

Privacy Notice

Tribe Aviation Technologies Ltd — Version 2026.08.10 — Effective 10 August 2026

Contents

1. Who we are and what this notice covers
2. Children
3. Information we collect
4. Payments
5. Automated processing and AI features
6. How we use your information
7. How we share your information
8. Information provided about others
9. Special categories of information
10. How long we keep your information
11. Chat data storage and security
12. Your rights
13. Where your information is processed
14. Security and data breaches
15. Contact us
16. Changes to this Privacy Notice

1. Who we are and what this notice covers

1.1 Tribe Aviation Technologies Ltd ("Tribe", "we", "us") is a company incorporated in the Dubai International Financial Centre (DIFC). We operate a digital marketplace and software services for the business aviation sector, including the Tribe Platform, our websites and mobile applications (together, the "Services").

1.2 Our role depends on the information concerned. For some information we are the controller, meaning we decide why and how it is used: this covers Member account and billing details, our own marketing, our website and security logs, and job applications. For other information we are a processor, meaning we hold and handle it on a Member's instructions and that Member decides why it is used: this covers the client, passenger and charterer information Members submit to, or generate through, the Platform. Where we act as processor, the Member is your first point of contact, though you may also contact us and we will assist.

1.3 "Controller" and "processor" describe who decides how information is used, not who owns it. Members retain ownership of what they submit, as set out in our General Terms and Conditions.

1.4 Tribe is subject to the DIFC Data Protection Law No. 5 of 2020. Because we provide Services to Members in the European Economic Area and the United Kingdom, the EU General Data Protection Regulation and the UK GDPR also apply to the relevant processing. Where this Notice refers to "applicable data protection law", it means all of these together.

1.5 This Notice applies to everyone whose personal data we process, including Members (brokers, agents and operators) and their staff; guest users; charterers and end clients; operators who access the Platform by emailed link; passengers and other individuals whose details are submitted to us; job applicants and contest entrants; recipients of our marketing; and visitors to our websites.

1.6 This Notice does not apply to information collected by third parties, including third-party websites accessible through the Services. Charter contracts and flight payments take place between brokers, operators and their customers outside the Tribe Platform, and are governed by those parties' own privacy notices.

2. Children

2.1 The Services are business tools and are not intended for children under 18. We do not knowingly collect personal data from children, except where a Member submits passenger details for a minor in connection with a flight request (see Section 8). If you believe we hold a child's personal data without an appropriate basis, contact us using the details in Section 15.

3. Information we collect

3.1 The table below sets out what we collect, why, and our lawful bases. Information that needs additional protection under data protection law is covered separately in Section 9.

Context	Types of information	Purpose	Lawful bases
Account information	Name, email address, contact number, company details, role, and other details provided at registration.	To create and administer your account, communicate with you, and personalise your experience.	Performance of a contract; legitimate interests.
Chat and marketplace activity	Messages sent and received through platform chat; flight requests; quotes; aircraft availability; attachments and documents you upload.	To operate the marketplace, deliver messages, and maintain your archive.	Performance of a contract; legitimate interests.
Flight information	Departure and arrival details, dates, number of passengers, aircraft type, and related operational data.	To provide accurate marketplace information.	Performance of a contract; legitimate interests.
Billing contact details	The contact and company details we use to invoice you for your membership.	To bill membership fees.	Performance of a contract; compliance with legal obligations.
Your own bank details (Members)	Where you choose to store them in your company profile: beneficiary name, bank name and address, account number, IBAN, SWIFT or institution code, routing number, intermediary bank details, and currency.	So that they can be reproduced on invoices generated through the Platform for your own clients, where that feature is available to you. See Section 4.	Performance of a contract; legitimate interests.
Correspondence	Records of your emails, messages, survey responses and support requests.	To respond to enquiries, provide support, and improve the Services.	Legitimate interests.
Operator and partner information	Names, email addresses, telephone numbers and company details, including operators invited by emailed access link.	To facilitate communication and manage business relationships.	Performance of a contract; legitimate interests.
Job applications	Name, contact details, CV, education and employment history.	To evaluate your application.	Steps prior to an employment contract; legal obligations; legitimate interests.
Marketing	Name, contact information, and your preferences.	To send news, offers and other communications.	Consent; legitimate interests in promoting our Services.
Contests and promotions	Contact information provided on entry.	To administer the contest and notify winners.	Legitimate interests.
Device and usage	Device identifiers, IP address,	To secure, troubleshoot,	Legitimate interests;

Context	Types of information	Purpose	Lawful bases
data	browser type, pages viewed, and server logs.	operate and improve the Services.	consent where required.
Information about others	Passenger details submitted by a Member, which may include name, date of birth and passport information. Health, mobility and dietary information is covered in Section 9.	To support flight requests and operations.	Legitimate interests; performance of a contract with the submitting Member.

4. Payments

4.1 No payments are taken through the Platform. We do not collect, receive, process or store payment card numbers or card security data at any point.

4.2 Membership fees are paid outside the Platform: either by card through Mamo Pay, a payment services provider regulated in the United Arab Emirates, which collects card details on its own pages and under its own privacy notice; or by bank transfer against an invoice we send you.

4.3 Separately, if you are a Member you may choose to store your own bank details in your company profile. We hold these for one purpose only: so that they can be reproduced on invoices generated through the Platform for your own clients, where that feature is available to you. We do not use them to take payment from you, and we do not disclose them other than by including them on invoices you create. You can update or remove them at any time in your profile.

4.4 Tribe does not charge, collect or hold payments for flights. All charter payments are settled directly between the parties concerned, outside the Platform.

5. Automated processing and AI features

5.1 What we use it for. We use automated features that read, interpret and summarise information, and an assistant that answers questions and helps prepare responses. Specifically:

- Quote extraction — when an operator sends a quote as a document or message, we read it automatically and extract details such as price, aircraft, dates, times and airports.
- Inquiry interpretation — we read flight requests to identify the route, dates, passenger numbers and requirements.
- Orion, our assistant — available in the Platform and through WhatsApp. It can answer questions about information you have access to, summarise conversations and documents, look up records, and prepare draft responses for you to review and send.

5.1a Document search. A Member may choose to make one of its own documents available to the assistant, so that the assistant can answer questions from it. No document is used this way unless the Member enables it. Before that happens, we check the document automatically to exclude those containing personal information — that check is automated and may not identify every case. The text we extract is stored separately from the document and in the same region, is available only to users of the Member that enabled it, and is kept only while the document remains enabled — it is removed if the Member turns the feature off for that document, deletes the document, or if our automated checks later flag it.

We will update this Notice before introducing any further AI-assisted feature that processes personal data.

5.2 How it works. These features — which we refer to together as our AI-assisted features, and which include the assistant currently provided under the name "Orion" — use large language models supplied by third parties. We select the model we consider best suited to each task, and the models we use may

change over time. We do not operate any model ourselves. The providers we currently use, and where they process information, are identified in our Sub-Processor List.

5.3 What goes into them. The content of quotes and the documents they arrive in, flight request details, chat messages, records you ask the assistant about, and anything you type into it. This can include names and contact details of people connected with a trip, and on occasion information of the kind described in Section 9. Do not submit payment card details, and please do not send passport images or health information through WhatsApp.

5.4 Where the processing happens. Model processing takes place on Amazon Web Services infrastructure. Our primary region is India, but AWS may route an individual request to another region depending on available capacity. Section 13 describes the safeguards that apply.

5.5 Training. Your information is not used to train, tune or improve any model. We use model providers only on terms that prevent the prompts we send and the outputs we receive from being used to train or improve their models, and we do not train any model of our own on your information. If we could not obtain that protection from a provider, we would not use it. This commitment applies whichever model we use, and does not change if we change provider.

5.6 How long it is kept. Documents, messages and the information extracted from them are kept in accordance with Section 10. Where we extract information from a document, a copy of that document is retained in your own storage area so that the extracted record has a source; the temporary files used during extraction are deleted after 30 days. The assistant retains recent conversation context so that it can follow a conversation; that context expires automatically after 90 days. We are able to clear an assistant conversation on request.

5.7 Accuracy, and what this is not. Automated reading can be wrong. It can misread figures, dates or aircraft details, omit conditions and exclusions that were present in the original, and occasionally produce something the original did not say. Information produced this way is not a quote, an offer, a confirmation or advice, and it binds no one. The original document takes precedence and should be checked before anyone relies on the extracted version.

5.8 Human involvement. These features assist people; they do not make decisions about you. Extraction and interpretation produce information for a person to review, and anything the assistant drafts is sent only if a person chooses to send it. No decision producing legal effects, or similarly significant effects, concerning you is made by automated means alone.

5.9 What the systems are permitted to do. These features operate within limits that we set and record. They may read, extract, structure and summarise information the requesting user is already entitled to see, and prepare drafts for that user, for the purposes described in this Notice. They may not access information outside that user's permissions, determine their own purposes, send a message or contact anyone without a person choosing to send it, make or accept an offer, or take any step that creates a contract.

5.10 Your choices. You may object to this processing, ask for a person to review anything produced by it that affects you, and exercise the other rights in Section 12, by contacting fn@flytribe.ae.

5.11 What we may not be able to undo. Once information has been extracted into a record, or reproduced in a document or a message thread, complete removal may not be technically possible. If you ask us to delete your information, we will tell you plainly what has been removed and identify anything that has not.

5.12 Responsibility. Tribe is responsible for these features and for how they process your information, even though the underlying models are operated by a third party.

6. How we use your information

6.1 In addition to the purposes in Section 3, we use personal data to:

- enable account registration and navigation of the Services;

- manage our relationship with you and keep you informed about your requests;
- send reminders, flight updates and service information;
- investigate and resolve complaints, provide support, and honour your rights and requests;
- send marketing where you have consented or where we may otherwise lawfully do so;
- monitor, secure and improve the Services, including preventing misuse; and
- comply with applicable laws and regulations.

6.2 We may create aggregated, de-identified statistics from Member data. Generic statistical data disclosed outside Tribe is drawn from at least three different Members, as described in our General Terms and Conditions.

7. How we share your information

7.1 Service providers. We share personal data with the providers that host and support the Services. As at the date of this Notice these are: Amazon Web Services (hosting and infrastructure, including Amazon SES for email delivery); Twilio (WhatsApp messaging); and Mamo Pay (card payment processing). Our current list, with purposes and processing locations, is maintained in our Sub-Processor List, available on request.

7.2 Other Members and users. Information you post to the marketplace, and messages you send through the Services, are shared with their intended recipients. Operator availability may be visible to Members using the marketplace.

7.3 Professional advisers. We may share information with consultants, banks, legal advisers, insurers and accountants who assist our business, and with providers of flight support and concierge services where relevant to a request.

7.4 Corporate transactions. We may share information within our corporate group, and with a buyer or successor in the event of a sale, merger or transfer of our business.

7.5 Legal. We may disclose information to comply with court orders, laws or legal process, including government and regulatory requests, or to enforce our agreements and protect the rights, property or safety of Tribe, our people, our users or others. Where we receive a request from a public authority we assess it and, where practicable, seek written assurances about how the information will be handled.

7.6 We do not sell personal data, and we do not share personal data with social media or advertising companies.

8. Information provided about others

8.1 Members and users may submit personal data about other individuals — for example passenger names, dates of birth and passport details in connection with a flight request. Passport and identity information is sensitive: only submit it where necessary, and only where you have informed the individual how their data will be used and have the right to share it with us.

8.2 We process such data only to support the relevant request and the operation of the Services, we restrict access to it, and we retain it in line with Section 10. Individuals whose data has been submitted to us may exercise the rights in Section 12.

9. Special categories of information

9.1 Some flight requests include information that needs extra protection under data protection law. Dietary requirements can reveal a person's religious beliefs, and accessibility or mobility requirements are health information. The law calls these "special categories" and sets a higher bar for handling them.

9.2 We do not collect this information in order to arrange or operate flights. That is done by the broker and the operator directly. Where it is present in our systems, it is because a Member has submitted it, or because it appeared in a document or message the Member sent through the Platform and was captured

when that document was read. We hold it on the Member's behalf so that the Member can carry out its own business.

9.3 Because we hold it on a Member's behalf, that Member is responsible for having a lawful basis for it — which, for this category of information, means the explicit consent of the individual concerned. Our General Terms and Conditions require Members to obtain that consent and to provide evidence of it on request. If you are a passenger and wish to know what has been shared about you, or to withdraw your consent, contact us at fn@flytribe.ae. We will handle your request directly where we are able to, and otherwise direct you to the Member who submitted the information.

9.4 How long we keep it. We do not delete this information on a fixed schedule. It is retained with the record of which it forms part, for as long as the Member requires it to conduct its business — a passenger's dietary or accessibility requirement may remain relevant to that Member for as long as it serves that passenger. We delete it on the Member's instruction, or on request from the individual concerned, so far as we are able to identify and remove it. It is not used for any other purpose, and is not used to train, tune or improve any model.

9.5 Access to this information within Tribe is restricted to staff who need it in order to support a Member.

10. How long we keep your information

10.1 We keep personal data only for as long as we need it for the purposes described in this Notice, and then delete or anonymise it. In deciding how long that is, we consider how long the data is needed to provide the Services to you, whether the data is sensitive, whether you can delete it yourself, and any legal, tax or accounting period we are required to observe.

10.2 In practice this means:

Information	How long we keep it
Your account, and the messages and quotes in it	While your account is open. When your account closes we keep them for thirty-five (35) days so you can export your records or reactivate. After that we remove your name, email address and telephone number from the account record and replace them with random values, so that what remains cannot be traced back to you. You can ask us to do this sooner.
Files you upload — documents, attachments and profile pictures	While your account is open, and for thirty-five (35) days after it closes. Then deleted. You can delete any file yourself at any time, and we delete it when you do.
The copy of a file retained when information is extracted from it	Where we extract information from a document, a copy of that document is kept in your storage area so that the extracted record has a source. That copy is kept and deleted on the same basis as the file it came from.
Records of a quote, request or booking involving another business	The record of the dealing is kept, because the other business was party to it and has its own reasons to keep it. Your name, email address and telephone number are removed from it when your account is anonymised, so the record no longer identifies you.
Dietary, accessibility and other special category information	Retained with the record of which it forms part, for as long as the Member requires it to conduct its business. Deleted on the Member's instruction, so far as we are able. See Section 9.
Conversation history kept by the Orion assistant	Expires automatically after ninety (90) days. You can ask us to clear a conversation sooner.
Temporary files created while an AI feature extracts information from a document	Thirty (30) days, then deleted.
Dormant accounts	Closed after an extended period of inactivity, as described in our General Terms and Conditions, and then treated as above.

Information	How long we keep it
Server and application logs	Up to ninety (90) days, then deleted automatically.
Database backups	Thirty-five (35) days on a rolling basis, then overwritten.
Billing records and invoices	For the period required by applicable tax and accounting law, which is longer than the periods above.

10.3 Where we must keep information because of a legal obligation, or because it is needed to establish, exercise or defend a legal claim, we keep only what is necessary for that purpose and delete the rest.

10.4 What "anonymised" means here, and why we do it rather than delete everything. When we anonymise your account we replace your name, email address and telephone number with random values, and we delete your files, your profile picture, your login history, your searches, your saved aircraft and your contacts. We keep no key, table or copy that would let us reverse this, so the remaining records cannot be linked back to you by us or by anyone else. We do this rather than erase the records outright because a quote or a request you sent involved another business, which has its own record of that dealing and its own reasons to keep it. Anonymising removes you from those records without destroying the other party's. Once information has been anonymised in this way it is no longer personal data, and this Notice no longer applies to it.

10.5 When you ask us to delete your data, we remove it from our live systems within one month and confirm this to you. Copies may remain in our routine backups for up to a further thirty-five (35) days, during which they are isolated from any further use and are not accessible to our team, and are then overwritten.

11. Chat data storage and security

11.1 Chat messages and submissions are stored on Amazon Web Services infrastructure, encrypted at rest and protected in transit by HTTPS/TLS.

11.2 Tribe personnel do not access the content of chat messages except where strictly required for support at your request, to comply with law or regulatory obligations, or on a verified request from the rightful account owner. Limited metadata and operational logs may be accessed for troubleshooting and security.

11.3 Tribe does not monitor, validate or control the content Members transmit through the chat feature. Members remain responsible for the legality, accuracy and appropriateness of the content they transmit.

11.4 On request, Tribe will provide an account's chat data to its rightful owner in a machine-readable format where technically feasible.

12. Your rights

12.1 Under applicable data protection law you have the right to:

- access your personal data and receive a copy, including in a structured, commonly used, machine-readable format;
- have inaccurate or incomplete data corrected;
- have your data erased where there is no longer a valid reason for us to process it;
- restrict processing in certain circumstances;
- object to processing based on legitimate interests, and to direct marketing at any time;
- withdraw consent at any time, where processing is based on consent; and
- not be subject to a decision based solely on automated processing that produces legal or similarly significant effects.

12.2 Exercising your rights is free of charge. To make a request, contact us at fn@flytribe.ae. We will verify your identity and respond within the timelines required by applicable law, generally within one month. Where a request is manifestly unfounded or excessive, in particular because it is repetitive, we may charge a reasonable fee reflecting the administrative cost of responding, or decline to act, and we will explain why. Fees described in our General Terms and Conditions relate only to optional services and never to the exercise of statutory rights.

12.3 You can also manage certain choices directly: update your details by logging into your account; unsubscribe from marketing using the link in each message; and adjust device permissions in your device settings.

12.4 How we carry out an erasure request. We delete your files, profile picture, login history, searches, saved aircraft and contacts, and we anonymise your account record and the transaction records attached to it, as described in Section 10.4. We do this within one month. Two things we will always tell you plainly: records of dealings you had with another business are anonymised rather than erased, for the reason given in Section 10.4; and copies may persist in our routine backups for up to a further thirty-five (35) days before they are overwritten, during which they are isolated and not available to our team. Where we are required by law to keep something, we will tell you what and why.

12.5 Complaints. If you are not satisfied with how we handle your data, you can complain to the DIFC Commissioner of Data Protection. Members and individuals in the EEA may contact their local supervisory authority, and those in the UK may contact the Information Commissioner's Office. We would appreciate the chance to resolve your concern first.

13. Where your information is processed

13.1 Tribe stores personal data on Amazon Web Services infrastructure in India (AWS Asia Pacific, Mumbai). Our team works remotely and may access these systems from countries other than the United Arab Emirates.

13.2 Some information is processed elsewhere. Audit logs recording access to our systems are held in the United Arab Emirates. Our WhatsApp messaging is operated through Twilio, which processes message content in the United States and Ireland. Membership card payments are handled by Mamo Pay in the United Arab Emirates. Our published legal documents and public assets are served from Amazon Web Services infrastructure in Sweden and the United Arab Emirates.

13.3 AWS processes data on our behalf under the AWS Data Processing Addendum, which incorporates the European Commission's Standard Contractual Clauses (Decision 2021/914) and commits AWS to corresponding protections including security measures and breach notification. Because we serve Members in the European Economic Area and the United Kingdom, those clauses — together with the UK International Data Transfer Addendum where UK data is involved — are the safeguards we rely on for transfers to India.

13.4 Model processing for the features described in Section 5 takes place on Amazon Web Services infrastructure, and AWS may route an individual request to a region other than India depending on available capacity. The safeguards in Section 13.3 apply to that processing.

13.5 Under DIFC law, transfers to jurisdictions the Commissioner of Data Protection has not recognised as providing adequate protection require appropriate safeguards. India, the United Arab Emirates and the United States are not recognised; Sweden and Ireland are.

13.6 You may request a copy of the safeguards applying to a particular transfer by contacting us at fn@flytribe.ae.

14. Security and data breaches

14.1 We implement technical and organisational measures proportionate to the risk of the processing, including encryption of data in transit and at rest, access controls and role-based permissions, network isolation of production systems, and use of managed security services. We review these measures on an

ongoing basis. No system can be guaranteed completely secure; if you believe your interaction with us is no longer secure, contact us immediately.

14.2 A "personal data breach" means an event leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data processed by Tribe.

14.3 Where a breach creates a risk to the rights and freedoms of individuals, we will notify the relevant supervisory authority without undue delay and, where feasible, within 72 hours. The notification will describe, to the extent known, the nature of the breach, the categories of data and individuals affected, the likely consequences, and the measures taken.

14.4 Where a breach is likely to result in high risk to individuals, we will notify those affected without undue delay, with the information available and steps they can take to protect themselves.

14.5 We take proportionate remedial steps, may delete affected data where its retention poses ongoing risk, and keep a record of personal data breaches which may be provided to supervisory authorities on request.

15. Contact us

15.1 Controller: Tribe Aviation Technologies Ltd, Unit IH-00-01-01-OF-01, Level 01, Innovation One, Dubai International Financial Centre, Dubai, UAE.

15.2 Privacy and data protection requests, including requests to access, correct or delete your information: fn@flytribe.ae. General enquiries: support@flytribe.ae. Telephone: +971 4 287 4677.

15.3 Data Protection Officer: Ferhan Nyo, fn@flytribe.ae.

16. Changes to this Privacy Notice

16.1 We may update this Notice from time to time. Each version carries a version number and effective date. We will notify you of material changes through the Services or by other means before they take effect, and the current version is always available on our website and applications.