Scan2Tray

Information Security Policy

Organisation: Scan2Tray Ltd (Company No. 17096824), Hilton Hall, Hilton Lane, Essington, Wolverhampton, WV11 2BQ, United Kingdom

Document owner: Paul Hinett, Director **Version:** 1.2 **Effective:** 24 September 2026

Review cycle: Annual, or after any material change **Contact:** hello@scan2tray.com

1. Purpose and scope

Scan2Tray Ltd ("Scan2Tray") provides a fulfilment tool for live-commerce sellers. Sellers connect marketplaces such as Whatnot, eBay Live and TikTok Shop; Scan2Tray receives their sale and order data, assigns each buyer's items to a physical tray, prints tray labels, and reorders the marketplace's shipping-label PDF so it matches the trays. This policy sets out how Scan2Tray protects the information it processes to deliver that service.

It applies to all Scan2Tray systems and to everyone who operates them: the production API and databases, the seller web application, the desktop application, the mobile scanning application, and the integrations with marketplace APIs including the TikTok Shop Open API. It applies to all staff and contractors with access to any of those systems.

2. Roles and responsibilities

- **Director / Security owner** is accountable for this policy, approves production access, owns incident response, and reviews the policy at least annually.
- **Engineers** follow the secure-development and access-control requirements below and report suspected security issues immediately.
- **Sellers (customers)** control which marketplaces they connect and can disconnect any integration at any time from the application's settings.

3. Information we process and how it is classified

Category	Examples	Classification
Seller account data	Name, email, mobile number, hashed password, subscription status, marketplace usernames	Confidential
Marketplace order data	Order identifiers, order status, item descriptions, SKUs, quantities, prices, buyer identifiers and buyer display names supplied by the marketplace, tracking numbers, shipping-label PDFs uploaded by the seller	Confidential (contains buyer personal data)
Marketplace credentials	OAuth access and refresh tokens, shop identifiers and ciphers issued by the marketplace	Restricted

Operational data	Application logs, proxy access logs, scan events, diagnostics	Internal

Data minimisation. We request only the marketplace API scopes needed to read orders and identify the authorised shop. For TikTok Shop we store the order identifier, status timeline, line items, the buyer's platform user identifier and the masked buyer contact fields returned by the API. We do not request or store payment card data; payments are handled by Stripe.

4. Access control

4.1 Customer access

- Authentication uses short-lived signed JSON Web Tokens with rotating refresh tokens. Google sign-in is offered as an alternative using OAuth 2.0 with server-side code exchange.
- Passwords are stored only as salted BCrypt hashes. Password reset and email verification use single-use, time-limited tokens.
- Every request is scoped to the caller's organisation. Data belonging to one seller is never returned to another.
- Role-based access within an organisation: owners manage settings, billing and integrations; packer sub-accounts are restricted to scanning and packing endpoints on a default-deny allow-list.
- Login and device-pairing endpoints are rate-limited per client IP to resist credential stuffing and enumeration.
- Sellers can revoke a connected marketplace at any time; the stored tokens are marked revoked and are no longer used.

4.2 Administrative and production access

- Production servers accept SSH with key-based authentication only; password authentication is disabled. Day-to-day administration is performed over a private WireGuard overlay network.
- The production database is not reachable from the public internet; it is accessible only from the application containers on the same host and over the private overlay network.
- Administrative functions in the web application require a separate admin claim issued only to Scan2Tray staff. Partner-tier admin access is limited to an explicit allow-list of endpoints and is scoped to the partner's own customers.
- Access is granted on a least-privilege basis, is reviewed when roles change, and is removed promptly when no longer required.

5. Protecting data in transit and at rest

- All customer, marketplace and internal traffic to Scan2Tray services uses HTTPS with TLS 1.2 or higher. Certificates are issued and renewed automatically. Plain HTTP is not served.
- Outbound calls to marketplace APIs, Stripe and email providers use HTTPS only.
- Application secrets (signing keys, marketplace app secrets, API keys, database credentials) are supplied to the runtime as environment variables managed by the deployment platform. They are

never committed to source control; production keys are distinct from development and test keys, and the service refuses to start in production if a required secret is missing.

- Marketplace OAuth tokens are held server-side only. They are never sent to the browser, desktop or mobile applications.
- Marketplace OAuth access and refresh tokens are encrypted at the application layer (AES-256-GCM, per-value nonce) before they are written to the database, so a database export alone cannot yield usable credentials.
- Seller passwords are stored only as salted BCrypt hashes.
- Uploaded shipping-label PDFs are stored on an access-controlled server volume that is not web-accessible; they are served only through authenticated, organisation-scoped API endpoints.
- Staff endpoints use full-disk encryption (FileVault / BitLocker). Block-level encryption of the production data volume is scheduled for Q4 2026; until then the volume is protected by the network and host controls in section 6 and by provider physical security.
- Hosting is with Hetzner in EU data centres; physical and environmental security is provided by the hosting provider under its ISO 27001 certified controls.

6. Network security and segregation

- **Perimeter.** A cloud firewall in front of the production host permits only the HTTPS/HTTP ingress ports, SSH and the ports required by the remote-support relay. All other ports, including the database, monitoring dashboards and container management interfaces, are blocked from the internet.
- **Single ingress.** All application traffic enters through one reverse proxy that terminates TLS and routes by hostname. Application containers do not expose ports directly.
- **Segregated container networks.** Each deployed service runs in its own container on an isolated Docker network; services can only reach the peers they are explicitly attached to. The production database sits on an internal network with no published port.
- **Administrative plane.** Server administration, database access and deployment tooling are used over a private WireGuard overlay network (Tailscale) with per-device keys, separate from customer traffic.
- **Host hardening.** Operating-system security updates are applied automatically; a host firewall (UFW) with a default-deny inbound policy is active alongside the cloud firewall.
- **Monitoring and threat prevention.** Reverse-proxy access logs are retained with rotation and reviewed when anomalies are detected; abusive sources are blocked by per-IP firewall rules and application-level rate limiting on authentication and device-pairing endpoints, which returns HTTP 429 and alerts the security owner on sustained abuse.

7. Marketplace integrations and webhooks

Integrations are built to the marketplace's published security requirements. For the TikTok Shop Open API specifically:

- Sellers authorise Scan2Tray through TikTok's OAuth flow. The authorisation state parameter is signed and time-limited to prevent cross-site request forgery.
- Every inbound webhook is verified against TikTok's HMAC-SHA256 signature over the raw request body before any processing. Requests that fail verification are rejected with HTTP 401 and are not stored.
- Webhook deliveries are de-duplicated on TikTok's notification identifier so retries cannot create duplicate orders or labels.
- Access tokens are refreshed automatically ahead of expiry. When a seller de-authorises the app, or a refresh fails, the connection is marked revoked and no further API calls are made on that seller's behalf.
- API calls are signed as required by the platform and are rate-limit aware; the integration backs off on HTTP 429 responses.

8. Secure development and change management

- All source code is held in version control. Changes are made on branches and merged to the main branch, which is the only branch deployed to production.
- Automated tests cover the security-relevant logic (signature verification, order matching, access rules) and run before every release.
- Dependencies are pinned and updated regularly; security advisories for the .NET, Node and Rust ecosystems are monitored.
- Desktop application releases are cryptographically signed and distributed through a signed auto-updater so users cannot be served tampered builds.
- Production deployments are automated from the main branch through the deployment platform, giving a full history of what was deployed and when.

9. Logging, monitoring and alerting

- The API logs authentication events, authorisation failures, rate-limit triggers, webhook receipts (with signature outcome), and administrative actions. Secrets and tokens are redacted from logs.
- Reverse-proxy access logs are retained with rotation and are used to identify abusive traffic; per-IP blocking rules can be applied without a deployment.
- Database health is monitored continuously and the security owner is alerted by email when connection saturation or transaction leaks are detected.
- High-volume diagnostic traces are automatically deleted after 14 days.

10. Backup and availability

- The production database is backed up automatically every day and backups are retained for at least 30 days on storage separate from the live database.
- Uploaded label files are stored on a persistent volume that is included in the host backup schedule.
- Restore procedures are documented and are tested at least annually.

- The desktop application keeps an encrypted local journal during a live show so that a temporary loss of connectivity does not lose sales; the journal is replayed to the server when connectivity returns.

11. Incident response

A security incident is any actual or suspected unauthorised access to, disclosure of, alteration of, or loss of Scan2Tray data or systems.

1. **Detect and report.** Anyone who suspects an incident reports it to the security owner immediately at hello@scan2tray.com.
2. **Contain.** Revoke affected credentials and tokens, block abusive sources, and isolate affected systems. Marketplace tokens can be revoked per shop without affecting other sellers.
3. **Assess.** Establish what data and which sellers or buyers are affected, and how.
4. **Notify.** Affected sellers are informed without undue delay. Where personal data is involved, the Information Commissioner's Office is notified within 72 hours as required by UK GDPR. Marketplace partners, including TikTok Shop, are notified in line with their partner terms where their data or platform is involved.
5. **Review.** A post-incident review identifies the root cause and the changes needed to prevent recurrence; this policy is updated where required.

12. Data retention and deletion

- Seller account and show data is retained while the account is active so that sellers can review, reprint and reconcile past shows.
- Marketplace OAuth tokens are retained only while the connection is active and are invalidated on disconnect or de-authorisation.
- Sellers may request deletion of their account and data at hello@scan2tray.com; requests are completed within 30 days, subject to any legal obligation to retain billing records.
- Diagnostic traces are deleted after 14 days; proxy access logs are rotated and retained for no more than 7 days.

13. Third-party service providers

Provider	Purpose	Data involved
Hetzner Online GmbH	Server hosting (EU)	All service data
Stripe	Subscription billing	Billing contact and payment details (held by Stripe)
ZeptoMail (Zoho)	Transactional email	Email address, message content
Google	Optional sign-in (OAuth)	Email address, name

Microsoft Azure Speech	Optional spoken scan feedback	Short non-personal phrases
Apple App Store / Google Play	Mobile app distribution	None beyond store accounts

Providers are selected for appropriate security certifications and are bound by their published data-processing terms. No provider is given marketplace API tokens.

14. Compliance

Scan2Tray Ltd is a company registered in England and Wales (No. 17096824) and is the data controller for seller account data and a processor of marketplace order data on behalf of sellers. Scan2Tray processes personal data in accordance with the UK General Data Protection Regulation and the Data Protection Act 2018, and, for EU sellers, the EU GDPR. Marketplace data is used solely to provide the fulfilment service the seller has requested and is handled in line with each marketplace's partner and developer terms, including the TikTok Shop Partner Center Terms of Service and data-use policies.

15. Policy maintenance

This policy is reviewed at least annually and whenever there is a material change to systems, integrations or applicable regulation. Changes are approved by the security owner and the version and effective date above are updated.