

Personal Data Protection Policy

Scan2Tray Ltd (Company No. 17096824) · Version 1.0 · 24 September 2026 · Owner: Paul Hinett, Director · hello@scan2tray.com

Internal policy. Supplement to the Scan2Tray Information Security Policy; the public-facing statement is the Privacy Policy at scan2tray.com/privacy.

1. Purpose and scope

This internal policy sets out how Scan2Tray Ltd handles personal data so that it complies with the UK General Data Protection Regulation, the Data Protection Act 2018 and, for EU sellers and buyers, the EU GDPR. It applies to all staff and contractors and to all personal data processed in the course of providing Scan2Tray, whether about sellers (our customers), their buyers, prospective customers, partners or staff.

2. Our roles

Data	Our role	Notes
Seller account data (name, email, phone, password hash, billing status, marketplace usernames)	Controller	Collected to provide and bill the service.
Buyer data received from marketplaces or uploaded by sellers (buyer identifiers and display names, names and addresses on shipping labels, order contents, tracking numbers)	Processor on behalf of the seller	The seller is the controller (alongside the marketplace). We process it only to assign, label and reconcile their shipments, on the seller's instructions, under our Terms of Service.
Website visitors, enquiries, onboarding-call bookings, affiliates and partners	Controller	Collected to respond, onboard and run partner programmes.
Staff and contractor data	Controller	Employment and engagement administration.

3. Principles we apply

Principle	How we meet it
Lawfulness, fairness, transparency	Seller data is processed to perform our contract with them (Art. 6(1)(b)); service emails, abuse prevention and security rely on legitimate interests (Art. 6(1)(f)); marketing emails rely on consent or the soft opt-in with an unsubscribe on every message. The public Privacy Policy explains what we do in plain language and is kept current.
Purpose limitation	Buyer data is used only for fulfilment of the seller's own orders. It is never used for marketing, profiling, resale or any purpose of our own.
Data minimisation	We request the minimum marketplace API scopes (orders and shop identity only). From TikTok Shop we store the order identifier, status, line items, the buyer's platform user identifier and the masked contact fields the API returns; we do not request buyer addresses from the API. Payment card data is never collected; Stripe holds it.

Accuracy	Sellers can correct their account details in the app at any time; marketplace order data is refreshed from the marketplace as it changes.
Storage limitation	Retention periods in section 6. Diagnostic traces are deleted automatically after 14 days; marketplace tokens are invalidated on disconnect.
Integrity and confidentiality	The technical and organisational measures in the Information Security Policy, Access Control Policy and Data Classification & Encryption Standard: TLS everywhere, organisation-scoped access, role-based permissions, encrypted marketplace tokens, hashed passwords, private administration network, logging and incident response.
Accountability	The Director owns this policy, keeps the records in section 8, reviews the policy annually and approves any new processing.

4. Individuals' rights and requests

We assist sellers, their buyers and marketplace partners (including TikTok Shop) with requests to access, correct, delete, restrict, port or object to the processing of personal data.

- **Channel:** requests are accepted at hello@scan2tray.com, from within the app, or relayed to us by a marketplace partner. The address is published in the Privacy Policy and on scan2tray.com/security.
- **Verification:** we confirm the requester's identity or, for buyer data, that the request comes from the seller who controls it or from the marketplace on the buyer's behalf.
- **Timescale:** requests are acknowledged within 2 working days and completed within one month (extendable by two months for complex requests, with the requester told why). Marketplace-relayed deletion requests are completed within the timescale the partner's terms require, and in any case within 30 days.
- **Buyer requests received directly:** because we act as a processor for buyer data, we tell the buyer which seller controls it, notify that seller, and carry out the seller's or marketplace's instruction. We do not refuse or delay a request because it arrived at the wrong door.
- **What deletion covers:** the seller's account, organisation, shows, trays, items, uploaded label files, scan events, marketplace connections and tokens, and backups on their normal expiry cycle. Billing records required by law are retained (section 6).
- **Portability:** seller data is provided in a structured, commonly used, machine-readable format (JSON or CSV) on request.
- **Record:** every request, the identity check, the action taken and the completion date are logged.

5. Sharing and transfers

- Personal data is shared only with the sub-processors listed in the Privacy Policy (hosting, payments, transactional email, sign-in, speech synthesis, app distribution) and only as needed to run the service. Each is bound by a data-processing agreement or equivalent published terms.
- Production data is hosted in the EU (Hetzner, Finland/Germany). Where a sub-processor processes data outside the UK or EEA, transfers rely on UK adequacy regulations, the UK International Data Transfer Agreement or EU Standard Contractual Clauses.
- Buyer data is never disclosed to other sellers, partners or third parties, and is never sold.
- Marketplace data is used only within the scope the seller authorised and in line with each marketplace's developer and data policies, including the TikTok Shop Partner Center terms; it is deleted when the seller revokes the connection or on the marketplace's instruction.

6. Retention

Data	Retention
Seller account, shows, trays, items, label files	While the account is active, so sellers can review, reprint and reconcile past shows; deleted within 30 days of an account deletion request or 12 months after an account is closed.
Marketplace access/refresh tokens	Only while the connection is active; invalidated on disconnect, revocation or expiry.
Marketplace webhook events and hydrated order records	Same lifetime as the show they belong to.
Billing and invoice records	6 years after the end of the financial year, as required by HMRC.
Support conversations, onboarding-call bookings	24 months after the last message.
Diagnostic traces / desktop capture diagnostics	14 days.
Proxy access logs	About 7 days (rotated).
Security incident records	3 years.

7. Breach handling

A personal-data breach is handled under the Incident Response Policy: contain immediately, assess within 24 hours, notify the ICO within 72 hours of becoming aware where the breach is likely to result in a risk to individuals, notify affected sellers without undue delay, and notify the relevant marketplace partner where its data or platform is involved. Every breach, notifiable or not, is recorded with the facts, effects and remedial action.

8. Governance and records

- The Director is responsible for data protection. Scan2Tray is not required to appoint a Data Protection Officer under Article 37 (it is not a public authority and does not carry out large-scale monitoring or special-category processing); the Director acts as the data protection contact at hello@scan2tray.com.
- A record of processing activities (purposes, categories, recipients, retention, security measures) is maintained and updated when processing changes.
- A data-protection impact assessment is carried out before any new processing likely to result in a high risk to individuals, including any new marketplace integration that changes the categories of buyer data received.
- Staff and contractors are briefed on this policy when they join and at each annual review; everyone with access to personal data signs up to the Operational Security Baseline.
- Individuals have the right to complain to the Information Commissioner's Office (ico.org.uk); the Privacy Policy says so.

9. Review

This policy is reviewed at least annually and whenever the law, our processing or our sub-processors change. Version history is kept with the document sources.