PRIVACY POLICY (INCLUDING U.S. STATE ADDENDA)

Applicable to All Softvivor Platforms

Version: 2026.2
Last Updated: February 6, 2026
Effective Date: February 6, 2026

Softvivor LLC ("Company," "Softvivor," "we," "us," or "our") considers protecting the privacy of our customers ("Riders"), business partners ("Drivers," "Fleets," or "Service Providers"), and individuals who visit our digital properties ("Visitors") a top priority.

This Privacy Policy ("Policy") explains how we collect, use, disclose, store, and protect personal information when you use any of our platforms (collectively, the "Platform"), including the brands **TransferBid, Priofer, Tripfer, Medifer, Mopany, Agentfer**, and the **DriverNest** and **TransferHelpdesk** infrastructures, through our websites and/or mobile applications.

This Policy is designed with particular attention to U.S. state privacy laws and related requirements, including **California CCPA/CPRA**, **Virginia VCDPA**, **Colorado Privacy Act**, **Connecticut Data Privacy Act**, **Washington My Health My Data Act (MHMDA)**, and **FCRA principles** for driver screening. Rights and procedures may vary by state. Where the Platform is used by individuals located in the **EEA**, the **United Kingdom**, or **Switzerland**, the relevant provisions of this Policy apply.

---

1. DATA CONTROLLER, CORPORATE STRUCTURE, HOSTING, AND CONTACT

1.1. Data controller and roles

- **Data Controller (and "Business" under California law): Softvivor LLC (U.S.)**. The Platform operator and primary party responsible for determining the purposes and means of processing personal information.
- **Processor / Service Provider: Softalya Ltd. (Türkiye)**. Our technology partner providing software development, technical maintenance, and infrastructure/operational support services on behalf of Softvivor.
- **Independent contractors:** Drivers and Fleets are independent businesses and remain responsible for their own legal obligations arising from their activities.

1.2. Data hosting

- **Primary hosting region:** Personal information is primarily hosted and stored in **Amazon Web Services ("AWS") Europe (Frankfurt) Region — eu-central-1 (Germany)**.

1.3. Cross-border access (U.S. and Türkiye) and access minimization

Even where data is stored in the EEA, limited remote access from the **United States** (data controller organization) and from **Türkiye** (through our technology partner) may occur for Platform operations, security, maintenance, troubleshooting, and support. Such access is restricted through:

- **role-based access controls**,
- **least-privilege** and **need-to-know** principles,
- **multi-factor authentication (MFA)**, and
- **access logging and auditing**.

Where feasible, access from Türkiye is performed using **masked or de-identified** data and technical logs; production-data access is exceptional and tightly controlled.

1.4. Contact

- **Email:** contact@transferbid.com
- **Address: 699 San Antonio Road, Palo Alto, CA 94306, USA**
- **Phone:** +1 (650) 505-5770
- (If applicable) **Privacy Portal:** [to be added]

---

2. NOTICE AT COLLECTION (CALIFORNIA) — SUMMARY

Under California law, we provide notice of the categories of personal information we collect and the purposes for which we use it. The table below is a summary notice.

Note: "Sale/Sharing" may include certain disclosures for cross-context behavioral advertising under California law.

Category	Examples	Purpose	Sale/Sharing	Typical Retention
Identifiers	Name, email, phone, IP address, account IDs	Account, bookings, communications, security	Generally no	Account term + **7 years**
Commercial Information	Booking history, route/time, fare, payment method	Service delivery, payment/refunds, accounting, disputes	Generally no	**7 years**

Category	Examples	Purpose	Sale/Sharing	Typical Retention
Precise Geolocation (Sensitive)	GPS, route, match-time location	Matching, navigation, safety, ETA	No	Trip duration + **default up to 180 days** (*longer only if needed for incidents/disputes/compliance*)
Internet/Network Activity	Device ID, cookies/SDK IDs, clicks, crash logs	Security, performance, analytics, debugging	May be for targeted ads	Technical/crash logs **180 days**; marketing identifiers **max 13 months**
Sensitive Driver Information	SSN/ITIN, driver's license number/images, background report	Verification, FCRA compliance, payouts	No	**3–7 years** (as required)
Driver Telematics	Acceleration, braking, turning	Safety monitoring, incident detection	No	**1–7 years** (incident-based)

Retention periods in this table are aligned with **Section 8 (Data Retention)**. We do not provide conflicting retention periods for the same data type; any extension occurs only in limited circumstances such as legal obligations, security incidents, or disputes.

---

3. INFORMATION WE COLLECT AND SOURCES

3.1. Information you provide directly

Rider/User: name, email, phone; booking information; special requests.
Driver/Fleet: driver's license, vehicle registration, insurance, work authorization; banking details; U.S. tax forms (e.g., W-9); identifiers required for background checks.
Support records: call center, chat, and email communications.
Password security: we do not store passwords in plain text; we use appropriate technical methods (e.g., hashing/salting).

3.2. Information collected automatically

- Location data: precise location (with permission), approximate location (via IP)
- Telematics/Sensors (Drivers): limited sensor data for safety and incident detection
- Device information: IP address, device model, operating system, crash logs and similar technical records

3.3. Information obtained from third parties

- Background check providers (e.g., Checkr, Sterling) and FCRA-aligned reports
- Marketing and measurement partners (as permitted by law and your choices)
- Referral programs (contact details provided by the referring user)

---

4. PURPOSES FOR USING INFORMATION

We process personal information for the following purposes:

- **Service delivery:** matching, navigation, payment collection, receipts
- **Security:** identity verification, fraud detection, incident management
- **Legal compliance:** court orders, tax records, regulatory requirements
- **R&D/Analytics:** ETA forecasting and product improvement
- **Marketing/Targeted advertising (if applicable):** consistent with your choices and applicable legal mechanisms

EEA/UK/Switzerland (where applicable): processing is based on contract performance, legal obligations, legitimate interests, and—only where required—consent.

---

5. LOCATION DATA AND GEOFENCING LIMITATIONS (MHMDA)

- **Rider permissions:** you can manage location permissions in device settings; you may use the service by manually entering an address without sharing precise location.
- **Drivers:** while "online" and actively providing services, location may be necessary due to the nature of the service.
- **Washington MHMDA commitment:** we do not use geofencing around hospitals, clinics, or reproductive health facilities to identify, track, or target consumers for health-related advertising.
- **Live location:** live location sharing ends after the trip is completed (see Section 7.3).

---

6. DRIVER BACKGROUND CHECKS AND FCRA

- **Separate authorization:** driver screenings require a separate disclosure and written authorization document independent of this Policy.
- **Adverse action process:** if an adverse decision may be made based on a report, we follow an FCRA-aligned process including a pre-adverse action notice, a dispute period, and a final notice.

---

7. DISCLOSURE AND SHARING OF INFORMATION

7.1. Operational sharing (service providers)

We may disclose personal information to service providers for hosting/infrastructure, payments, communications, analytics, error monitoring, security, and support. These parties are contractually limited to processing data on our behalf and under our instructions.

7.2. Sharing among Softvivor Platforms

Softvivor operates multiple brands/products under the same corporate organization, serving different customer types within the same general line of services. Personal information may be shared among Softvivor Platforms **only** for the following purposes and under a **minimum necessary data** approach:

- Service delivery and operational continuity (including single account/booking management),
- Security, fraud prevention, and incident management,
- Customer support and quality improvement,
- Compliance with legal obligations.

Sharing among Softvivor Platforms is not the same as "Sale/Sharing" of personal information to third parties for targeted advertising; targeted advertising-related processing, if any, is governed by the separate mechanisms described in this Policy.

7.3. Rider–Driver sharing (minimum necessary data)

- **To Drivers:** Rider name, location, and (where necessary) photo.
- **To Riders:** Driver name, vehicle details, license plate, and live location during the trip.
- **Note:** live location sharing ends after the trip is completed.

7.4. Advertising-related "Sale/Sharing"

Cookie identifiers and internet/network activity may be disclosed to third parties for targeted advertising. Under California law, this may be considered a "Sale" or "Sharing." You have the right to opt out (see Section 9).

7.5. Legal requirements and protection of rights

We may disclose personal information to comply with legal obligations (e.g., court orders, government requests) and as necessary for legitimate purposes such as security and fraud prevention.

---

8. DATA RETENTION

We retain personal information for as long as needed to fulfill the purposes described and to comply with legal requirements:

- **Account:** for the account term + **7 years**.
- **Bookings/transactions: 7 years**.
- **Precise location (sensitive):** trip duration + **default up to 180 days**; longer only where needed for security incidents, fraud investigations, disputes/appeals, or legal obligations.
- **Security/technical logs (crash/performance):** typically **180 days** (may be extended for security incidents/investigations).
- **Marketing identifiers:** maximum **13 months**.
- **Driver qualification/sensitive files: 3–7 years** (as required by applicable rules).
- **Driver telematics: 1–7 years** (incident-based).
- **Deletion requests:** where no legal retention obligation applies, data is deleted or de-identified within **30–90 days**.
- **Note:** longer retention practices are applied only where legally required.

---

9. YOUR RIGHTS AND CHOICES

9.1. U.S. state privacy rights

Depending on your state of residence, you may have rights to access/know, delete, correct, and opt out (including opt out of Sale/Sharing and, in some states, targeted advertising).

9.2. "Do Not Sell or Share" and GPC

- You may use our "Do Not Sell or Share My Personal Information" link/mechanism on our websites (and where available, in-app preferences) to exercise opt-out rights.
- We recognize the Global Privacy Control (GPC) signal as an opt-out request where applicable.

9.3. Sensitive data preferences

In some states, processing sensitive personal information may require opt-in consent. You can manage and withdraw location permissions via device settings and may withdraw consent as applicable.

9.4. Request channels and appeals

You may submit requests using the contact methods in Section 1.4. We may need to verify your identity. Where required, we provide an appeals process for denied requests.

9.5. Additional information for EEA/UK/Switzerland users

Where applicable, individuals located in the EEA/UK/Switzerland may have rights to access, correct, delete, restrict processing, data portability, object, and withdraw consent (where consent is the legal basis). Requests are generally addressed within **one (1) month**, subject to lawful extensions where permitted. You also have the right to lodge a complaint with a competent supervisory authority.

If conditions arise requiring a representative under GDPR Article 27, we will appoint an EU/UK representative and publish the representative's details in this Policy.

---

10. COOKIES AND SIMILAR TECHNOLOGIES

We use cookies and similar technologies on our websites and/or mobile applications for security, performance, analytics, and (if applicable) targeted advertising. **Cookies/SDKs and their purposes may vary across different Softvivor websites and applications.** Cookie preferences and detailed cookie lists for each site/app are managed through the relevant cookie notice or preference center on that site/app.

- In regions such as the EEA/UK, we provide legally required consent mechanisms for non-essential cookies/trackers.
- In California and other applicable states, we provide opt-out mechanisms for Sale/Sharing and targeted advertising as required.

---

11. DATA SECURITY

We implement appropriate technical and organizational measures to protect personal information (e.g., TLS 1.2/1.3, encryption, MFA, role-based access, access logging, and auditing). No digital system can be guaranteed to be 100% secure.

Security incidents: We assess incidents that may constitute a personal data breach and, where required, follow applicable legal notification processes.

---

12. INTERNATIONAL DATA TRANSFERS

Due to our global operations, personal information may be transferred to, or accessed from, other countries (e.g., remote access from Türkiye through Softalya Ltd.; operational access from the United States).

Where personal information originating from the EEA/UK/Switzerland is transferred to, or accessed from, outside those regions, we use appropriate safeguards as applicable, including:

- **Standard Contractual Clauses (SCCs)** and/or similar transfer mechanisms,
- **Data Processing Agreements (DPAs)**, and
- where appropriate, **Transfer Impact Assessments (TIAs)** and additional technical/organizational measures (e.g., encryption, access restrictions, logging/monitoring, MFA).

DPF note: We do not currently rely on the EU–U.S. Data Privacy Framework (DPF) certification for transfers.

13. CHANGES TO THIS POLICY

We may update this Policy from time to time. Changes will be posted here and reflected by updating the version/date information above.

---

14. NOTICE AND CONSENT

Your use of the Platform indicates that you have been provided notice of the processing described in this Policy. **Where explicit consent is required by law** (e.g., non-essential cookies/trackers, certain marketing activities, or sensitive-data processing in some jurisdictions), we will obtain consent separately, and you may withdraw it at any time through applicable settings or by contacting us.

---

15. CONTACT US

For privacy questions or requests:

- **contact@transferbid.com**
- **+1 (650) 505-5770**
- **699 San Antonio Road, Palo Alto, CA 94306, USA**