Data Processing Addendum

Ojasys Transportation Management System (TMS) Suite of Products

Document Identifier	OJASYS-DPA-2026-V1
Effective Date	October 1, 2026
Parties	Ojasys LLC, a Virginia limited liability company ("Ojasys"), and the Customer named in the Order Form ("Customer")
Part of	Ojasys TMS Master Terms of Service (OJASYS-TOS-2026-V2) (the "Terms")
Contact	tms.privacy@ojasys.com

This Data Processing Addendum ("DPA") forms part of the Terms and applies whenever Ojasys processes Customer Personal Data. Capitalized terms not defined here have the meanings given in the Terms. If this DPA conflicts with the Terms on the processing of personal data, this DPA prevails.

1. Definitions

- **"Customer Personal Data"** means personal data within Customer Data that Ojasys processes on behalf of Customer.
- **"Data Protection Laws"** means all laws on data protection and privacy that apply to the processing of Customer Personal Data, including: the Digital Personal Data Protection Act, 2023 and the rules made under it (the "DPDP Act"); the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "SPDI Rules"), to the extent in force; and U.S. state privacy laws, including the California Consumer Privacy Act (the "CCPA").
- **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.
- **"Sub-processor"** means a third party engaged by Ojasys that processes Customer Personal Data.

2. Roles and Scope

2.1 Customer is the controller (Data Fiduciary under the DPDP Act, and "business" under the CCPA). Ojasys is the processor (Data Processor under the DPDP Act, and "service provider" under the CCPA).

2.2 The subject matter, duration, nature and purpose of the processing, and the types of data and individuals concerned, are described in Annex 1.

2.3 Customer is responsible for: the lawfulness of the processing instructions it gives; giving the notices, and obtaining the consents or other lawful basis, that Data Protection Laws require; and responding to individuals who exercise their rights.

3. Ojasys's Obligations

3.1 Instructions. Ojasys will process Customer Personal Data only on Customer's documented instructions, unless the law requires otherwise. The Terms, this DPA and Customer's configuration and use of the Service are Customer's complete instructions. Ojasys will tell Customer if it believes an instruction violates Data Protection Laws, and may suspend the affected processing until the instruction is confirmed or changed.

3.2 Confidentiality. Ojasys will ensure that the personnel who process Customer Personal Data are bound by confidentiality obligations and have access only as needed for their role.

3.3 Security. Ojasys will implement and maintain the security measures described in Annex 2, which are designed to provide reasonable security safeguards appropriate to the risk. Ojasys may update these measures, provided that the overall level of protection is not reduced.

3.4 Assistance. Taking into account the nature of the processing, Ojasys will provide reasonable assistance to Customer: (a) in responding to requests from individuals exercising their rights, through the Service's features or, where these are insufficient, on request; (b) with data protection impact assessments and consultations with authorities relating to the Service; and (c) in meeting Customer's breach notification obligations. If Ojasys receives a request directly from an individual about Customer Personal Data, it will forward the request to Customer within three (3) business days and will not respond to it except to direct the individual to Customer, unless the law requires otherwise.

3.5 No other use. Ojasys will not sell or share Customer Personal Data (as those terms are defined in the CCPA). It will not retain, use or disclose Customer Personal Data for any purpose other than performing the Service and the purposes permitted by the Terms and Data Protection Laws, including those in Section 15.1 of the Terms. It will not retain, use or disclose Customer Personal Data outside its direct business relationship with Customer, and will not combine it with personal data received from other sources except as permitted by the CCPA. Ojasys certifies that it understands and will comply with these restrictions.

3.6 De-identified data. Where Ojasys creates de-identified data under Section 15.1 of the Terms, it will take reasonable measures to ensure the data cannot be associated with an individual, will publicly commit to keeping it de-identified, will not attempt to re-identify it, and will contractually require any recipients to comply with the same conditions.

3.7 Notice of inability to comply. Ojasys will notify Customer if it determines that it can no longer meet its obligations under Data Protection Laws. Customer may then take reasonable and appropriate steps to stop and remediate any unauthorized processing.

4. Sub-processors

4.1 Customer gives general authorization for Ojasys to engage Sub-processors. The Sub-processors in use at the effective date are listed in Annex 3.

4.2 Ojasys will enter into a written agreement with each Sub-processor that imposes data protection obligations no less protective than those in this DPA. Ojasys remains responsible for each Sub-processor's performance.

4.3 Ojasys will notify Customer at least thirty (30) days before engaging a new Sub-processor, by email to the account administrator or through the Service. Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection in good faith, Customer may terminate the affected part of the Service by written notice, and Ojasys will refund the prepaid fees for the remainder of the Subscription Term, calculated from the termination date.

5. Personal Data Breaches

5.1 Ojasys will notify Customer of a Personal Data Breach without undue delay, and in any event within seventy-two (72) hours of becoming aware of it.

5.2 The notice will describe, to the extent then known, the nature of the breach, the categories and approximate number of individuals and records concerned, its likely consequences, and the measures taken or proposed to address it. Ojasys will provide further information as it becomes available.

5.3 Ojasys will take reasonable steps to contain and remediate the breach. Customer is responsible for notifying authorities and individuals as required by law, including the Data Protection Board of India. Ojasys will not make such notifications on Customer's behalf unless Customer instructs it to or the law requires it.

5.4 A notification is not an admission of fault or liability.

6. International Transfers

Customer Personal Data is hosted in the United States. Customer authorizes this transfer. Ojasys will not transfer Customer Personal Data to any country or territory restricted by the Government of India under Section 16 of the DPDP Act. It will ensure that any onward transfer to a Sub-processor is subject to the protections required by this DPA.

7. Return and Deletion

When the Terms end, Customer may export Customer Personal Data during the sixty (60) day Export Window described in Section 20.5 of the Terms. Ojasys will then delete Customer Personal Data from its active systems within thirty (30) days. Backup copies will expire in normal rotation within ninety (90) days after that and remain protected under this DPA until they do. Ojasys may keep Customer Personal Data longer only where the law requires it, and only for as long as required. On request, Ojasys will confirm deletion in writing.

8. Audits

8.1 On written request, and no more than once in any twelve (12) month period (unless a Personal Data Breach has occurred or an authority requires it), Ojasys will make available the information reasonably necessary to demonstrate its compliance with this DPA. This will include responses to a reasonable security questionnaire and a summary of Ojasys's security policies.

8.2 If that information is not sufficient to demonstrate compliance, Customer may, at its own cost, carry out an audit, or have an independent auditor bound by confidentiality do so. Customer must give at least thirty (30) days' notice. The audit must be conducted during business hours, in a way that does not unreasonably disrupt Ojasys's operations or compromise the security or confidentiality of other customers' data, and within a scope agreed in advance.

9. Liability and Term

Each party's liability under this DPA is subject to the limitations and exclusions in Section 19 of the Terms. This DPA remains in effect for as long as Ojasys processes Customer Personal Data.

Annex 1: Details of Processing

Subject matter and purpose	Providing the Ojasys TMS Service to Customer, including dispatch, fleet and trip tracking, document management, driver records, invoicing and support
Duration	The Subscription Term plus the Export Window and deletion periods in Section 7
Nature of processing	Collection, storage, organization, retrieval, display, transmission, analysis and deletion
Individuals	Customer's drivers (employed, owner-operator and contract), dispatchers and staff, and the contacts of shippers and consignees
Types of personal data	Identification and contact details; driving licence details; medical fitness certificate status and copies; precise location and trip data from the mobile app; mobile device data; operational documents, photos and signatures; shipment and invoice records
Sensitive data	Medical fitness certificates, and precise location. Biometric data is not processed.

Annex 2: Security Measures

- **Encryption.** Data is encrypted in transit over the internet using TLS, and encrypted at rest at the disk or database level.
- **Access control.** Access to production systems is limited to authorized personnel who need it for their role. Each person has an individual account, and access is removed promptly when no longer needed.

- **Authentication.** User passwords are stored using a salted, one-way hashing algorithm. Administrative access to production systems requires multi-factor authentication.
- **Customer isolation.** Customer Data is logically separated so that each Customer can access only its own data.
- **Logging and monitoring.** Access to and changes in production systems are logged, and logs are retained for at least one year.
- **Backups and continuity.** Regular backups are taken and stored in encrypted form, and restoration is tested periodically.
- **Vulnerability management.** Operating systems and dependencies are patched on a risk-based schedule.
- **Personnel.** Personnel with access to Customer Data are bound by confidentiality obligations and receive security and privacy training.
- **Incident response.** Ojasys maintains an incident response procedure that supports the breach notification commitments in Section 5.

Annex 3: Sub-processors

Sub-processor	Purpose	Location
Database Mart LLC	Hosting of the Service, databases and file storage	United States (Texas)
Google LLC (Google Maps Platform)	Maps, geocoding, and route and distance calculation	United States and other locations where Google operates
Mochahost LLC	Sending account and notification emails	United States
Apple Inc. and Google LLC (Firebase Cloud Messaging)	Delivering push notifications to the mobile apps	United States

Stripe, Inc. processes Ojasys's own subscription billing data as an independent service provider to Ojasys, and it provides payment services to Customers under its own agreement with them. For these reasons, it is not listed as a Sub-processor of Customer Personal Data.