Privacy Policy

Updated November 7, 2026 I Rider, Driver, Website, Admin, Payment and Support Data

Company-approved privacy policy update, November 7, 2026. Originally effective October 7, 2026. Publication does not activate commercial rides or certify that operational requirements are complete. Public rides require applicable permits, insurance, verified driver screening, safety operations, payment accounts and release acceptance.

1. SCOPE AND CONTROLLER

This Privacy Policy explains how Mars Jr LLC (DBA MyD.D. Rideshare) collects, uses, discloses, protects, retains, and deletes personal information through its rider app, driver app, admin panel, website, transportation platform, payment and payout functions, support, and safety operations.

Mars Jr LLC, doing business as MyD.D. Rideshare, 1122 Lady Street, Columbia, South Carolina 29201. Support and privacy contact: Marsjrllc@outlook.com; (803) 381-0790.

2. INFORMATION COLLECTED FROM RIDERS

- Account and contact data: name, email, telephone number, authentication and consent records.
- Location and ride data: pickup, destination, coordinates, route, estimated and actual distance and duration, driver assignment, status history, PIN-verification event, and receipt.
- Payment data: Stripe customer/payment identifiers if configured, authorization and charge status, amount, platform fee, refund, dispute, and limited card metadata supplied by Stripe; never full card number or security code.
- Device and preference data: push token, app kind, platform, notification and analytics choices, saved places, and session/security metadata.
- Support and safety data: complaint, incident, deletion, refund, appeal, and related communications.

3. INFORMATION COLLECTED FROM DRIVERS

- Account, contact, vehicle, license-plate, availability, and application data.
- Driver's license, insurance, registration, inspection, expiration dates, review status, and private uploaded files.
- Screening authorization and eligibility status; reports are collected only after a compliant provider and process are activated.
- Online and active-trip location, heading, accuracy, login/availability times, assignments, trip events, earnings, and payout status.
- Stripe Connect account identifier, onboarding and payout capability status; Stripe collects bank, identity, and tax details in its hosted process.

4. SOURCES

Information comes from users, their devices, assigned trip participants, administrators and support staff, payment and payout providers, screening and identity providers when activated, mapping and platform providers, and lawful authorities or insurance participants.

5. PURPOSES

- Create and secure accounts; authenticate users; record consent.
- Search locations, estimate routes and fares, match riders and drivers, synchronize trip status, provide navigation and receipts.
- Authorize and capture payments, issue refunds, calculate platform fees and earnings, onboard drivers for payouts, and reconcile financial records.
- Review driver eligibility and documents; prevent unapproved or expired drivers from going online.
- Deliver ride, payment, safety, account, and support notifications.
- Provide support, investigate incidents and fraud, enforce policies, meet TNC, insurance, tax, accounting, legal, and safety duties, and improve reliability.

6. VENDORS AND DISCLOSURES

Technical components for the updated apps: Firebase (authentication, Firestore, private storage, Functions and realtime updates); Stripe/Connect (payments, refunds, onboarding and transfers); Expo/APNs/FCM (push); Vercel/Firebase Hosting (websites and Admin); Google Maps and Google routing/address search. Google web embeds receive displayed coordinates and network metadata. Native and web implementations have different location and background capabilities. Legacy records may remain with Supabase while migration and retention obligations are resolved. Designated web demos use isolated Firebase staging and Stripe TEST. Production apps use the production Firebase service and Stripe LIVE for ordinary ride payments; designated reviewer accounts use synthetic TEST payment flows.

MyD.D. discloses information to assigned riders/drivers, vendors acting for the service, insurers and claims participants, screening providers, professional advisers, and authorities when consented to, necessary for the requested service, or permitted or required by law. MyD.D. does not sell personal information or share it for cross-context behavioral advertising in this launch version.

7. LOCATION

Rider location is used while the app is open to choose a pickup and plan a route. Riders may enter pickup and destination locations manually. MyD.D. Driver uses precise location while a driver is available or on an active trip for nearby ride requests, pickup, navigation, trip synchronization, support, and safety. With the driver's separate in-app consent and the device's background-location permission, Driver also collects and sends location to MyD.D. when the app is not in use. Assigned riders receive relevant driver location during their trip. Android displays an ongoing location-service notification; iOS may display its location indicator. Drivers may decline background access and use location while the app is open, revoke permission in device settings, or sign out to stop availability and location sharing. MyD.D. does not use location for advertising.

8. PAYMENTS AND PCI BOUNDARY

Payment entry is handled by the Stripe mobile SDK or Stripe-hosted web payment elements. MyD.D. receives a PaymentIntent client secret on the authenticated device and stores limited provider identifiers and financial ledger data in Firebase for the updated apps. Legacy financial records may remain in Supabase until migration and retention requirements are resolved. Do not send payment card numbers, security codes, or bank credentials to MyD.D. support. Stripe's own privacy notice governs its independent processing.

9. RETENTION

- South Carolina TNC service records, driver qualification verification, and vehicle-inspection documentation: at least three years from the applicable service, verification, or inspection, and longer if required for a claim or law.

- Company-approved retention schedule: financial records for three years after the transaction, subject to any applicable longer tax or accounting requirement and unresolved payment, refund, dispute or legal hold. Retention controls and hold review must implement this schedule; it does not represent every law as mandating the same period.
- Company-approved retention schedule: closed safety, insurance, fraud, complaint, and dispute records for three years after closure, except where an applicable retention requirement, unresolved matter, claim or legal hold requires longer preservation.
- Push tokens: until replaced, invalidated, account deletion is completed, or the user withdraws notification access.
- Unsubmitted drafts and superseded optional preferences: deleted or de-identified when no longer needed.
- Account data: retained while active, then deleted or de-identified after a verified deletion request except for records covered by the categories above.

10. ACCOUNT DELETION AND PRIVACY REQUESTS

Riders and drivers can initiate whole-account deletion in the app. MyD.D. verifies the request, prevents deletion during an active trip, revokes the device session, and tracks completion. Requests for access, correction, deletion, or a data summary may also be sent to Marsjrllc@outlook.com. MyD.D. will authenticate the requester and explain any lawful denial or retained category.

11. SECURITY

Controls include encrypted transport, managed authentication, short-lived sessions and refresh rotation, role and row-level access controls, private driver-document storage, server-authoritative trip transitions and fares, webhook signature verification and deduplication, idempotent payments, audit events, and separation of public app keys from service and payment secrets. No system is perfectly secure. Report suspected compromise promptly.

12. CHOICES

- Use device settings to control location and push permissions.
- Use in-app preferences to control optional marketing and analytics where available; operational ride and safety messages cannot be disabled while using an active service.
- Correct profile data in the app or through Support.
- Request deletion or a data summary through the app and privacy contact.

13. CHILDREN

The account services are not directed to children under 18, and MyD.D. does not knowingly allow them to create independent accounts. If MyD.D. learns that an ineligible minor created an account, it will restrict the account and delete eligible data, subject to safety and legal retention.

14. INTERNATIONAL PROCESSING

MyD.D. is initially intended for South Carolina. Vendors may process information in the United States and other locations where they operate, subject to contracts and applicable safeguards.

15. CHANGES AND CONTACT

A new version and effective date will accompany material changes. MyD.D. will seek renewed consent where appropriate. Contact Marsjrllc@outlook.com, (803) 381-0790, or 1122 Lady Street, Columbia, SC 29201 for privacy questions or complaints.

16. LEGAL AND TECHNICAL REFERENCES

South Carolina Transportation Network Company Act, S.C. Code Title 58, Chapter 23, Article 16: https://www.scstatehouse.gov/code/t58c023.php. Apple account deletion guidance: https://developer.apple.com/support/offering-account-deletion-in-your-app/. Stripe privacy and security materials: https://stripe.com/privacy and https://stripe.com/docs/security. Firebase privacy and security materials: https://firebase.google.com/support/privacy. Legacy Supabase privacy and security materials: https://supabase.com/privacy and https://supabase.com/security. Original company approval recorded October 7, 2026; factual Android privacy update approved November 7, 2026. Operational activation and acceptance remain separately required.