

AeroRide Privacy Policy (Version 3.2)

Version 3.2 — Effective 2026-09-15

AeroRide Privacy Policy

AeroRide Inc., a Delaware corporation · U.S. Air Charter Broker · 14 C.F.R. Part 295 · Version 3.2

1. Who we are and who controls your data

AeroRide Inc. is a corporation organized under the laws of the State of Delaware, United States, with its registered address at 1401 Pennsylvania Avenue, Suite 105, Wilmington, Delaware 19806, United States. Telephone +1 786 982 6354. E-mail sac@aeroride.app, which is our channel for support, claims, notices and every request concerning your personal data.

AeroRide is an air charter broker under 14 C.F.R. Part 295, contracting as an indirect air carrier. It arranges and sells private air transportation performed by properly licensed direct air carriers; it does not operate aircraft and is never in operational control of a flight. AeroRide Inc. is the controller of the personal data described in this policy for every booking, whatever the route, except where it acts as a service provider or processor for a business customer. Each operating air carrier is an independent controller of the data it needs to discharge its own obligations as the carrier.

2. Scope

This policy applies to visitors to our website, registered users, passengers, Sales Partners and Operator personnel who use our services through the website, the mobile application and the APIs. Our services are offered from the United States and are directed principally to the United States market, including bookings for flights operated elsewhere. Where we serve individuals located in the United Kingdom, the European Economic Area or another jurisdiction with its own data-protection regime, the additional rights described in Section 12 apply to them and we apply the stricter standard.

3. Data we collect

- Identification: full name, one identification or passport number per passenger (a passport for international flights) and date of birth, to verify identity and manage bookings. The Platform records the document number exactly as it is entered; the air carrier checks the document itself at boarding.
- Contact: e-mail, telephone and address, for confirmations, invoicing and operational communications.
- Payment: we do not store the full card number. Every booking is paid in advance through the Platform; charges and refunds are processed by our payment gateway, Tilopay, using tokens it issues, consistent with the PCI DSS standard. Where AeroRide staff record a booking paid outside the gateway (for example by bank transfer), we keep only the record of the payment and the receipt.
- Payout data: for Sales Partners, the PayPal e-mail address registered for the payment of commissions; for Operators, the bank account details provided to AeroRide for the weekly settlement of flown flights.
- Travel: date, time, origin, destination, service type, the declared or estimated weight of each passenger, and any add-on requests you make (such as special luggage, catering or ground transport), to arrange the charter, check aircraft payload and issue the receipt; and, if you cancel a booking, the reason you give for the cancellation.
- Identity verification: when you create an account we verify your e-mail address, and we may verify your identity before processing a booking or a payment. Where in-app document validation or identity-verification mechanisms are used, for example liveness checks, the data is used exclusively to verify identity and prevent fraud, with prior notice and an impact assessment. Verification for boarding is performed by the air carrier, which checks each passenger's identification document against the document number registered in the booking and the booking QR code; the result of that check is recorded in the booking timeline on the Platform.
- Sensitive data: we do not collect health, disability or special-assistance information through the Platform, and the booking form has no field for it. If a passenger needs special assistance, tell us at

sac@aeroride.app; we handle that request only to arrange the assistance with the air carrier, and we do not process health information for any other purpose.

- Technical data: your IP address, which we use to limit abusive traffic and to estimate the country from which a booking is made, and which may appear in our server logs; and the local storage on your device that keeps you signed in. We do not use analytics or advertising cookies or software development kits in the application.

4. Purposes of processing

We process personal data to: arrange bookings and issue receipts; invoice and collect payment; make the disclosures required of an air charter broker; verify identity and prevent fraud and money laundering; record your acceptance of our legal documents; pay Operators and Sales Partners; provide customer support; send operational notifications; carry out marketing only with prior consent; analyze and improve the service through aggregate statistics; and comply with legal, tax and regulatory obligations.

5. Legal basis

Under United States law we process personal data to perform our contract with you, to comply with legal obligations, to prevent fraud and secure our services, and — for marketing and non-essential cookies — with your consent, which you may withdraw at any time. Where the EU or UK GDPR applies to an individual, the corresponding legal bases are performance of the contract, legal obligation, legitimate interest and consent.

6. Anti-money-laundering and sanctions

As a United States company, AeroRide applies U.S. law to its compliance program, including the Bank Secrecy Act and the USA PATRIOT Act as applicable to its activity and the sanctions programs administered by the Office of Foreign Assets Control (OFAC). AeroRide may verify user identity, screen users and passengers against U.S. and international sanctions and security lists, monitor transactions and report suspicious activity to the competent authorities. This processing is carried out to comply with a legal obligation.

7. Minors

7.1 Account holder. Accounts and contracting are directed at persons of legal age. We do not knowingly collect personal data from children under 13, and we do not knowingly sell or share the personal data of anyone under 16.

7.2 Minor passengers. A minor may travel as a passenger only when the person who makes the booking — the account holder or, for bookings made without an account, the contact person named in the booking — adds the minor to the booking, provides the minor's data and assumes responsibility for that data and for the minor's travel. We do not verify the relationship between the booking holder and the minor. Infants under three (3) may travel as lap infants; their age is checked against the date of the flight. We process the minor's data solely to arrange the flight.

8. Who we share data with

- Air carriers (Operators): we share only the data necessary for the flight and for boarding verification — each passenger's name, identification or passport number and date of birth, the declared weight, the itinerary and the booking QR code. We do not share the customer's e-mail address or telephone number with Operators; all communication between an Operator and a customer goes through AeroRide at sac@aeroride.app. Operators are contractually restricted to using that data only for the flight, and are prohibited from marketing to passengers or selling their data.
- Sales Partners: where a booking was made through a Sales Partner, that partner sees the booking data necessary to service its own customer — the booking, its status, its total price and the partner's commission — and nothing more; it does not see the Operator's pricing breakdown.
- Service providers: Tilopay, our payment gateway, which processes charges and refunds through tokens without sharing the card number with us; Microsoft Azure, which hosts the Platform and stores our databases and files; SendGrid, which delivers our e-mails; Google Maps, which provides maps and airport

locations in the Platform; and PayPal, through which we pay Sales Partner commissions. Each of them acts under confidentiality and data-protection agreements. We do not use analytics providers.

- Authorities: we may share limited data — name, itinerary, identification — with aviation, immigration, security or law-enforcement authorities where required by law.

We do not sell personal data, and we do not share it for cross-context behavioral advertising.

9. International transfers

Our providers, including Microsoft Azure, may operate servers in the United States and in other countries. Where personal data is transferred outside the country in which it was collected, we use contractual safeguards — including the European Commission’s standard contractual clauses and the UK addendum where applicable — together with encryption in transit (TLS) and encryption at rest provided by our cloud provider for our databases and file storage, with additional application-level encryption of passport and identification numbers and dates of birth.

10. Retention

- Accounting, invoicing and payment records: kept for at least five (5) years, and for longer where U.S. federal or state law requires it. These records are kept even after an account is closed.
- Booking and travel data: two (2) to five (5) years after the last interaction, for claims, disputes and regulatory purposes.
- Profile data: contact and profile data up to two (2) years after inactivity.
- Records of your acceptance of our legal documents: for each legal document you accept, we record the account that accepted it, the date and time of acceptance and the version accepted, and we keep that record for as long as your account exists and thereafter for the period applicable to booking records. Each version of our legal documents is kept as a separate, dated file. Where you give or withdraw consent to marketing communications, we keep a record of the date of that choice.

If you ask us to delete your data (Section 12), we anonymize your account and the personal data linked to it and keep only what the law requires us to retain, such as accounting, invoicing and payment records and the record of the legal documents you accepted.

11. Security

We apply technical and organizational measures including encryption in transit (TLS), encryption at rest of our databases and file storage, additional AES-256 application-level encryption of passport and identification numbers and dates of birth, secure authentication with revocable sessions, role-based access control that limits each operator and Sales Partner to its own bookings, rate limits by origin and the blocking of accounts that show abusive use, application logging, and a record of the staff member responsible for sensitive operations such as refunds, no-show decisions and cancellations. Staff and contractors sign confidentiality agreements. Access to passenger data is limited by role: AeroRide administrators; the staff of the air carrier performing the flight, including the assigned pilot, who see only their own operator’s bookings and never the customer’s e-mail address or telephone number; the Sales Partner that made the booking, who sees only its own bookings; and the person who made the booking.

12. Your rights

12.1 Rights. Depending on where you live, you may have the right to know what personal data we hold about you and to obtain a copy; to correct inaccurate data; to delete data; to opt out of sale, sharing or targeted advertising (we do not sell or share for advertising); to limit the use of sensitive personal information (we use identification and passport numbers only to arrange the flight, for boarding verification and to issue the receipt, and we do not use sensitive personal information for any other purpose, so no separate limitation setting is needed); to data portability; and not to be discriminated against for exercising these rights. Where the EU or UK GDPR applies to you, you also have the rights to restrict and object to processing and to withdraw consent at any time.

12.2 How to exercise them. Access and portability: you can download a copy of your personal data at any time from the app, using “Download my data”, which gives you a file in a structured, machine-readable format (JSON); you may also request a copy by writing to sac@aeroride.app. Correction: you can update your contact and profile data in the

app, or ask us at sac@aeroride.app. Deletion: send your request to sac@aeroride.app; we anonymize your account and the personal data linked to it and keep only the records the law requires us to retain, as described in Section 10. Any other request may be sent to sac@aeroride.app. We respond within forty-five (45) days of receiving a request, or within any shorter period the applicable law sets, and we may need to verify your identity before acting on it. An authorized agent may submit a request on your behalf with proof of authorization.

12.3 Appeal. If we decline your request, you may appeal by replying to our decision or writing to sac@aeroride.app with the word "Appeal" in the subject line. We will inform you of the outcome and of the further options available to you under the law of your state.

13. Complaints

If you have a concern about how we handle your personal data, contact us first at sac@aeroride.app so we can resolve it. If you are not satisfied, you may contact the consumer protection office of the attorney general of your state or, where the EU or UK GDPR applies to you, your national supervisory authority.

14. Cookies

We use only strictly necessary cookies and local storage — those needed to keep you signed in and to secure the service, including security cookies set by our hosting provider — which do not require consent. We do not currently use analytics or marketing cookies. If we introduce them, we will ask for your consent through a cookie banner before setting them, and you will be able to change your choice at any time through that banner and your browser settings. Where we ask for cookie consent, we will log your choice with its date and scope, and you will be able to withdraw it at any time. We do not sell or share personal data for cross-context behavioral advertising, so there is currently nothing for an opt-out preference signal to opt you out of. If that ever changes, we will honor the Global Privacy Control signal where the law requires it.

15. Breach notification

In the event of a security breach we follow a protocol of containment, risk assessment, remediation and notification, and we notify affected individuals and the competent authorities within the time frames and conditions established by the applicable U.S. federal and state breach-notification laws and, where they apply, the EU and UK GDPR. Operators and Sales Partners must notify us of any breach affecting passenger data within twenty-four (24) hours.

16. Impact assessments

Before implementing biometric verification or processing sensitive data, AeroRide carries out an assessment to evaluate the risks, define mitigation measures and confirm the proportionality of the processing. These assessments are reviewed periodically.

17. Updates

This policy is reviewed periodically and whenever there is a substantial change in our processing or in the law. Each version is published as a separate file bearing its version number and effective date, in the app and on the website, and earlier versions remain available on request at sac@aeroride.app. When we make material changes, you will be asked to review and accept the updated policy the next time you sign in to the app, before continuing to use the service; where the law requires it, we will ask for your consent again.

18. Contact

AeroRide Inc. · 1401 Pennsylvania Avenue, Suite 105, Wilmington, Delaware 19806, United States

+1 786 982 6354 · sac@aeroride.app