AERRAND INC.

Privacy Policy

Effective Date: April 7, 2025

Last Updated: April 7, 2025

This policy explains how Aerrand Inc. collects, uses, shares, and protects your personal information, and describes your rights under Canadian, EU/EEA/UK (GDPR), and U.S. (CCPA/CPRA) data protection law.

---

1. Who We Are

Aerrand Inc. (“Aerrand,” “we,” “our,” “us”) is a corporation headquartered in Windsor, Ontario, Canada. We operate a consumer-to-consumer (C2C) delivery and trust platform at aerrand.com and through our mobile application (collectively, the “Platform”). This Privacy Policy applies to all Platform users, including Buyers and verified delivery partners (“Aerranders”).

Contact for all privacy matters: operations@aerrand.com | aerrand.com

2. Legal Frameworks

We comply with all applicable privacy laws, including:

- Canada: PIPEDA and applicable provincial privacy legislation
- EU / EEA / UK: General Data Protection Regulation (EU GDPR 2016/679) and UK GDPR as retained in domestic law
- United States — California: CCPA as amended by CPRA
- United States — Other states: Virginia VCDPA, Colorado CPA, Connecticut CTDPA and other emerging state laws monitored on an ongoing basis

Where frameworks impose different requirements, we apply the standard most protective of user rights.

3. Data Controller and EU/EEA/UK Representative

Aerrand Inc. is the data controller. Contact: operations@aerrand.com. Until our EU/EEA user volume requires a formal Article 27 GDPR representative, EU/EEA and UK users may contact us directly at operations@aerrand.com. We will appoint a representative when required under applicable guidance.

4. Information We Collect

4.1 Information You Provide Directly

- Account registration: full name, email address, phone number, date of birth
- Profile: delivery address, optional profile photo
- Transaction data: item descriptions, marketplace listing URLs, declared item value, delivery instructions

- Communications: in-app messages, support requests, dispute submissions
- Parental or guardian consent documentation (users aged 16–17)

4.2 Analytics Data

- Page views, session duration, navigation paths, feature interactions, referral sources
- We use Google Analytics with IP anonymization enabled — your full IP address is not stored
- We use HubSpot for CRM, email campaign tracking, and form analytics (Buyer and Aerrander waitlist signups)
- Analytics data: raw session data retained 14 months; aggregated and anonymized within 26 months

4.3 Crash and Diagnostic Data

- Device type, operating system version, application version, session state at time of crash
- Error codes, stack traces, and performance metrics used to identify and resolve bugs
- Crash logs do not include message content or transaction details unless directly relevant to the crash event
- Retained for a maximum of 12 months from collection

4.4 Location Data

- Approximate location: derived from IP address for Aerrander matching and regional availability; not stored long-term
- Precise GPS: collected from Aerranders only, during active dispatch, with explicit in-app permission. GPS tracking begins when an Aerrander accepts a job assignment and is used to calculate pickup trip distances and DPWRA-compliant engaged time.
- Buyers provide delivery address manually — no Buyer GPS is collected
- Aerrander real-time GPS coordinates are not displayed to Buyers at any point
- Precise GPS location data for a completed or cancelled job is deleted within 30 days of delivery confirmation or cancellation

4.5 Payment Information

All payments are processed by Stripe, Inc. (PCI-DSS Level 1 certified). Aerrand does not store full card numbers, CVV, or bank credentials. We retain: Stripe payment tokens, transaction amounts and timestamps, escrow state records, Guard fee calculations, and transaction identifiers — for financial record-keeping, chargeback defence, DPWRA compliance logging, and tax obligations.

4.6 Aerrand Guard™ Verification Media

- Aerranders capture a minimum of 2 photos and 1 video of the item at pickup; customers may request up to 3 additional media items per job

- The Aerrander provides explicit in-app consent before media capture begins. Buyers are informed through the Guard transaction flow.
- Media is transmitted via TLS-encrypted connection and stored on access-controlled, encrypted servers
- Media is used solely for item verification, AI-assisted condition assessment, escrow release decisions, and dispute resolution
- Media is NEVER used to train, fine-tune, or benchmark any AI or machine learning model, whether operated by Aerrand or any third party
- No biometric data is collected; capture is limited to the item and its immediate surroundings
- Retained for 90 days from transaction completion or active dispute resolution (whichever is longer), then permanently and irreversibly deleted

4.7 Environmental Impact Data

Our Avoided Emissions Attribution Engine calculates estimated CO_2 avoided based on item category, delivery route distance, and vehicle class. Stored in association with transaction records; aggregated and anonymized for platform-level reporting. Not used for regulatory compliance or carbon credit purposes.

4.8 Transaction and Pricing Records

We retain complete records of all fee calculations, Guard fee tiers applied, cancellation outcomes, Aerrander payout amounts, DPWRA minimum wage calculations, and escrow release events for financial, legal, and regulatory compliance purposes.

5. Purposes and Legal Bases for Processing

Purpose	Data Used	GDPR Basis	PIPEDA / CCPA
Account creation and management	Registration data	Contract (Art. 6(1)(b))	Consent / necessity
Age verification and parental consent	Date of birth, consent docs	Legal obligation (Art. 6(1)(c))	Legal obligation
Transaction processing and escrow	Payment, transaction data	Contract (Art. 6(1)(b))	Contractual necessity
Guard verification and AI analysis	Media, item description	Contract (Art. 6(1)(b))	Contractual necessity
GPS distance calculation (trip fees, DPWRA)	Aerrander GPS data	Contract + legal obligation (Art. 6(1)(b)(c))	Necessity + legal
Fraud prevention and chargeback defence	Account, device, transaction data	Legitimate interest (Art. 6(1)(f))	Legitimate interest

Purpose	Data Used	GDPR Basis	PIPEDA / CCPA
Analytics and product improvement	Usage, crash, device data	Consent (Art. 6(1)(a))	Consent
Retargeting / advertising	Cookie, behavioral data	Consent (Art. 6(1)(a))	Consent / opt-out
Transactional communications	Email, phone, account	Contract (Art. 6(1)(b))	Contractual necessity
Marketing communications	Email, preferences	Consent (Art. 6(1)(a))	Consent (CASL)
DPWRA minimum wage compliance	Timestamps, GPS, payout data	Legal obligation (Art. 6(1)(c))	Legal obligation
Tax and financial record-keeping	Transaction, identity data	Legal obligation (Art. 6(1)(c))	Legal obligation

6. Disclosure of Personal Information

Aerrand does not sell your personal information. We do not share personal information with third parties for their own marketing without your consent.

With Other Platform Users

- Aerranders receive: Buyer name, delivery address, item category, and transaction reference
- Buyers receive: Aerrander first name and delivery status updates only. Aerrander GPS is not shared.

With Service Providers (Data Processors)

- Stripe Inc. — payment processing, escrow, chargeback handling, Aerrander payouts (U.S.)
- HubSpot Inc. — CRM, platform notifications (U.S.)
- Google LLC — analytics (IP anonymized), advertising, Google Maps Distance Matrix API for trip fee and DPWRA calculations (U.S.)
- Meta Platforms Inc. — advertising retargeting via Meta Pixel (U.S.)
- Cloud infrastructure and hosting providers — encrypted Platform hosting and data storage

Legal, Safety, and Fraud-Related Disclosures

- When required by law, court order, or legal process
- To anti-fraud organizations, financial institutions, or law enforcement where there is an imminent risk of fraud or criminal conduct
- To Stripe and card issuers in chargeback defence proceedings, including verification media, Aerrander inspection records, and transaction logs

Business Transfers

- In connection with a merger, acquisition, asset sale, or insolvency proceeding, your data may transfer to a successor entity bound by equivalent protections

7. Data Retention

- Account data: active account lifetime plus 3 years for fraud prevention and legal dispute purposes
- Transaction and financial records (fees, payouts, Guard calculations, escrow events): 7 years for Canadian tax compliance
- Guard verification media: 90 days from completion or dispute resolution, then permanently deleted
- Aerrander GPS location (precise): deleted within 30 days of job completion or cancellation
- Analytics data: raw session data 14 months; aggregated 26 months
- Crash and diagnostic data: 12 months maximum
- DPWRA engaged time logs and minimum wage compliance records: 7 years
- Marketing consent records: 3 years from withdrawal
- Parental consent documentation: lifetime of minor's account plus 1 year

8. Data Security

- TLS/SSL encryption for all data in transit
- AES-256 or equivalent encryption at rest for sensitive data
- Role-based and least-privilege access controls
- Multi-factor authentication required for all Aerrand personnel accessing production systems
- Audit logging of personal data access
- Regular vulnerability assessments

In the event of a personal data breach, we will notify affected users and applicable supervisory authorities within the timeframes required by applicable law — generally within 72 hours for EU/EEA/UK users under GDPR.

9. Minors and Parental Consent

The Platform is open to users aged 16 and older. Users aged 16–17 must provide verifiable parental or guardian consent prior to account creation. To become an Aerrander, users must be at least 18. We do not knowingly collect data from individuals under 16 without verified parental consent. Contact operations@aerrand.com to report a suspected underage account.

10. International Data Transfers

- EU/EEA–Canada: The European Commission adequacy decision for Canada (PIPEDA) permits transfers without additional safeguards. Onward transfers to U.S. processors rely on Standard Contractual Clauses (SCCs).
- UK–Canada/US: We rely on ICO-approved International Data Transfer Agreements (IDTAs) or SCCs.
- Canada–US: We rely on processor SCCs and applicable transfer frameworks for all U.S. service providers.

11. Your Rights

11.1 All Users (PIPEDA)

- Right to access, correct, and request deletion of personal information
- Right to withdraw consent, subject to legal or contractual limitations
- Right to file a complaint with the Office of the Privacy Commissioner of Canada (priv.gc.ca)

11.2 EU / EEA / UK Users (GDPR)

- Access (Art. 15), rectification (Art. 16), erasure (Art. 17), restriction (Art. 18), portability (Art. 20), objection (Art. 21)
- Right to withdraw consent at any time without affecting prior lawful processing
- Right to lodge a complaint with your national DPA. EU list: edpb.europa.eu. UK: ico.org.uk

11.3 California Residents (CCPA/CPRA)

- Right to know categories and specific pieces of PI collected, sources, purposes, and third-party disclosures
- Right to delete and correct personal information
- Right to opt out of sale or sharing for cross-context behavioural advertising. Aerrand does not sell PI. Our retargeting cookies (Meta Pixel, Google Ads) may constitute "sharing." Opt out via Cookie consent manager or by emailing operations@aerrand.com with subject "CCPA Opt-Out"
- Right to limit use and disclosure of sensitive personal information (SPI): precise geolocation (Aerranders) and date of birth
- Right to non-discrimination for exercising these rights
- Response window: 45 days, extendable by 45 days with notice

11.4 CCPA Personal Information Categories

CCPA Category	Examples Collected	Sold / Shared?
Identifiers	Name, email, phone, IP, device ID	Not sold; retargeting with consent only

CCPA Category	Examples Collected	Sold / Shared?
Customer records (Cal. Civ. Code §1798.80)	Name, address, Stripe payment token	Not sold
Protected classifications	Age (parental consent for 16–17)	Not sold
Commercial information	Transaction history, Guard records, Aerrand Points	Not sold
Internet / network activity	Platform browsing, analytics, crash logs	Shared for retargeting with consent
Geolocation (sensitive PI)	Precise GPS — Aerranders during active dispatch only	Not sold
Sensory data	Guard verification photos and video	Not sold
Inferences from PI	Interest profiles for ad retargeting	Shared for retargeting with consent

12. Contact and Complaints

Aerrand Inc.
Windsor, Ontario, Canada
Email: operations@aerrand.com | Website: aerrand.com

EU/EEA: Contact your national DPA (edpb.europa.eu). UK: ico.org.uk. Canada: Office of the Privacy Commissioner, priv.gc.ca. California: California Privacy Protection Agency, cppa.ca.gov.