

PRIVACY NOTICE

We are an innovative and dynamic company on a mission to simplify sustainable mobility internationally. Our application offers a user friendly ticketing solution for travellers, transport authorities and public transport operators.

We invite you to read our privacy notice below to learn more on how we are committed to respect your privacy and protect your personal data.

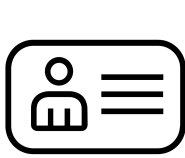
To give you a convenient overview of how we process your data, we use [Privacy Icons](#), an initiative by leading Swiss companies to create transparency in data processing.

Table of contents

A. How we treat your data (privacy icons)	2
B. Contact information of the Controller and the DPO	4
Data Controller	4
Data Protection Officer	4
C. Data controllership and applicable law	4
D. Processed personal data	4
General information about the customer	4
Details of fellow travellers in accordance with GTC, section III. A. 2.	5
Means of payment data	5
Purchase data	5
Information about the device	5
Usage data	5
E. Processing purposes and modalities	5
F. Legal basis	6
G. Automated decision-making and profiling	7
H. Security	7
I. Data Transfer	7
J. Account Creation and Administration via SSO	9
K. Customer contact	10
L. Data retention period	11
M. Exceptions to the time limits according to section L	11
N. Right to erasure and to be forgotten	11
O. Correction and limitation	12
P. Information and transmission rights	12
Q. Right of objection	12
R. Right to lodge a complaint	13
S. Data processing location	13
T. Data protection representation in the European Union	13
U. Changes of this privacy notice	13
V. Accessibility and download of the privacy notice	13

A. How we treat your data (privacy icons)

Our aim is to provide you with an easy-to-understand overview of how your personal data is processed. The main purpose of the processing is, of course, to fulfil the contract with you, i.e. to provide you with the correct, valid ticket.



General Data

We process general personal data about you, such as your name and contact details.

Example: We display your name on the digital ticket in the FAIRTIQ app.

See section:
[Processed personal data](#)



Financial Data

We process your financial data.

Example: You register a payment method in the FAIRTIQ app.

See section:
[Processed personal data](#)



Location Data

We process your location data.

Example: We process location data when you are checked in to calculate the public transport journey you've made.

See section:
[Processed personal data](#)



Provided Data

We process personal data that you provide to us.

Example: You register in the FAIRTIQ app with your name and your email address.

See section:
[Processed personal data](#)

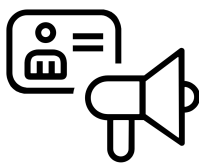


Collected Data

We process personal data that we collect about you.

Example: We collect location and movement data while you're checked in.

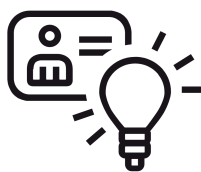
See section:
[Processed personal data](#)



Marketing

We use your personal data for marketing and advertising.

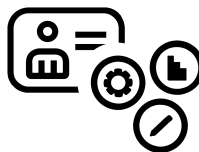
Example: We send product related marketing information to the



Product Development

We use your personal data for the development and improvement of products and services.

Example: We use the journeys calculated in anonymised or



Other Purposes

We use your personal data for other purposes without direct connection with the core service.

Example: We analyse whether the check-out is made when the



Data Transfers

We transfer your personal data to other companies that decide themselves how to use the data.

Example: If you submit a customer care request, it will be



No Data Sale

We do not sell your personal data.

email address
you have
registered.

pseudonymised
form to minimise
errors in the
journey
calculation.

means of
transport is in
motion to detect
possible
fraudulent
activities.

managed by the
public transport
operators that are
in partnership
with us.

See section:

[Processing
purposes and
modalities](#)

See section:

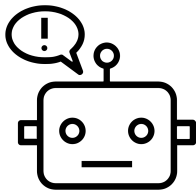
[Processing
purposes and
modalities](#)

See section:

[Processing
purposes and
modalities](#)

See section:

[Data Transfer](#)



**Automated
Decision-Making**

We make
decisions based
on fully
automated
processing.

Example: The
journey mapping
and parts of the
customer care
and fraud
detection
processes are
automated.

See section:

[Automated
decision-making
and profiling](#)



Profiling

We analyse your
behaviour.

Example: We
analyse whether
you use the
application
fraudulently.

See section:

[Automated
decision-making
and profiling](#)



Worldwide

We also process
your personal
data outside of
Switzerland and
the EEA.

Example: We
generally process
and store data in
Switzerland and
the EEA. In
exceptional cases
certain data may
flow outside
Europe.

See section:

[Data processing
location](#)

B. Contact information of the Controller and the DPO

Data Controller

FAIRTIQ Ltd.
Aarbergergasse 29
3011 Bern
Switzerland
CEO: Dr. Gian-Mattia Schucan, Anne Mellano
UID: CHE-370.720.489
feedback@fairtiq.com

Data Protection Officer

FAIRTIQ Ltd.
Data Protection
Aarbergergasse 29
3011 Bern
Switzerland
app.privacy@fairtiq.com

C. Data controllership and applicable law

FAIRTIQ Ltd. («FAIRTIQ» or «we») is the operator and controller in connection with the FAIRTIQ App («application») and processes personal data in accordance with

- the Federal Act on Data Protection (FADP) if the customer obtains services from FAIRTIQ in Switzerland;
- the EU General Data Protection Regulation 2016/679 (GDPR), including the applicable data protection legislation of the EU member states, if the customer obtains services in the European Union or the European Economic Area; and
- other applicable privacy legislation, if the customer obtains services outside the European Union or Switzerland.

When purchasing tickets for fellow passengers in accordance with section III A 2 of the General Terms and Conditions, the customer acts as a controller according to Art. 5 lit. j FADP/Art. 4 para 7 GDPR and FAIRTIQ takes on the role of the processor according to Art. 5 lit. k FADP/Art. 4 para 8 GDPR.

FAIRTIQ and the partner companies / partnering tariff communities («partners») are independently responsible controllers for the provision of the services and fraud and abuse detection and prevention (see section [Data Transfer](#)). In exceptional cases, a joint controllership applies, which is indicated accordingly in the application.

D. Processed personal data

General information about the customer

- First and last name, date of birth according to the applicable tariff regulations;

- Mobile phone number;
- Email address;
- Google account profile picture (if Google login is used – not stored by FAIRTIQ; see section [Account Creation and Administration via SSO](#))
- Account identifier (if SSO is used as a login method, see section [Account Creation and Administration via SSO](#))
- Ticket settings: chosen class and discount level;
- Deposited zone subscriptions or discount authorisations (optional);
- User ID;
- IP-address and device ID;
- Information on abusive or other fraudulent behaviour;
- Interactions with customer care.

Details of fellow travellers in accordance with GTC, section III. A. 2.

- First and last name, date of birth;
- Settings for the selected / registered tickets, deposited zone subscriptions and discount authorisations.

Means of payment data

- Payment method;
- Partially anonymized payment method details.

Travel data

- Tracking (location) and activity data (based on a motion sensor, if active);
- Registered electronic tickets (ticket data);
- Bluetooth beacon signals;
- Calculated journey;
- Digital ticket control stamps.

The recording of travel data starts with opening the application and ends at the latest 5 minutes after the check-out process has been completed. The completion of the check-out process is signalled in the application.

Bluetooth signal detection is only enabled in selected regions. Further information is available at https://fairtiq.com/docs/beacon_signals.pdf.

Purchase data

- Purchased products;
- Charged amount;
- Date and time;
- Payment ID and token.

Information about the device

- Device: brand and model;
- Operating system;
- Battery level.

Usage data

Where consent is provided, additional usage data may be collected via PostHog, a product analytics tool. This includes interactions with the app interface (e.g. screen views, clicks, navigation events), technical information (e.g. truncated IP address, device type, operating system), and behavioural event logs. Data is processed in a pseudonymised manner.

E. Processing purposes and modalities

FAIRTIQ exclusively collects and processes data in connection with the application and the purchase of electronic tickets.

Personal data transferred by the customer to FAIRTIQ via the application are processed by FAIRTIQ for the following purposes:

- To **set up and manage the customer's user account**.
- To **provide electronic ticketing applications**, in particular the purchase and processing of electronic tickets, the identification and payment of decisive rides, including customer coupons (e.g., FAIRTIQ bonus), for customer service (help desk) and functions serving to support the check-out process.
- To combat **abuses** (prevention from and investigation of unlawfully obtained services and behaviour that violates the terms of use). For this purpose, data of alleged abusive customers in Switzerland is checked and compared across all check-in/out solutions operated by FAIRTIQ and entered in a registry. A delayed cease of the activity and location data collection (see above, section [Processed personal data](#)) serves combating abuse and the continuous improvement of the functions used to support the check-out process, thus optimising the services provided by FAIRTIQ to the customer. The completion of the check-out process is signalled in the application.
- To **capture the nearest public transport** stop before check-in, location data and Bluetooth signals are collected when the application is active in the foreground of the device display. This data is stored in temporary log files.
- For the **provision of discounted rides**, i.e. the generation of an individual code for a free/discounted journey of a new customer.
In specific cases, FAIRTIQ processes special categories of personal data, namely health-related information, for the sole purpose of issuing discounted tickets to persons with a recognised disability, where such discounts are provided for under the applicable fare regulations. This data is only processed if the user actively selects the corresponding ticket category within the application settings.
- For the **further development of the application and the services**. In particular, FAIRTIQ may use the location and activity data in pseudonymised form for 12 months (see section [Data retention period](#)) in order to further develop the application. The data collected after the check-out process (see section [Processed personal data](#) → Travel data) is only processed in anonymized form for this purpose.

- To **analyse and understand user behaviour and app usage patterns** in order to improve application usability, navigation, and functionality. This includes collecting aggregated usage and interaction data through the analytics tool PostHog, where consent has been provided by the user.
- For the means of **communication with the customer and commercial purposes** (promotion among existing customers).
- To ensure the **security and stability of our system** and to prevent spam.
- For **auditing / due diligence purposes**.
- In relation to **legal proceedings and requirements**.
- For **research purposes (academia)**, in particular for non-personal scientific research purposes (see section [Data transfer](#)).

The customer has the right to object to the use of personal data for the purposes of optimising the application and the services or evaluating its use. FAIRTIQ strongly advises sending the request directly via the application (menu item 'Contact → Others') and adding the keyword 'DSR' to the message.

In the case of requests via email (feedback@fairtiq.com) or contact form (<https://fairtiq.ch/en/contact>), the processing of the request is subject to the unambiguous identification of the customer by means of an SMS validation code (identification process initiated by FAIRTIQ). Fellow travellers are encouraged to inform FAIRTIQ of any request via the customer in order to enable identification.

F. Legal basis

This section is applicable only if and to the extent that the GDPR applies.

The processing of personal data for electronic tickets and the provision of discounted travel is required to fulfil the services of FAIRTIQ (performance of a contract). Furthermore, the App needs to ensure that it is interacting with a human, not a bot, and that activities performed by the user are not related to fraud or abuse, which serves the performance of the contract. In addition, processing for the purpose of CAPTCHA may also be based on legitimate interest: protecting the service from abusive automated crawling, spam, and other forms of abuse that can harm FAIRTIQ's service or other users of our service. The further development of the service and the utilisation analysis are in the legitimate interest of FAIRTIQ and serve the optimisation of the user experience and the dissemination of the application. The provision of data to academia is in the public interest with regard to the data processing by academic institutions. Fraud detection and prevention is in the legitimate interest of FAIRTIQ. Communication with the customer serves to support the customer's use, to inform the customer about services in relation to the application and to improve the offer and serves the performance of a contract and/or is in the legitimate interest of FAIRTIQ. Sending newsletters and the related processing of data are based on the customer's consent or on

legitimate interest. Consent can be withdrawn at any time via the Application menu without any adverse consequences.

FAIRTIQ is subject to a variety of legal obligations. Primarily, these are legal requirements (e.g. commercial and tax laws, regulations), but also regulatory or other official requirements where applicable. The purposes of processing may include identity and age verification, fraud and money laundering prevention, the prevention, combating and investigation of terrorist financing and criminal offences endangering assets, the fulfilment of control and reporting obligations under tax law, as well as the archiving of data for the purposes of data protection and data security as well as auditing by tax and other authorities. In addition, the disclosure of personal data may become necessary in the context of official/court measures for the purposes of gathering evidence, criminal prosecution or the enforcement of civil law claims.

The storage and use of tracking and activity data for a period of up to five years to improve FAIRTIQ's systems, including the training of models to optimise performance, is based on the customer's explicit consent. This also applies to the collection and analysis of app interaction data in pseudonymised form using the analytics tool PostHog, with the aim of enhancing the app's usability, navigation, and functionality. Consent may be withdrawn at any time via the app menu without any adverse consequences for the customer. Withdrawal of consent does not affect the lawfulness of processing carried out prior to withdrawal.

The legal basis for the processing of personal data of customers within the European Union is Art. 6 para. 1 lit. a, b, c, e, f GDPR. The processing of special category data is further based on Art. 9(2)(c) GDPR.

G. Automated decision-making and profiling

Automated decision-making processes and profiling mechanisms are used:

- To calculate/map the public transport journey and for detecting journey sections outside of public transport, based on tracking and activity data according to section [Processed personal data](#);
- To detect and prevent fraudulent behaviour. Examples:
 - The system checks whether the means of transport is in motion when check-in and check-out are performed to ensure that the complete journey is recorded and charged. If the system detects incorrect behaviour multiple times, the account is automatically blocked;
 - If a past journey cannot be charged to the deposited means of payment, the check-in will automatically be blocked until the journey can be charged;
- In the context of customer service, to answer standard enquiries promptly. The system generates the answers based on the content of the customer service enquiries.

Affected persons have the right

- to request the intervention of a natural person in the decision-making process;

- to express their own point of view;
- to have the decision reviewed or challenged outside of the legal process.

FAIRTIQ strongly advises sending the request directly via the application (menu item 'Contact → Others') and adding the keyword 'DSR' to the message.

In the case of requests via email (feedback@fairtiq.com) or contact form (<https://fairtiq.ch/en/contact>), the processing of the request is subject to the unambiguous identification of the customer by means of an SMS validation code (identification process initiated by FAIRTIQ).

H. Security

FAIRTIQ protects personal data against foreseeable risks and unauthorised access with suitable technical and organisational measures. FAIRTIQ minimises the use of personal data.

For security reasons, the data for the means of payment are stored only at the service provider of the payment service and not on the mobile phone of the customer. Furthermore, the registration of the means of payment takes place directly with the contractual payment partner of FAIRTIQ without the intervention of FAIRTIQ.

I. Data Transfer

To **our affiliates**, based on our instructions and in compliance with our Privacy Notice and any other appropriate confidentiality and security measures, including but not limited to our offices in Germany, Austria, Portugal, and Singapore.

To our **service providers**: Subprocessors commissioned by FAIRTIQ for the tasks specified in section [Processing purposes and modalities](#) process the personal data of the customers (including storage). FAIRTIQ has entered into data processing agreements with these service providers to ensure the protection of personal data. A list of subprocessors is available at https://fairtiq.com/docs/subprocessor_list.pdf

To **legal and professional advisors**, including accountants and auditors.

To **payment providers**: Information about the mode of payment is not recorded on the mobile phone, in the application, with FAIRTIQ or any partner association (see section [Processed personal data](#) for exceptions). The registration of the means of payment in connection with the application is directly arranged by the payment provider (Datatrans AG / Planet – protel Hotelsoftware GmbH), Stadelhoferstrasse 33, 8001 Zurich, Switzerland, info@datatrans.ch and Adyen N.V., Simon Carmiggeltstraat 6-50, 1011 DJ Amsterdam, the Netherlands, dpo@adyen.com. Further information on data processing by Adyen is available at <https://www.adyen.com/policies-and-disclaimer/privacy-policy>

To **NOVA**: If the application is used to purchase a ticket within the GA travelcard validity area (Switzerland, Liechtenstein and the border belt) and the Swisspass / Swisspass ID is registered in the application, the calculated travel route including timestamps will be

forwarded to the public transport sales and distribution platform NOVA in personalised form (using Swisspass ID, which enables a link to purchases via other digital public transport sales platforms). NOVA is operated by Swiss Federal Railways SBB on behalf of Alliance Swisspass. SBB may use the clients' personal data for its own purposes (e.g. to combat misuse).

Information on the processing of personal data by SBB can be found at

<https://www.sbb.ch/en/meta/legallines/data-protection.html>.

FAIRTIQ and SBB AG, Hilfikerstr. 1, 3000 Bern 65, Switzerland act as independent controllers within the meaning of Art. 5 lit. j FADP / Art. 4 para. 7 GDPR. FAIRTIQ has no influence on and bears no responsibility for data processing by SBB.

To **Google** or **Apple** in case of using SSO (see section [Account Creation and Administration via SSO](#))

To **Google Pay** and **Apple Pay**: On the application, the option to pay with Google Pay or Apple Pay is offered depending on the region of use. This is performed via the payment provider Adyen.

For the purpose of payment processing, the customer deposits the required payment data with Google Pay or Apple Pay. FAIRTIQ only stores an ID created by the payment provider and a token to process future payments.

The provision of the payment data is necessary and mandatory for the conclusion or execution of the contract. If the payment data is not provided, a conclusion of the contract and / or the execution by means of Google Pay or Apple Pay is impossible. The data required for payment processing are transmitted securely via the "SSL" procedure and processed exclusively for payment processing.

The data accruing in this context will be deleted after the storage is no longer necessary or the processing will be restricted if there are legal obligations to retain data. FAIRTIQ is obliged to store the payment and order data for a period of up to ten years due to mandatory commercial and tax regulations.

When using Google Pay or Apple Pay, data may also be processed in the USA. In the opinion of the European Court of Justice, there is currently no adequate level of protection for data transfers to the USA. A transfer may therefore be associated with various risks for the legality and security of the data processing.

Further information on data processing by Apple Pay is available at

<https://support.apple.com/en-ie/HT203027>

Further information on data processing by Google Pay is available at

https://payments.google.com/payments/apis-secure/get_legal_document?ldo=0&ldt=pri_vacynotice&ldl=en

To the **CAPTCHA security service** integrated in the App (hereinafter "hCaptcha"): This service is provided by Intuition Machines, Inc., a Delaware US Corporation ("IMI"). hCaptcha is used to verify whether user actions on our online service (such as login or registration attempts) meet the security requirements.

To this end, hCaptcha automatically analyzes the user's behavior as soon as the registration process is initiated in the app. The analysis is based on various factors, such as IP address, device information, and session duration. This analysis may occur in "invisible mode", meaning it can be carried out entirely in the background without notifying the user, unless a manual verification is triggered.

The data collected through this process is transmitted to IMI, which acts as a data processor on behalf of FAIRTIQ. For more information about hCaptcha's privacy policy and terms of use, please visit the following links: <https://www.hcaptcha.com/privacy> and <https://www.hcaptcha.com/terms>

To **Analytics provider – PostHog Cloud**: Data is processed within the EEA on infrastructure operated by PostHog or its authorised subprocessors. PostHog acts as a data processor on behalf of FAIRTIQ. More information about PostHog's privacy practices is available at: <https://posthog.com/docs/privacy>

To **partners**: FAIRTIQ forwards the required personal data to the allied transportation company / tariff community to fulfil the customer care, to combat abuse, and to communicate with customers (see the 'Partner Companies' on fairtiq.com). In this context, the relevant partner companies are independently responsible for the personal data processing.

FAIRTIQ forwards ticket data to partners for the purpose of payment and accounting. Furthermore, FAIRTIQ forwards location data in an anonymised form to partners for improving their products and their public transport offer, for the partially personalised communication of information and offers as well as for further statistical evaluation purposes.

Information in accordance with art. 13 para 1 & 2 GDPR related to the processing of personal data by partners, in case of a transfer to partners acting as independent controllers, is available on the partners' @website. A list of partners per region is available at https://fairtiq.com/docs/fairtiq_Privacy_principles_annex_1.pdf

If the application is used for ticket purchase within the GA travelcard validity area (Switzerland, Liechtenstein and the border belt): To **app operators who have integrated a check-in/out solution operated by us into their app** if there is any indication of abusive behavior by the customer: in this case, the data necessary to identify and block the customer in the corresponding app and the reason for blocking is shared with the app operators.

To **competent authorities**, including supervisory, tax, debt collection and bankruptcy authorities, courts, arbitral tribunals or bar associations (if it is necessary to provide our services, if we are legally obliged or entitled to such disclosure or if it appears necessary to protect our interests).

To **transaction partners** and advisors (e.g. in relation to mergers, acquisitions or other business transactions involving us or our affiliates).

For **research purposes (academia)**: FAIRTIQ is entitled to disclose pseudonymised personal data to universities from Switzerland, the EU or the EEA for non-personal scientific research purposes under the following conditions:

- A. FAIRTIQ shall take measures to prevent the identifiability of the data subjects by pseudonymization.
- B. The results of the research may only be published or otherwise passed on if no conclusions can be drawn about the data subjects.

The customer has the right to object against the disclosure of their data for research purposes at any time and without any disadvantage (please consult section [Right of Objection](#) for further information).

J. Account Creation and Administration via SSO

Registration and creation of a user account with personal data is a precondition for using the application. As an alternative to registration or login using an e-mail address and password, the following single sign-on services can be used:

Registration with Google (Google Sign-in):

The application offers the option to register with the customer's existing Google profile data. For this purpose, Google Sign-In is used – a service provided by Google Ireland Limited ('Google'), Gordon House, Barrow Street, Dublin 4, Ireland.

If the customer uses this feature, they will first be directed to a Google form integrated into the application and asked to sign in with their Google account credentials. This links the Google Account to our service. FAIRTIQ receives the following information when Google Sign-in is used:

- Account identifier
- First and last name;
- Email address;
- Profile Picture (which we do not store).

FAIRTIQ does not transmit any personal data of the customer from the customer account of the application to Google within this context. FAIRTIQ has no influence on the scope and further use of data collected by Google through the use of Google Sign-In. Google may be aware that the Google Sign-in has been used to create an account or log in to the customer account in the application.

Further information can be found in the terms of use and privacy policy of Google (<https://business.safety.google/privacy/>).

Registration with Apple (Sign in with Apple):

The application offers the option to register with the customer's existing Apple user profile data. For this purpose, "Sign in with Apple" is used – a service provided by Apple Inc., One Apple Park Way, Cupertino, CA 95014, USA.

If the customer uses this feature, they will first be redirected to an Apple form integrated into the application and asked to sign in with their username and password. When first signing up, Apple will only provide the following information to FAIRTIQ:

- Account identifier
- First and last name (voluntary information);
- E-mail address

FAIRTIQ does not transmit any personal data of the customer from the customer account to Apple within this context. FAIRTIQ has no influence on the scope and further use of data collected by Apple through the use of Sign in with Apple. Apple may be aware that the Apple login has been used to create an account or log in to the customer account in the application.

For more information, please see the Apple terms of use and privacy policy (<https://www.apple.com/legal/privacy/>).

K. Customer contact

FAIRTIQ is entitled to contact the customer concerning topics affecting FAIRTIQ. This includes:

- Information in connection with the offer or about its amendment
- Information to help customers use the app
- Surveys on the use of FAIRTIQ and mobility in general. Participation in surveys is voluntary.

If the customer has given consent, FAIRTIQ is allowed to contact the customer concerning further offers and information not necessarily related to FAIRTIQ. The customer can revoke the consent at any time.

Depending on the type of contact, the messages may contain tracking pixels that enable a log file recording for the statistical evaluation of the contact. FAIRTIQ can see if and when a message has been opened and which links in the message have been activated.

The customer can unsubscribe from being contacted by writing FAIRTIQ at app.privacy@fairtiq.com or following the unsubscription link or the instructions in each message that FAIRTIQ sends to the customer.

L. Data retention period

FAIRTIQ retains personal data only as long as it is required for the purposes for which it was collected or in accordance with legal and official regulations or contractual agreements.

The travel, purchase and means of payment data and the information about the device in accordance with Section [Processed personal data](#) shall be retained **for 12 months** after the end of the journey for fulfilling the services, for after-sales services of FAIRTIQ and the partner transportation companies and tariff communities, for the purpose of combating abuse and for improving the services, in particular the price optimisation. Subsequently, deletion/anonymisation of this data is performed and the connection to a data subject is no longer possible. With the aim of data minimisation, part of the tracking data may be deleted

before this period expires provided the purposes for which it was collected have been fulfilled.

The general information about the customer and details of fellow travellers shall be retained for the purpose of combating abuse, for the means of communication with the customer and for commercial purposes **for two years** from the last journey or from joining a campaign (depending on what occurs later).

Change and deletion logs of personal data are retained for two years.

The data can also be saved in backup files and temporary databases (caches) after deletion. The final deletion takes place when the backup files are overwritten (typically within days).

M. Exceptions to the time limits according to section L

Location data collected to capture the nearest public transport stop before check-in shall be retained in temporary files for a few days.

Data which is relevant under tax law and for accounting purposes of FAIRTIQ or the partner companies shall be retained by FAIRTIQ and/or the partner companies in accordance with the legally prescribed retention periods (usually 10 years plus duration of the current accounting year) and subsequently deleted.

If the customer has been excluded from using FAIRTIQ due to a justified suspicion of misuse, FAIRTIQ has the right to store the personal data in accordance with section [Processed personal data](#) in order to prevent repeated misuse and to enforce their legal claims, including the date and reason for the exclusion, even against the customer's deletion request until the rights have been exercised or the limitation period has expired. If the exclusion is reversed (e.g., because the suspicion of abuse turns out to be unfounded), the retention period of 12 months until the anonymisation of the travel data starts anew.

In the case of outstanding invoices, FAIRTIQ has the right to retain personal data according to section [Processed personal data](#) until the invoice and any additional claims have been fully settled or the limitation period has expired.

If the customer does not purchase a ticket with the application during the period of one year at a time, FAIRTIQ has the right to delete the customers' user account. The customer must then repeat the registration process before they can use FAIRTIQ to purchase electronic tickets again. With the deletion of the user account, they also lose access to their travel and payment history with FAIRTIQ.

If the customer does not purchase a ticket with the application within four months, FAIRTIQ has the right to delete the customer's payment method data. The customer must then repeat the registration of a valid means of payment before being able to purchase electronic tickets with FAIRTIQ again.

If consent is provided by the customer, tracking and activity data is retained for up to five years to improve our system, including training models for better performance. Consent can

be withdrawn at any time via the Application menu. Withdrawal does not affect processing already carried out.

N. Right to erasure and to be forgotten

Subject to the foregoing storage provision and if FAIRTIQ or a partner company does not require the data to safeguard and exercise their rights, provided that the data is no longer necessary for the purposes for which it was collected or otherwise processed, or provided that there are no overriding legitimate grounds for processing, the customer has the right to request the deletion of their personal data at any time.

FAIRTIQ strongly advises sending the request directly via the application (menu item 'Contact → Account deletion') adding the keyword 'DSR' to the message.

With the request for deletion, the customer expressly waives the right to use customer service with regard to past trips and to complain about any trips affected by the request.

In the case of deletion requests via email (feedback@fairtiq.com) or contact form (<https://fairtiq.ch/en/contact>), the deletion is subject to the unambiguous identification of the customer by means of an SMS validation code (identification process initiated by FAIRTIQ).

Deletion requests for fellow passengers' personal data shall be submitted by the customer to enable the identification of the fellow passengers.

O. Correction and limitation

The customer has the right to correct and limit the data stored for the respective customer account, if the data is faulty or a limitation does not affect the processing purposes. The customer can adjust the general account information according to section [Processed personal data](#) directly in the app.

Modifications are not possible during an ongoing journey.

P. Information and transmission rights

The customer and fellow passengers have the right to request information about the data stored on the customer's account and its transmission.

FAIRTIQ strongly advises sending the request directly via the application (menu item 'Contact → Others') and adding the keyword 'DSR' to the message.

In the case of deletion requests via email (feedback@fairtiq.com) or contact form (<https://fairtiq.ch/en/contact>), the processing of the request is subject to the unambiguous identification of the customer by means of an SMS validation code (identification process initiated by FAIRTIQ).

Deletion requests for fellow passengers' personal data shall be submitted by the customer to enable the identification of the fellow passengers.

Q. Right of objection

The customer has the right to object at any time to the processing of personal data concerning them for reasons arising from their particular situation, if the data processing is carried out on the basis of art. 6 para. 1 lit. f GDPR. This also applies to profiling and automated decision making based on these provisions. If the customer objects, FAIRTIQ will no longer process their personal data unless compelling legitimate grounds for the processing can be demonstrated which override the interests, rights and freedoms of the customer, or the processing serves to assert, exercise or defend legal claims.

If the customer's personal data are processed for the purpose of direct marketing, the customer shall have the right to object at any time to the processing of personal data concerning them for the purpose of such marketing; this shall also apply to profiling insofar as it is related to such direct marketing. If the customer objects, their personal data will subsequently no longer be used for the purpose of direct advertising.

FAIRTIQ strongly advises sending the request directly via the application (menu item 'Contact → Others') and adding the keyword 'DSR' to the message.

In the case of deletion requests via email (feedback@fairtiq.com) or contact form (<https://fairtiq.ch/en/contact>), the deletion is subject to the unambiguous identification of the customer by means of an SMS validation code (identification process initiated by FAIRTIQ).

Deletion requests for fellow passengers' personal data shall be submitted by the customer to enable the identification of the fellow passengers.

R. Right to lodge a complaint

Data subject rights are not absolute and may be subject to exemptions or derogations under applicable data protection laws.

The customer further has the right to lodge a complaint with the competent supervisory authority, as follows:

- in Switzerland, with Swiss Federal Data Protection and Information Commissioner (FDPIC);
- In the EU/EEA, with the [competent authority of the member state](#) relevant for the data subject.

S. Data processing location

Personal Data is processed in the EEA, Switzerland, the United Kingdom, in countries where FAIRTIQ has an affiliate (see section [Data transfer](#)) or any other country for which an adequacy decision has been issued by the European Commission respectively which are listed in Annex 1 of the Swiss Ordinance on Data Protection (in particular the USA).

If FAIRTIQ transfers data to a country without adequate data protection level, FAIRTIQ will, as provided for by law, use appropriate contracts (namely on the basis of the so-called Standard Contract Clauses of the European Commission) and appropriate or suitable safeguards (available on request via app.privacy@fairtiq.com) and / or rely on the statutory exceptions of consent, contract execution, the establishment, exercise or enforcement of legal claims, overriding public interests, published personal data or because it is necessary to protect the integrity of the persons concerned.

Details are available at https://fairtiq.com/docs/subprocessor_list.pdf

T. Data protection representation in the European Union

In case of questions or uncertainties about data protection, FAIRTIQ's data protection representation in the EU is available for interested parties at the following address. FAIRTIQ Austria GmbH, Data Protection, Straubingerstraße 12, 5020 Salzburg, Austria, app.privacy@fairtiq.com

U. Changes of this privacy notice

FAIRTIQ regularly checks this privacy notice. To be informed about the latest version, it is recommended to check it regularly via <https://fairtiq.com/en/app-privacy-policy>.

V. Accessibility and download of the privacy notice

The current version of the privacy notice can be viewed and printed at <https://fairtiq.com/en/app-privacy-policy>