Standard Data Processing Agreement (DPA)

Effective date: 25 November 2026 · Version 1.0

1. Parties and roles

The Customer is the Data Controller. Neta Ofis Kırtasiye Sanayi Ticaret Limited Şirketi (Yenibosna Merkez Mah. Kavak Sok. No:3A, Bahçelievler / İstanbul, Türkiye, Tax ID / VKN 6312115665, ersin@packlistly.com) is the Data Processor for personal data in the Customer's shipment, buyer, supplier and forwarder document-request records (Customer Data).

Paddle.com acts independently as Merchant of Record for checkout and payment records.

2. Scope, duration and categories of data

Customer Data may include business contact names, work emails, phone numbers, business addresses, customs and tax IDs, uploaded trade documents, and revision and approval logs. The Processor uses this information solely to provide, secure and support Packlistly for the term of the workspace and until the data is deleted.

The Customer must exclude unrelated special-category personal data, consumer payment card numbers and classified defense data.

3. Processor commitments

The Processor processes Customer Data only on documented Customer instructions, including instructions on international transfers, unless applicable law requires otherwise. Authorized personnel are bound by confidentiality. Packlistly never sells Customer Data or uses it to train AI models.

The Processor immediately informs the Customer if, in its opinion, an instruction infringes applicable data-protection law.

The Processor assists the Customer with applicable data-subject requests, security obligations and compliance reviews, taking into account the processing and information available to the Processor.

4. Security controls and audit scope

Controls include TLS in transit, authenticated encryption at rest for new and updated shipment, product, buyer and settings records, and encrypted envelopes for forwarder files and backup archives. Packlistly uses company tenant isolation, password hashing, two-factor authentication, and logs for business-field revisions and approval invalidation.

On reasonable written request, up to once per 12 months or following a personal data breach affecting Customer Data, the Processor makes available written security documentation and questionnaire responses necessary to demonstrate compliance with this DPA and allows reasonable documentary or remote compliance reviews. Reviews take place on 30 days' prior written notice during normal business hours, subject to confidentiality and protection of other customers' records and third-party hosting facilities. These procedures preserve any audit and inspection rights required by applicable data-protection law.

Packlistly does not claim a SOC 2 report, ISO 27001 certificate or independent penetration-test report.

5. Authorized subprocessors

Render hosts the service in Virginia (US East). Cloudflare R2 provides private encrypted object storage in North America for forwarder files and backups. Google delivers account email when configured and stores encrypted backup archives in Google Drive. Postmark and Resend provide

transactional email when configured.

Anthropic’s commercial API processes documents only when the Customer explicitly invokes optional AI reading. Anthropic does not train on commercial API data by default. Its standard API abuse-monitoring retention is up to 30 days, subject to its published retention exceptions.

HubSpot is Packlistly’s own CRM and processes only Customer account and subscription contact records. It does not receive shipment files.

The Customer authorizes the listed subprocessors. The Processor imposes written data-protection obligations on each subprocessor no less protective than this DPA and remains responsible to the Customer for the performance of those obligations.

At least 14 calendar days in advance, the Processor publishes on /trust and /privacy notice of any addition or replacement of a subprocessor that processes Customer Data and emails the notice to all Company Owners of the workspace at their account email addresses. The Processor publishes and emails notice of urgent security or continuity replacements without undue delay. For both advance and urgent notices, if the Customer reasonably objects in writing on data-protection grounds within 14 calendar days of notice and the parties cannot resolve the objection, the Customer may export its records and terminate the affected workspace with a pro-rata refund of unused prepaid subscription fees.

6. Personal data breach notification

The Processor notifies the Customer without undue delay, and in any event within 48 hours after becoming aware of an unauthorized personal data breach affecting Customer Data. The notice includes the known scope, affected records and remediation steps. Any shorter notification period required by applicable law applies.

7. Self-serve data return, export and deletion

At the end of the provision of services, the Processor, at the Customer’s choice, returns or deletes all Customer personal data and deletes all existing copies, unless applicable law requires storage. The Customer may also instruct the Processor in writing to return or delete its personal data.

In exporter workspaces, including after cancellation when the workspace returns to Free, authorized users can export shipment lines (CSV) and structured shipment records (JSON). They can also download generated PDF and ZIP document sets after completing open blocking checks and obtaining any required workspace approval, and can delete individual shipments in the app.

In forwarder workspaces, authorized forwarder users can download available customer-uploaded files and accepted-document ZIP bundles from /forwarder according to their role permissions and active storage retention. Accepted-document ZIP bundles are limited to 50 files and 200 MB per download. If checks remain open, users must confirm by selecting “Download anyway”.

On written request from the verified Company Owner to ersin@packlistly.com, the Processor deletes active workspace records within 30 calendar days, subject to mandatory tax, billing and security-log retention. Encrypted forwarder backups expire on a rolling 35-day cycle. Other encrypted backups expire according to the applicable backup retention settings.

The Processor deletes copies in encrypted backups when their rolling retention period expires. Until then, those copies are restored to production only for disaster recovery, in which case the Processor reapplies deletion.

8. International transfers, governing law and counter-signature

The service is hosted in the United States and administered from Türkiye. The parties will use the applicable transfer mechanism and safeguards required by mandatory data-protection law for cross-border transfers.

The laws of the Republic of Türkiye govern this agreement, with jurisdiction in the courts of Istanbul, without prejudice to mandatory data-protection law. This agreement takes effect upon counter-signature.

Email the completed PDF to ersin@packlistly.com for counter-signature.

For Customer (Controller)	**For Neta Ofis (Processor)**
Company:	Ersin Gökmen, Founder
Name and title:	
Signature:	Signature:
Date:	Date: