

Privacy Policy

Ojasys Transportation Management System (TMS) Suite of Products

Document Identifier	OJASYS-PRIV-2026-V2
Effective Date	October 1, 2026
Legal Entity	Ojasys LLC, a Virginia limited liability company 22213 Windy Pine Ct, Ashburn, VA 20148, United States
Scope	The Ojasys TMS web platform (https://tms.ojasys.com), mobile applications and APIs
Privacy Contact	tms.privacy@ojasys.com
Grievance Officer (India)	Neha Parikh, tms.privacy@ojasys.com (see Section 13)

Summary. This summary highlights key points. Please read the full policy below.

- **Two roles.** For the business contacts who buy and manage Ojasys TMS accounts, Ojasys decides how their data is used. For driver, vehicle and shipment data that our customers (transport companies) put into the platform, the customer decides, and Ojasys processes it on the customer's behalf.
- **Drivers:** your employer or the company you drive for controls your data in Ojasys TMS. Please send privacy requests to them. If you contact us, we will pass your request on and help them respond.
- **No selling.** We do not sell personal data or use it for targeted advertising.
- **Where data is stored.** Data is hosted in the United States.
- **Your rights.** Depending on where you live, you can ask to access, correct or delete your data, and you can complain to our Grievance Officer.

1. Who We Are and What This Policy Covers

Ojasys LLC ("Ojasys", "we", "us") provides the Ojasys TMS software to transport companies, fleet operators and logistics businesses ("Customers"). This policy explains how we handle personal data in connection with the Ojasys TMS web platform, mobile applications and APIs (the "Service"), our website and our customer support.

The Service is currently offered to businesses in India and the United States. It is intended for business use only and is not directed at consumers.

2. Our Two Roles

2.1 Where Ojasys decides how data is used

Ojasys is the "Data Fiduciary" (under Indian law) or "controller"/"business" (under other laws) for:

- account and contact data of Customer administrators, dispatchers, managers and billing contacts;
- billing and subscription records;
- support and sales communications; and
- technical and usage data that we use to operate, secure and improve the Service.

2.2 Where Ojasys processes data for Customers

Ojasys is a "Data Processor" (under Indian law) or "processor"/"service provider" (under other laws) for data that Customers and their users put into, or collect through, the Service ("Customer Data"). This includes driver, vehicle, location, shipment and document data. The Customer decides why and how this data is processed, and is responsible for giving individuals any required notice and for having a lawful basis, including consent where required. We process Customer Data only on the Customer's instructions, under our Data Processing Addendum with the Customer.

3. Data We Collect for Our Own Purposes

Category	Examples	Why we use it
Account data	Name, work email, phone number, job title, company, login credentials (passwords are stored in hashed form), login history	To create and manage accounts, authenticate users and communicate about the Service
Billing data	Billing contact, billing address, GST or tax identifiers, invoices, payment status and the last four digits of payment cards. Full card numbers are collected by Stripe, not by us.	To bill subscriptions and Professional Services, collect payment, and meet tax and accounting obligations
Support and communications	Support tickets, emails, call notes and feedback	To provide support, respond to requests and improve the Service
Technical and usage data	IP address, browser and device type, operating system, app version, crash logs, pages and features used, error logs	To operate, secure, troubleshoot and improve the Service, and to prevent fraud and abuse
Marketing contacts	Name, work email and company of people who ask for information or a demo	To respond to enquiries and send business updates. You can unsubscribe at any time.

4. Data We Process for Customers

The data processed depends on how each Customer uses the Service. It typically includes the following:

Category	Examples	Individuals concerned
Driver identification	Name, phone number, driver ID, driving licence number, issuing authority, licence class and expiry date, date of birth	Employed drivers, owner-operators and contract drivers
Medical fitness certificates	Certificate copy, status and expiry date (for example, Form 1-A in India or a medical examiner's certificate in the United States)	Drivers whose licence requires medical certification
Location and trip data	GPS coordinates, speed, heading, timestamps, route history, geofence arrivals and departures, trip status	Drivers using the mobile app while location tracking is enabled
Mobile device data	Device identifier, operating system, app version, network status, crash logs	Drivers and field staff using the mobile app
Operational documents	Consignment notes, lorry receipts, bills of lading, proof-of-delivery photos and signatures, vehicle inspection and incident records	Drivers, shippers, consignees and Customer staff
Shipment and payment records	Shipper and consignee contact details, delivery addresses, invoices and payment records for the Customer's shipments	Shippers, consignees and their contacts

5. Sensitive Personal Data

- **Medical data.** The Service stores medical fitness certificates, and their status and expiry dates, so that Customers can confirm drivers are certified as required by transport law. We do not ask for or analyze clinical records, diagnoses or test results. Customers must not upload them.
- **Financial data and passwords.** These are protected as described in Section 10. Full payment card numbers are handled by Stripe, not by Ojasys.
- **Location data.** Precise location is collected only through the mobile app, when the Customer has enabled tracking and the driver has granted location permission.
- **Biometric data.** The Service does not currently collect or process biometric data, such as facial recognition or fingerprints. If this changes, we will update this policy before we launch that feature.
- **Aadhaar.** Customers must not upload Aadhaar numbers unless they are masked so that no more than the last four digits are visible.

6. Legal Basis for Processing

For data we control (Section 3), we rely on the following bases:

- **Contract.** To provide the Service and perform our agreement with the Customer.
- **Legal obligation.** To keep tax and accounting records and respond to lawful requests.
- **Legitimate uses or legitimate interests.** To secure the Service, prevent fraud, and understand and improve how the Service is used, as permitted by applicable law.
- **Consent.** Where the law requires it, for example for marketing emails in some cases. You can withdraw consent at any time. Withdrawal does not affect processing that took place before it.

For Customer Data (Section 4), the Customer determines the legal basis. In India, this may be consent under Section 6 of the Digital Personal Data Protection Act, 2023 (DPDP Act), or a legitimate use under Section 7, such as employment purposes.

7. How We Share Data

We do not sell personal data, and we do not share it for targeted or cross-context behavioral advertising. We share personal data only as follows:

- **Service providers (sub-processors)** that host and operate the Service for us, under written contracts that require them to protect the data and use it only to provide services to us. The current list is in Annex 3 of our Data Processing Addendum and is available on request from tms.privacy@ojasys.com.
- **Stripe, Inc.** processes our subscription payments. If a Customer uses the Service to collect payments from its own customers, Stripe provides those payment services under its own agreement with the Customer.
- **Google Maps Platform.** We use it to display maps, convert addresses to coordinates and calculate routes. Addresses and locations sent to Google are handled under the Google Privacy Policy (policies.google.com/privacy).
- **Customers.** Data collected through a Customer's account, including a driver's location and documents, is available to that Customer's authorized users.
- **Legal requirements.** We disclose data to courts, law enforcement or regulators when required by law or binding legal process. Where the law allows, we notify the affected Customer first.
- **Business transfers.** If Ojasys is involved in a merger, acquisition or sale of assets, data may be transferred to the successor, subject to this policy.

8. International Transfers

Ojasys is based in the United States, and the Service is hosted in the United States. If you are in India, your data will be transferred to and stored in the United States. We will not transfer personal data to any country or territory that the Government of India restricts under Section 16 of the DPDP Act. Wherever your data is processed, we protect it as described in this policy.

9. How Long We Keep Data

Data	Retention
Account data	For as long as the account is active. After it closes, for up to 2 years to handle follow-up questions and legal claims.
Billing and tax records	7 years after the end of the financial year to which they relate, or longer if tax or accounting law requires it.
Support communications	For as long as the account is active, and for 2 years after it closes.
Security and access logs	At least 1 year, and longer if needed to investigate a security incident.
Marketing contacts	Until you unsubscribe, or after 2 years without any engagement.
Customer Data (Section 4)	During the subscription, for as long as the Customer keeps it in the Service. The Customer can delete data earlier. After the subscription ends, the Customer has 60 days to export its data. We then delete it from active systems within the next 30 days, and backup copies expire within 90 days after that. We keep data longer only where the law requires it.

Customers are responsible for exporting and keeping any records that transport, employment or tax law requires them to retain.

10. Security

We maintain reasonable security practices and procedures, including administrative, technical and physical safeguards designed to protect personal data against unauthorized access, loss, misuse or alteration. These include encryption of data in transit, access controls based on job role, secure storage of passwords, logging and monitoring, and backups. No system is completely secure. If you believe your account has been compromised, contact tms.support@ojasys.com immediately.

11. Personal Data Breaches

If a personal data breach affects Customer Data, we will notify the affected Customer without undue delay, and in any event within 72 hours of becoming aware of it. We will provide the information the Customer needs to meet its own notification obligations. If a breach affects data we control, we will notify the authorities and affected individuals as required by applicable law, including the Data Protection Board of India where the DPDP Act requires it.

12. Your Rights

12.1 Drivers and other individuals whose data is in a Customer's account

Your employer, or the company you drive or ship for, controls this data. Please send requests to them. If you contact us, we will tell you which Customer controls your data, pass your request to them within three (3) business days, and help them respond.

12.2 Individuals whose data Ojasys controls

Depending on the law that applies to you, you may have the right to:

- obtain a summary of your personal data and how it is processed, and the identities of those it has been shared with;
- correct, complete or update your data;
- have your data erased, unless we need to keep it for a legal purpose;
- withdraw consent, where we rely on consent;
- nominate someone to exercise your rights in the event of your death or incapacity (India); and
- have a grievance addressed by our Grievance Officer, and then complain to the relevant data protection authority.

To make a request, email tms.privacy@ojasys.com. We may need to verify your identity. We will respond within 30 days, or sooner if the law requires it. We will not treat you differently for exercising your rights.

13. Grievance Officer (India)

In accordance with the Information Technology Act, 2000, the rules made under it, and the DPDP Act, our Grievance Officer is:

Name	Neha Parikh
Designation	Grievance Officer, Ojasys LLC
Email	tms.privacy@ojasys.com
Address	22213 Windy Pine Ct, Ashburn, VA 20148, United States

We will acknowledge grievances within 7 days and resolve them within 30 days of receipt. If you are not satisfied with our response, you may complain to the Data Protection Board of India once the relevant provisions of the DPDP Act are in force.

14. Cookies and Mobile App Permissions

Cookies. The Service uses only cookies that are strictly necessary for login sessions, security and load balancing. We do not use advertising cookies or third-party advertising tags in the Service.

Mobile app permissions. The mobile app may ask for:

- **Location, including in the background.** To share trip progress and arrival updates with the Customer's dispatch team, and to record arrivals and departures at pickup and delivery points, while the Customer has enabled tracking.
- **Camera and photos.** To capture delivery documents, proof of delivery and damage photos.
- **Notifications.** To send dispatch updates and alerts.

You can change these permissions at any time in your device settings. Features that depend on a permission will not work while it is turned off.

15. Children

The Service is for business use and is not directed at anyone under 18. We do not knowingly collect personal data from children. If you believe a child's data has been provided to us, contact tms.privacy@ojasys.com and we will delete it.

16. Changes to This Policy

We may update this policy from time to time. We will post the new version with a new effective date and, for material changes, notify Customer administrators at least 30 days in advance.

17. Contact Us

Ojasys LLC, Attn: Privacy, 22213 Windy Pine Ct, Ashburn, VA 20148, United States. Email: tms.privacy@ojasys.com.

Addendum A: India

- **Applicable law.** The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, as their provisions come into force. Until then, the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), to the extent they remain in force.
- **Sensitive personal data.** Under the SPDI Rules, passwords, financial information (such as bank account or card details) and medical records are sensitive personal data. We collect such data only where necessary for a lawful purpose, and Customers must obtain written consent (which may be electronic) before uploading drivers' medical certificates.
- **Language.** On request, we will provide this policy in any of the languages listed in the Eighth Schedule to the Constitution of India that we support.
- **Contact.** See our Grievance Officer in Section 13.

Addendum B: United States

- **State privacy laws.** If a state privacy law, such as the California Consumer Privacy Act, applies to your data, you may have the right to know, access, correct and delete your personal data, and to appeal our decision on your request. You may use an authorized agent to make a request, subject to verification.
- **No sale or sharing.** We do not sell personal data, and we do not share it for cross-context behavioral advertising. We do not use sensitive personal information to infer characteristics about individuals.

- **Categories.** The categories of data we have collected in the past 12 months, their sources and their purposes are described in Sections 3 and 4. The recipients are described in Section 7.
- **Global Privacy Control.** We do not sell or share personal data. If your browser sends a Global Privacy Control signal, we treat it as a request not to sell or share your data.