures.

Annex A — Evidence map for the TikTok Shop Security & Privacy Questionnaire

PIPS = this Standard. Program = Information Security & Data Protection Program v1.1.

Questionnaire item	Answer	Evidence
Published information security policy or program	Yes	Program §1 (https://scaleonerp.com.br/security)
Network segregation and threat monitoring	Yes	Program §2; PIPS §4
Antivirus on company endpoints	Yes	Program §3; PIPS §4
Security baseline (screen lock, passwords, clean desk, MFA)	Yes	Program §4; PIPS §4
Access control policy / least privilege	Yes	Program §5; PIPS §4
Data classification and encryption in transit / at rest	Yes	Program §6; PIPS §3–4
Incident response policy with roles and channels	Yes	Program §7; PIPS §8
Vulnerability / threat management	Yes	Program §8; PIPS §4
Breach in last 3 years	No	—
Regulatory complaint in last 3 years	No	—
Countries where data is stored / processed	Brazil, United States	PIPS §5; Program Annex A
Internal personal data protection policy, regularly updated	Yes	This Standard (PIPS); Program §9
Help sellers / TikTok delete, update, provide data	Yes	PIPS §6; Program §10
Privacy policy regularly updated	Yes	https://scaleonerp.com.br/privacidade
Data Protection Officer	Yes — privacidade@scaleonerp.com.br	PIPS §2
Breach notification process to TikTok / sellers	Yes	PIPS §8; Program §11
Delete all customer data at end of relationship	Yes	PIPS §7; Program §10

Approved by: Gabriel Molina Teramoto, Founder — Security & Privacy Owner / DPO Date: October 14, 2026

Signature: _____