

ACMI.Direct Privacy Policy

1. Who We Are

This Privacy Policy explains how **Aeromanage LTD**, established in Cyprus and providing services as **ACMI.Direct**("ACMI.Direct", "we", "us"), processes personal data in connection with the ACMI.Direct online platform.

Data Controller:

Aeromanage LTD
Leontiou 163A, office 302, Limassol, Cyprus
Email for privacy matters: info@acmi.direct

If you are located in the UK, UK-GDPR applies; if in the EU, EU GDPR applies.

2. Types of Data We Process

ACMI.Direct is intentionally designed to store **minimal personal data**. We only collect:

2.1 Identity & Authentication Data

****Authentication Process:****

User authentication is handled via federated identity providers:

- Microsoft Entra ID B2C (for Microsoft corporate users),
- Google Cloud Identity (for Google Workspace users)

Upon successful authentication, identity claims are passed to ACMI.Direct.

****Data Collected and Stored by ACMI.Direct:****

- email address
- first name and surname
- company/legal entity name
- job title or position within the organization
- authentication tokens (session management)
- tenant identifiers

ACMI.Direct does NOT store passwords or credential secrets.

Authentication credentials remain with your identity provider (Microsoft or Google).

****Why we store this data:****

- To verify you are authorized to represent your organization
- To maintain audit trails of platform actions (RFQ submissions, offers, acceptances)
- To prevent abuse by unauthorized parties or fraudulent accounts
- To support fee calculation and dispute resolution
- **To display user identity to other Users for transparency**

2.2 Platform Operational Data (Business Data)

Necessary to operate the service:

- aircraft availability windows
- RFQs and RFQ metadata
- platform actions and audit logs
- offers submitted
- response timestamps
- flight-performance metadata used to validate successful leads
- analytics derived from your activity
- communications between Users conducted through Platform messaging features (used for fraud detection and fee validation purposes only)

2.3 Technical Data

- IP address
- device/browser metadata
- usage logs
- cookies strictly necessary for platform functionality

We do **not** use marketing cookies.

3. What We Do NOT Collect

We do **not** collect:

- passport data
- personal addresses

- financial credit card data
- crew information
- flight passenger data
- sensitive or special-category personal data

4. Legal Bases for Processing (GDPR Art. 6)

We process personal data under the following legitimate bases:

4.1 Contract Performance (Art. 6(1)(b))

To:

- create and verify User accounts
- authenticate access and validate user authorization to act on behalf of their organization
- maintain records of who submitted RFQs, offers, and acceptances
- support fee calculation and invoicing with accurate party identification
- deliver RFQs and offers with visible sender/recipient information
- operate the Platform workflows
- track actions for billing accuracy and dispute resolution

4.2 Legitimate Interests (Art. 6(1)(f))

To:

- verify User legitimacy and prevent fraudulent account creation
- detect and prevent platform abuse by unauthorized intermediaries
- maintain audit trails for security and compliance purposes
- maintain platform security
- prevent circumvention (Three-Strike Rule enforcement)
- generate anonymised analytics
- calculate success-based introduction fees

We ensure these interests do not override User rights.

4.3 Legal Obligations (Art. 6(1)(c))

For record-keeping required under applicable commercial or tax laws.

5. Why We Process Data (Purposes)

We process data solely for:

1. **Providing the ACMI.Direct Platform**
2. **User authentication via federated identity providers**
3. **Delivering RFQs and offers**
4. **Tracking actions for billing and fee calculation**
5. **Detecting circumvention or fraud**
6. **Analytics and service optimisation**
7. **Security and misuse prevention**
8. **Verifying user legitimacy and organizational authority**
9. **Maintaining audit trails and supporting dispute resolution**
10. **Preventing fraudulent activity and unauthorized access**

We do **not** sell personal data.

We do **not** share identifiable data with third parties, except subprocessors listed below.

6. Data Sharing & Subprocessors

We use service providers ("subprocessors") to operate the Platform:

6.1 Microsoft Azure & Microsoft Entra B2C

- federated identity authentication (Microsoft corporate users)
- identity claims processing
- cloud hosting
- database operations
- security logs

6.2 Google Cloud Platform

- federated identity authentication (Google Workspace users)
- identity claims processing

6.3 Internal verification providers (*optional*)

For confirming flight performance based on public or aviation databases.

6.4 No marketing/advertising processors

We do not use Google Analytics, Meta Pixel, or any advertising trackers unless you explicitly instruct (currently: **none**).

7. International Transfers

Data may be stored in Microsoft Azure regions within the EU or UK. If transfers outside the EU/UK occur, they rely on:

- EU Standard Contractual Clauses (SCCs)
- UK International Data Transfer Addendum
- Adequacy decisions where applicable

Microsoft maintains GDPR compliance and security certifications.

8. Data Retention

- User identity data (name, company, job title): **retained for duration of account + 7 years** (aligned with RFQ metadata retention for audit purposes)
- RFQ metadata: **7 years** (commercial accounting compliance)
- Activity logs: **24 months**
- Authentication tokens: **per Microsoft Entra B2C lifecycle**
- Billing data: **7 years**
- Analytics: anonymised and retained indefinitely

Users can request deletion of their account; operational data linked to billing and audit requirements cannot be erased before statutory retention periods.

9. Your Rights (GDPR Articles 12--23)

You may request:

- access to your data
- correction
- deletion ("right to erasure")
- restriction
- portability
- objection to legitimate interest processing
- withdrawal of consent (if ever used)

Requests can be made to info@acmi.direct.

You also have the right to lodge a complaint with your EU/UK supervisory authority.

10. CCPA/US Privacy Requirements

If you are a California resident:

- We do **not** sell or share personal data.
- You may request access, deletion, or correction of your data.
- You may request what categories of data we process.
- Your identity will be verified through your account.

11. Cookies

The Platform uses:

- **strictly necessary cookies** for authentication
- **session cookies** for login continuity

We do not use marketing or tracking cookies by default.

12. Security Measures

We implement:

- Microsoft Entra B2C identity protection
- Azure network isolation
- access controls
- encryption in transit and at rest
- audit logging
- role-based access management
- incident response protocols

13. Changes to This Policy

We may update this Privacy Policy from time to time.
The latest version will always be available on our website.

14. Contact Us

For questions, rights requests, or concerns:

Email: info@acmi.direct

Legal entity: Aeromanage LTD

Registered address: Leontiou 163A, office 302, Limassol, Cyprus