

Privacy Policy

AlterEgo Travel Concierge

Effective date: 11 December 2025

Last updated: 2 September 2026

1. WHO WE ARE

The controller of personal data is:

ALTER EGO CONCIERGE SERVICE LLC

Email for data protection matters: support@alterego.travel

In this Policy, 'we', 'us', and 'our' mean the above-mentioned Company, and 'User' means a natural person who installs or uses the AlterEgo Travel Concierge mobile application (hereinafter – the 'App').

We act in accordance with the laws of Ukraine and, where applicable, with Regulation (EU) 2016/679 (GDPR) with respect to Users located in the EU/EEA.

2. SCOPE OF THIS POLICY

This Policy applies to:

- use of the App;
- interaction with managers in chat;
- processing of requests related to travel and related services;
- electronic communication with us (email, push notifications, etc.);
- all other situations in which we receive personal data from you in the course of our business.

3. KEY TERMS

Personal data – any information relating to an identified or identifiable natural person.

Processing – any operation or set of operations performed on personal data (collection, recording, organisation, storage, adaptation, alteration, transfer, access, deletion, etc.).

Controller – the Company that determines the purposes and means of processing personal data.

Processor – a natural or legal person who processes personal data on behalf of the Controller on the basis of a contract (for example, cloud services, email/SMS providers).

Soft Delete – deactivation of an account without physical deletion of all User personal data from our systems.

Hard Delete – final, irreversible deletion of personal data from our operational systems (with the exception of data that must be retained under the law).

4. PRINCIPLES OF PERSONAL DATA PROCESSING

We process personal data in accordance with the following principles:

- lawfulness, fairness and transparency;
- purpose limitation – data are collected for specific and legitimate purposes;

- data minimisation – we collect only the data that are necessary;
- accuracy – we strive to keep data up-to-date and accurate;
- storage limitation – data are stored no longer than necessary;
- integrity and confidentiality – we protect data against unauthorised access;
- accountability – we are able to demonstrate compliance with these principles.

5. WHAT DATA WE COLLECT

5.1. Data you provide yourself

When registering and using the App, you may provide:

- first name and last name;
- date of birth;
- phone number;
- email address;
- password (stored in hashed form);
- interface language / locale settings;
- other profile data if provided for by the functionality.

For arranging trips (where necessary):

- passport details (series/number, date of issue, expiry date, issuing authority, citizenship);
- photos of passports and other documents that you upload or scan with the camera;
- data needed for visas, insurance and bookings (for example, gender, place of residence, emergency contact details).

In correspondence with managers (chats):

- text messages;
- media files (photos, videos, documents);
- voice messages;
- geolocation (if you send it);
- any other information that you voluntarily provide.

5.2. Data collected automatically

When using the App, we may automatically receive:

- device information (model, type and version of operating system, App version, language settings);
- IP address and approximate geographical location (at the country/region level);
- technical identifiers of the App and device;
- event logs (screen views, button clicks, session duration);
- information on errors, crashes and performance indicators.

As a rule, these data are used in an aggregated and/or anonymised form for statistics and service improvement.

5.3. Geolocation data

The App may request access to geolocation via standard operating system mechanisms (for example, 'Allow once', 'Allow while using the app', 'Always'), depending on the version of the App and the device settings.

At the time of updating this Policy:

- geolocation is mainly used at your initiative (when you press 'Share location' in the chat with a manager);
- future versions of the App may include features of personalised recommendations based on your location (for example, suggestions for nearby restaurants or activities) if you have granted the relevant permission in your device settings.

Providing access to geolocation is voluntary. You can change your choice at any time in your device operating system settings.

5.4. Address book contacts

If you create a group chat and grant the App access to your contacts, the phone numbers from your address book are sent to Alterego servers solely in order to determine which of your contacts already have an Alterego account. The numbers are used only for this matching, are not stored on our servers and are not transferred to third parties. Granting access is voluntary: if you do not grant it, the App will not read your address book and will not send any numbers, and creating a group chat will be unavailable – the rest of the App's features will work as usual. You can withdraw access at any time in your device settings.

5.5. Automated recognition of document data

To spare you manual data entry, the App offers to scan the page of your international passport. If you choose this option, the photo of the document page is transferred to Alterego servers and further – to the automated recognition service Microsoft Azure Document Intelligence (Microsoft Corporation), which reads the document data from it (surname, given name, number, date of birth, sex, date of issue and expiry date, citizenship) and returns them to us to fill in the fields. The recognised data are shown to you for checking before saving. Neither the photo nor the data obtained from it are used to train artificial intelligence models. Scanning is voluntary: you can always fill in the same fields manually, in which case the document photo is not transferred to the recognition service.

6. SOURCES OF DATA

We obtain personal data:

- directly from you (registration, chat, forms in the App);
- from your device and software libraries (analytics, logs, crashes);
- from travel service providers (booking confirmations, trip statuses);
- where permitted by law – from public authorities and other sources.

7. PURPOSES AND LEGAL BASES OF PROCESSING

7.1. Performance of a contract / provision of services (GDPR Art. 6(1)(b))

We process your data because it is necessary to:

- create, maintain and administer your account;
- provide access to the App's features;
- communicate with you via chat or other channels;
- prepare, agree and implement individual travel offers;
- arrange bookings of tickets, hotels, transfers, insurance and other services;
- transfer your passport and contact details to the relevant service providers (airlines, hotels, insurers, tour operators, transfer services, visa centres, etc.).

7.2. Legitimate interests of the Company (GDPR Art. 6(1)(f))

We may process your data for:

- protecting the rights and interests of the Company in case of disputes;
- preventing fraud, abuse of the App and security breaches;
- assessing the quality of service and improving the service;
- internal analytics, including analysis of anonymised or aggregated data;
- ensuring stable and uninterrupted operation of the App.

We always assess that our legitimate interests do not override your fundamental rights and freedoms.

7.3. Compliance with legal obligations (GDPR Art. 6(1)(c))

We may process data where necessary for:

- fulfilling accounting and tax obligations;
- compliance with legal requirements in the field of financial monitoring (where applicable);
- responding to lawful requests from public authorities.

7.4. Consent (GDPR Art. 6(1)(a))

Where the legal basis for processing is your consent (for example, certain types of marketing communications, use of geolocation for personalised recommendations), we:

- clearly request consent;
- explain why the processing is needed;
- provide the possibility to withdraw consent at any time.

Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal.

8. CHATS WITH MANAGERS

8.1. All messages in chats (text, photos, documents, voice messages, geolocation) are stored in our system for the period necessary to provide services, resolve possible disputes and fulfil legal obligations.

8.2. We may use the content of chats to:

- respond to your requests and provide support;
- document agreements regarding trips, bookings and other services;
- resolve disputes between you and third parties (service providers), where appropriate;
- conduct internal audits of service quality, training and control of staff performance (within reasonable limits and with restricted access).

8.3. Only authorised employees of the Company who need such access to perform their duties (managers, support service, legal and finance specialists in case of disputes) have access to chats.

8.4. In case of Soft Delete of your account, the chat history remains in the CRM, but:

- is not used for direct marketing mailings in relation to such account;
- may be used in aggregated/anonymised form for analytics;
- may be used for protection of the Company's rights or fulfilment of legal obligations.

8.5. In case of Hard Delete (final deletion), the chat history that is not subject to mandatory retention by law is deleted or anonymised.

9. PUSH NOTIFICATIONS

The App may send you push notifications regarding:

- new messages from managers;
- confirmations and changes in bookings;
- reminders about upcoming trips and important actions;
- technical updates of the service;
- in some cases, marketing or informational offers.

Push notifications are sent only if you have enabled them in your device operating system settings. You can change notification settings at any time in your device settings.

10. TRANSFER OF DATA TO THIRD PARTIES

We may transfer your personal data to the following categories of recipients:

- airlines and their reservation systems;
- hotels, apartments and other accommodation providers;
- tour operators and other providers of travel services;
- insurance companies;
- providers of transfers and ground transport;
- visa centres and other involved organisations (if you request assistance with document preparation).

In doing so, we act as a technical intermediary: you provide the data, and we transfer them to the provider. You are responsible for the accuracy and completeness of the data provided.

11. PROCESSORS (TECHNICAL PROVIDERS)

To operate the App, we engage the following providers:

- Amazon Web Services (AWS) – hosting, file storage and computing;
- Microsoft Corporation (Azure Document Intelligence) – automated recognition of data from document photos;
- Google LLC (Firebase) – delivery of push notifications and analytics of App usage;
- Telnyx LLC – sending SMS with verification codes.

Each of these providers acts under a contract with the Company that obliges them to process personal data only in accordance with our instructions, to ensure the confidentiality of the information and to apply protection measures equivalent to those observed by the Company.

12. INTERNATIONAL DATA TRANSFERS

Your data may be stored and processed on servers located both in Ukraine and in other countries. In case of data transfer to countries where the level of data protection may differ from European standards, we take measures provided for by law (for example, standard contractual clauses).

13. DATA RETENTION PERIODS AND DELETION

We store personal data for as long as necessary for the purposes for which they were collected or to comply with legal obligations.

Approximately:

- account data – for the duration of use of the App and for a certain period after deactivation (taking into account possible claims);
- booking data (including passport data) – until the end of the trip and for a reasonable period thereafter;
- chat data – for the period necessary to provide services, resolve disputes and conduct audits;
- financial and accounting data – for the periods established by law (usually at least 3–5 years).

13.1. Soft Delete (deletion of account in the App)

When you press 'Delete account' in the App:

- the account is marked as 'deleted';
- account data (including chat history, profile, trip history) are stored in the CRM without physical deletion;
- when attempting to log in again, the User sees a screen with the message 'Account deleted' and an option to restore the account;
- data of such an account are not used for direct marketing mailings, but may be processed to comply with legal obligations and to protect the rights of the Company.

13.2. Hard Delete (final deletion)

To fully delete personal data, the User may send a request to: support@alterego.travel

After receiving the request, an authorised employee of the Company:

- 1) identifies the User and clarifies the scope of data to be deleted (if necessary);
- 2) confirms receipt of the request;

3) within up to 30 calendar days carries out irreversible deletion of personal data from operational systems, except for data that must be retained by law (in particular, accounting documentation);

4) informs the User about completion of the request.

After Hard Delete, personal data that are not subject to mandatory retention are deleted or anonymised.

14. DATA SECURITY

We apply technical and organisational measures to protect personal data, including:

- encryption of data during transmission (HTTPS/SSL);
- restricting access to information systems based on the 'need-to-know' principle;
- access control and authentication of employees;
- backup and access monitoring;
- internal confidentiality policies and staff training.

No online service can guarantee absolute security; however, we take all reasonable steps to protect your data.

15. YOUR RIGHTS

You have the right (within the limits established by law):

- to know whether we process your personal data;
- to obtain access to your data and a copy of them;
- to request correction of inaccurate or outdated data;
- to request restriction of processing in certain cases;
- to object to processing based on legitimate interest;
- to request deletion of data (Hard Delete);
- to withdraw consent where processing is based on consent;
- to lodge a complaint with the competent data protection authority.

To exercise your rights, you can contact us at: support@alterego.travel

16. CHILDREN

The App is intended only for adults (18+). We do not knowingly collect data of persons under 18 years of age. If we become aware that we have received such data, we will take steps to delete them.

17. CHANGES TO THIS POLICY

We may update this Policy from time to time. The new version takes effect from the moment it is published in the App, unless otherwise expressly stated.

18. CORPORATE CHANGES (MERGERS AND ACQUISITIONS)

In the event of reorganisation, merger, acquisition or sale of the Company's business, personal data may be transferred to the successor, provided that it ensures a level of data protection that is equivalent to or

higher than that provided by this Policy.

19. COOKIES AND SIMILAR TECHNOLOGIES

We may use cookies and similar technologies (for example, mobile SDKs) for:

- user authentication;
- saving settings;
- ensuring stable operation of the App;
- analytics and performance improvement.

Cookies are not used to directly identify you outside the App. You can manage permissions for collection of certain data via your device settings.

20. FRAUD PREVENTION AND SECURITY

We may process certain data in order to:

- detect and prevent fraud;
- detect and prevent unauthorised access to accounts;
- monitor suspicious activity in chats;
- ensure technical and operational security of the App.

Where necessary and in accordance with the law, we may transfer data to competent public authorities.

21. CONTACTS

For all questions related to the protection of personal data, you can contact us at:

Email: support@alterego.travel