FAIRTIQ APP 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 about how we are committed to respecting your privacy and protecting your personal data.

This privacy notice is for information purposes only and does not constitute a contract.

The FAIRTIQ app may support different Travel Modes depending on the area of use and availability, including journeys started and ended manually (check-in/check-out), journeys started manually and ended automatically (Smart Stop), and journeys recorded while the Be-in/Be-out mode is activated and the customer is travel ready (FAIRTIQ Go). Smart Stop and FAIRTIQ Go are collectively referred to as "Automatic Travel Modes".

In this privacy notice, references to journeys recorded with the application include all such Travel Modes. Where this privacy notice refers specifically to check-in or check-out, this applies to the Travel Modes in which such steps are required; in Automatic Travel Modes, the corresponding processing relates to the automatic detection, recording and completion of the journey.

For automatic journey detection, the application may process movement sensor data and, where available, Bluetooth beacon signals locally on the device to assess whether a public transport journey may be starting or taking place. If no public transport journey is detected, this locally processed data is deleted after a short period and is not transmitted to FAIRTIQ's backend. If a possible public transport journey is detected, location data may also be collected and the data required to record and process the journey is transmitted to the backend. Automatic journey detection may not always be fully accurate.

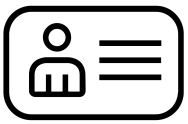
To give you a convenient overview of how we process your data, we use Privacy Icons, an initiative by leading Swiss companies to create transparency in data processing.

Table of contents

A. How we treat your data (privacy icons) 3
B. Contact information of the Controller and the DPO 4
Data Controller 4
Data Protection Officer 5
C. Data controllership and applicable law 5
D. Processed personal data 5
In particular, FAIRTIQ processes the following personal data: 5
General customer information 5
Details of fellow travellers in accordance with GTC, section III. A. 2. 6
Means of payment data 6
Travel data 6
Purchase data 7
Information about the device 7
Usage data 7
E. Processing purposes and modalities 7
Account setup and management: 7
Electronic ticketing services: 7
Abuse prevention and investigation: 8
Nearby stop and area-of-use detection detection: 8
Referral, loyalty and other discounts: 8
Discounts for recognised disabilities: 8
Product development: 9
Analytics and insights: 9
Communications: 9
Security and stability: 9
Audit and due diligence: 9
Legal proceedings and regulatory requirements: 9
Academic research: 10
F. Legal basis 10
G. Automated decision-making and profiling 12
H. Security 13
I. Data Transfer 13
J. Account Creation and Administration via SSO 16
K. Customer contact 17
L. Data retention period 18
M. Exceptions to the time limits according to section L 18
N. Right to erasure and to be forgotten 19
O. Correction and limitation 20
P. Information and transmission rights 20
Q. Right of objection 21
R. Right to lodge a complaint 21
S. Data processing location 21
T. Data protection representation in the European Union 22
U. Changes to this privacy notice 22
V. Accessibility and download of the privacy notice 22

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 service, i.e. to provide the correct travel authorisation or ticket and to calculate the applicable fare.



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

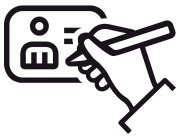


Location Data

We process your location data.

Example: We process location data 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

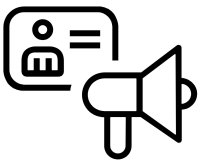


Collected Data

We process personal data that we collect about you.

Example: We process movement sensor data, Bluetooth beacon signals and location data to detect and calculate journeys with the application.

See section: Processed personal data



Marketing

We use your personal data for marketing and advertising.

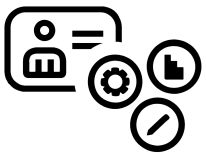
Example: We send product



Product Development

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

Example: We use the journeys



Other Purposes

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

Example: We analyse whether



Data Transfers

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

Example: If you submit a



No Data Sale

We do not sell your personal data.

related marketing information to the email address you have registered.

calculated in anonymised or pseudonymised form to minimise errors in the journey calculation.

the check-out is made when the means of transport is in motion to detect possible fraudulent activities.

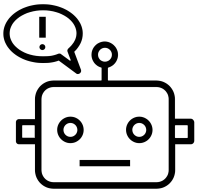
customer care request, it will be managed by the public transport operators that are in partnership with us.

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 or whether an attempted use is linked to previous misuse, outstanding claims or a blocked account

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
CEOs: 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 and EEA 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 EU, EEA 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 (7) GDPR and FAIRTIQ takes on the role of the processor according to Art. 5 lit. k FADP/Art. 4 (8) GDPR.

FAIRTIQ and the partner companies / partnering tariff communities (“partners”) act as 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

In particular, FAIRTIQ processes the following personal data:

General customer information

- First and last name, date of birth according to the applicable tariff regulations;
- Mobile phone number;
- Email address;
- Language, based on the operating system settings of the device;
- 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;
- Tariff region assigned during registration;
- Deposited zone subscriptions or discount authorisations (optional);
- User ID;
- IP address and device ID;
- Technical security identifiers and device-related risk status values, including Apple DeviceCheck information where applicable;
- Information on abusive, fraudulent or otherwise improper behaviour, including related blocking or usage restrictions;
- Interactions with customer care;
- Security- and compliance-related logs, such as consent, change and deletion logs.

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 anonymised payment method details.

Travel data

- Tracking (location) and activity data including movement sensor data where required for the selected Travel Mode;
- Travel authorisations, control proofs and registered electronic tickets, including ticket data;
- Bluetooth beacon signals;
- Calculated journey;
- Digital ticket control stamps;
- Journey-based statistics, to the extent they relate to the customer.

To determine the nearest public transport stop before the activation of any Travel Mode, location data and Bluetooth signals are collected when the application is active in the foreground of the device display.

In Automatic Travel Modes, Bluetooth beacon signals from stops or vehicles may also be used, together with movement sensor data, to support the local on-device assessment of whether a public transport journey may be starting or taking place.

Movement sensor data used only for local on-device assessment are not transmitted to FAIRTIQ's backend if no public transport journey is detected and are deleted after a short period.

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;
- Information on failed charges, outstanding amounts and claims status;
- Date and time;
- Payment ID and token.

Information about the device

- Device: brand and model;
- Operating system;
- Battery level;
- Further technical device and application information, including device configuration data and derived device signals, used to verify application integrity, prevent abuse and recognise repeated abusive use across accounts.

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

Personal data are processed by FAIRTIQ for the following purposes:

Account setup and management:

- To create and manage the customer's user account, including language settings and the assignment of a region.

Electronic ticketing services:

- To provide the application's ticketing functions, including the provision of travel authorisations, the purchase and processing of electronic tickets and the calculation of applicable fares;
- to identify, record and charge chargeable public transport journeys;
- to support Automatic Travel Modes, including automatic journey detection, check-out support and journey completion;
- to handle customer coupons (e.g., the FAIRTIQ bonus);
- for customer service (help desk), debugging and troubleshooting;

Abuse prevention and investigation:

- To prevent, detect and investigate abuse, including fraud, fare evasion, breaches of the terms of use, failed charges, outstanding claims and repeated misconduct, as well as to verify the reliability and trustworthiness of data received from the device.

  For this purpose, data relating to suspected or confirmed abuse, failed payments, outstanding amounts and usage restrictions may be checked, matched across all FAIRTIQ-operated in /out ticketing solutions and Travel Modes and recorded in an abuse prevention register. FAIRTIQ may use such information to prevent users who have been restricted or excluded due to abuse, journeys that could not be charged, outstanding claims or other significant misconduct from repeating such behaviour by creating further accounts or by using the same or comparable devices again.

  For this purpose, technical security identifiers, device information, Apple DeviceCheck status values or risk indicators derived from them may be matched with account, payment, journey and abuse-related information. Apple DeviceCheck or comparable technical security features are not used as the sole basis for determining fraudulent behaviour, but only in combination with further information, such as account, payment, usage, journey or customer care information. Depending on the outcome, FAIRTIQ may require additional checks, prevent account creation or check-in, block or restrict an existing account, or review and enforce outstanding claims.
- Collection of activity and location data may continue for five minutes after check-out, deactivation of FAIRTIQ Go or completion of the journey in the respective Travel Mode (see section *Processed personal data*) to combat abuse and to improve the check-out support, deactivation or journey end, and optimisethe services provided to the customer.

Nearby stop and area-of-use detection detection:

- To determine the nearest public transport stop or the applicable area of use before check-in or activation of a Travel Mode, location data and, where available, Bluetooth beacon signals are collected when the application is active in the foreground of the device display. This data may be stored in temporary log files.

Referral, loyalty and other discounts:

- To provide discounts, rewards and other promotional benefits, for example through referral programmes, loyalty schemes, or free or discounted journey offers.

Discounts for recognised disabilities:

- In specific cases, FAIRTIQ processes health-related information solely for issuing discounted tickets to persons with a recognised disability, where such discounts are provided under the applicable fare regulations. This data is processed only if the customer actively selects the corresponding ticket category within the application settings.

Product development:

- If the customer has given consent, travel data (see *Processed personal data* → *Travel data*) is used for a period of up to five years for the further development and improvement of FAIRTIQ's front- and backend, including the training of machine learning models to optimise the performance;
- data collected after the check-out process (see *Processed personal data* → *Travel data*) is used for this purpose only in anonymised form.

Analytics and insights:

- To analyse and understand user behaviour, app usage patterns and consumption behaviour in order to assess and improve application usability, navigation, and functionality. This may include statistics based on journeys made with the application.
- Where consent has been provided by the customer, this includes collecting aggregated usage and interaction data through the analytics tool PostHog and, where applicable, the sharing of results of the analysis of public transport journeys and spending in personalised form to third parties.

Communications:

- To communicate with the customer and for commercial purposes, in particular service communications about the customer's account and use of the application, promotion of services to existing customers, surveys concerning the use of FAIRTIQ and mobility in general, and for requesting consent for further purposes.
- This may include the use of information related to the customer's past use of the application, such as regions travelled in, frequency of use, or whether certain mobility services have been used, in order to tailor communications and provide relevant information.
- This may also include checking whether electronic communications have been delivered and/or opened.

Security and stability:

- To ensure the security and stability of our systems and to prevent spam.

Audit and due diligence:

- For audit and due-diligence purposes.

Legal proceedings and regulatory requirements:

- In connection with legal proceedings, legal requests and regulatory requirements.

Academic research:

- In particular, for non-personal scientific research purposes in collaboration with academic institutions (see section *Data transfers*).

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 and loyalty programmes, including de-bugging and troubleshooting, is required to fulfil the services of FAIRTIQ (performance of a contract). Furthermore, the application needs to ensure that it is interacting with a human, not a bot, and that activities performed by the customer are not related to fraud or abuse, which serves the performance of the contract.

The processing of location data and, where available, Bluetooth beacon signals while the application is active in the foreground before check-in or activation of a Travel Mode is necessary to determine the nearest public transport stop or applicable area of use and is based on the performance of a contract or pre-contractual steps requested by the customer.

Where an Automatic Travel Mode is activated or used, the processing of movement sensor data and, where available, Bluetooth beacon signals on the device for automatic journey detection, and the subsequent processing of location data and journey data once a possible public transport journey has been detected, is necessary to provide the selected ticketing service and is therefore based on the performance of a contract. To the extent that such data is processed for abuse prevention, security, product improvement, analytics or legal purposes, the legal bases set out in this section apply accordingly.

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 carried out in the legitimate interest of FAIRTIQ and serve to optimise the user experience and promote the application. To the extent that Travel Data is processed for the further development and improvement of the service, such processing is based on the customer's consent.

The provision of data to academia is in the public interest with regard to the data processing by academic institutions.

Fraud detection and prevention includes the legitimate interest of FAIRTIQ and its partners in preventing abusive or fraudulent use of the application, repeated misconduct, unpaid journeys, payment defaults and further journeys that cannot be charged, as well as in asserting, exercising or defending legal claims. Where FAIRTIQ uses Apple DeviceCheck or comparable technical security mechanisms for these purposes, the processing is based on legitimate interest. Where the processing is necessary for the provision, processing or charging of journeys, or for reviewing and collecting outstanding amounts, it may additionally be based on the performance of a contract. Statutory retention and documentation obligations may also require the processing of certain data.

Communication with the customer serves to support the customer's use of the application, to provide service-related information, to improve the offer and, where applicable, to communicate marketing or other information. Processing for service-related communications is based on the performance of a contract and/or on FAIRTIQ's legitimate interest. Processing for existing-customer marketing is based on legitimate interest, unless consent is required. Newsletters and similar consent-based communications, including the related processing of data, are based on the customer's consent. Consent can be withdrawn at any time via the link provided in the email or via the application menu without any adverse consequences.

The processing of language, region and communication-related log data follows the legal basis of the respective processing purpose, in particular the performance of a contract, legitimate interest or consent where required. This also applies to delivery, opening and interaction data collected through tracking pixels or similar technologies in electronic communications. Where applicable law requires consent for such technologies, FAIRTIQ uses them only on the basis of consent.

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 and to the transfer of consumption and usage data and related analysis to partners. Consent may be withdrawn at any time via the application 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 (1) (a), (b), (c), (e), and (f) GDPR. The processing of special category data for disability-related discounts is based on the customer's explicit consent under Art. 9(2)(a) GDPR, unless another applicable legal basis applies under the relevant fare regulations or local law.

G. Automated decision-making and profiling

Automated processing, including profiling, is used in the following cases:

- **For journey calculation and mapping:** To calculate and map public transport journeys and, where Automatic Travel Modes are used, to assess locally on the device whether a public transport journey may be starting or taking place and to detect the start and end of journeys, based on tracking, movement, Bluetooth beacon and activity data as described in the section Processed personal data;
- **For loyalty programmes, discounts and rewards:** To administer loyalty benefits and other promotional advantages, for example by determining eligibility and calculating discounted fares, free journeys or other rewards based on the number, frequency or volume of journeys taken.
- **For fraud detection and prevention:** Examples:
    - The system checks whether the means of transport is in motion when check-in, check-out, activation or deactivation of a Travel Mode is performed, or when travel-ready status is assessed, 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 stored payment method, check-in may be automatically blocked until the outstanding amount has been settled;
- **For customer service:** To respond promptly to enquiries. In such cases the system generates responses based on the content of the customer service enquiry.

Automatic journey detection is based on technical signals and probability-based assessments and may not always be fully accurate. Customers may therefore be asked to confirm, correct or report journeys in the application or through customer support.

Where required by applicable law, in particular where a decision is based solely on automated processing, including profiling, and produces legal effects concerning the

affected person, or similarly significantly affects them, or otherwise results in a significant disadvantage, the affected person has the right to request human intervention, to express their point of view and to contest the decision.

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** who support FAIRTIQ in **the context of** legal and contractual **obligations and questions**, 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 for a journey that includes at least one section within the validity area of "Automatic Ticketing", 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). This applies regardless of whether the journey starts or ends outside Switzerland or outside the GA travelcard validity area. NOVA is operated by Swiss Federal Railways SBB on behalf of Alliance SwissPass. SBB may use the customers' 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 (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.

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=privacynotice&ldl=en

To **Apple** in connection with Apple DeviceCheck: Where the application is used on an iOS device, FAIRTIQ may use Apple DeviceCheck to prevent abuse, repeated misconduct, renewed account creation after blocking or exclusion, and further journeys that cannot be

charged. In this context, the application generates a DeviceCheck token, which is transmitted by our server to Apple in order to query or update a device-related DeviceCheck status. Apple stores and processes device-related DeviceCheck status values on Apple servers. FAIRTIQ determines what these status values mean for its abuse prevention checks.

FAIRTIQ does not use Apple DeviceCheck status values as the sole indicator of fraudulent behaviour, but only together with further information. DeviceCheck tokens are not shared with third parties, except with service providers acting on behalf of FAIRTIQ where this is necessary for operating the security function. Further information on Apple's processing of personal data is available in Apple's Privacy Policy at https://www.apple.com/legal/privacy/en-ww/.

To the **CAPTCHA security service** integrated in the application (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 analyses the customer's behaviour 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 customer, 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 the **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 provide customer care, to combat abuse, for bookkeeping purposes 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 transfers the data required for ticketing, travel authorisations, payment and accounting to partners for the purpose of payment and accounting. Furthermore, FAIRTIQ forwards public transport journey data in an anonymised form to partners for improving their products and their public transport offer and for statistical evaluation purposes. If consent is provided by the customer, this data may be transferred in personalised form for personalised communication of information and offers as well as the analysis of consumption and usage behaviour.

Information in accordance with Art. 13 (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 respective partner's website. A list of partners per region is available at https://fairtiq.com/docs/fairtiq_Privacy_principles_annex_1.pdf

To **app operators who have integrated a FAIRTIQ-operated ticketing solution into their app** if there is any indication of abusive behaviour 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 pseudonymisation.
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 email 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);
- Email 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 and content of the communication, messages may contain tracking pixels or similar technologies. FAIRTIQ may use them to determine whether a message has been delivered or opened and, where applicable, which links have been activated. This may apply to service-related communications, existing-customer marketing, newsletters and similar communications, in each case where permitted by applicable law or where consent has been obtained if required.

The customer can unsubscribe from being contacted by writing to FAIRTIQ at app.privacy@fairtiq.com or following the unsubscribe 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 **up to 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. 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.

Movement sensor data and Bluetooth signals processed only locally on the device for automatic journey detection with FAIRTIQ Go are **deleted after a few minutes** if no public transport journey is detected and are not transmitted to FAIRTIQ's backend.

The general customer information 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 **up to two years** from the last journey or from joining a campaign (depending on what occurs later).

Security- and compliance-related logs, such as consent, change and deletion logs, are retained for **as long as required to document and manage security and compliance settings**, requests and obligations.

Travel data processed for product improvement and development based on the customer's consent is retained for **up to five years.**

Aggregated usage and interaction data processed for analytics **and insights** purposes **based on the customer's consent is retained for up to three years.**

In general, data may be stored 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 and, where applicable, Bluetooth beacon signals collected to capture the nearest public transport stop before check-in or activation of a Travel Mode 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, or if the customer's use of FAIRTIQ has been restricted, for example because of a justified suspicion of misuse, repeated misconduct, failed charges or outstanding claims, FAIRTIQ has the right to retain the personal data required for preventing repeated misuse, further journeys that cannot be charged, and for establishing, exercising or defending its legal claims. This may include the personal data listed in section Processed personal data, the date and reason for the exclusion or restriction, technical security identifiers, Apple DeviceCheck status values or risk indicators derived from them, as well as information on outstanding claims, even against the customer's deletion request. Such data is retained only for as long as necessary for these purposes. If the exclusion or restriction is reversed, for example because the suspicion of abuse turns out to be unfounded or because outstanding claims have been settled, the corresponding security and risk status values will be reviewed, adjusted or deleted and the retention period of 12 months until the anonymisation of the travel data starts anew, unless overriding legitimate grounds or statutory retention obligations require further retention.

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, activity and data derived from it are 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.

If the customer requests deletion of data relating to past trips, FAIRTIQ may no longer be able to provide customer service or process complaints relating to those trips.

In the case of requests sent 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 inaccurate or a limitation does not affect the processing purposes. The customer can adjust the general account information according to the section Processed personal data directly in the app.

If a data subject believes that a blocking, usage restriction, technical security status or Apple DeviceCheck-related status is incorrect, for example because a device has been transferred, sold or used by another person, they may request a review, correction, restriction or, where applicable, reset of the relevant status. FAIRTIQ reviews such requests taking into account the available account, payment, journey, customer care and abuse-related information. Correction, deletion or reset will be carried out where no overriding legitimate grounds, outstanding claims or statutory retention obligations prevent it.

User account 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 requests sent 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).

Requests concerning 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(1)(e) or (f) GDPR.

This also applies to automated decision making and profiling 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 requests sent 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.

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 the 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;
- In the UK, with the Information Commissioner's Office.

S. Data processing location

Personal Data are 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 or that are listed in Annex 1 of the Swiss Ordinance on Data Protection (in particular the USA).

When Apple DeviceCheck is used, DeviceCheck tokens and device-related DeviceCheck status values may be transmitted to Apple and processed on Apple servers. Apple may process or make personal data accessible globally, including in Ireland and the United States. For individuals in the European Economic Area, the United Kingdom and Switzerland, Apple identifies Apple Distribution International Limited, Ireland, as the Apple entity controlling personal data where Apple acts as controller. According to Apple, international transfers of personal data are governed in particular by Standard Contractual Clauses or other appropriate safeguards.

If FAIRTIQ transfers data to a country without an adequate level of data protection, FAIRTIQ will, as provided for by law, use appropriate contracts (namely on the basis of the so-called Standard Contractual 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 to this privacy notice

FAIRTIQ regularly reviews 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

Version 5.3. Last updated in November 2026