

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 respect your privacy and protect your personal data.

Table of contents

A. Contact information of the Controller and the DPO	2
Controllership depends on the processing purpose:	2
Data controller for core functionalities (accurate journey capture, ticket purchase/fulfilment, settlement, fraud prevention, support)	2
Data Protection Officer	2
Data Protection Officer	2
B. Data controllership and applicable law	2
C. Processed personal data for core purposes	3
General customer information	3
Means of payment data	3
Purchase data	3
Information about the device	4
Usage data	4
D. Processed personal data for pilot analytics and surveys	4
E. Processing purposes and modalities	4
F. Legal basis	5
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. Right to erasure and to be forgotten	12
N. Correction and limitation	13
O. Information and transmission rights	13
P. Right of objection	13
Q. Right to lodge a complaint	14
R. Data processing location	14
S. Data protection representation in the European Union	14
T. Changes of this privacy notice	15
U. Accessibility and download of the privacy notice	15

A. Contact information of the Controller and the DPO

Controllership depends on the processing purpose:

Data controller for core functionalities (accurate journey capture, ticket purchase/fulfilment, settlement, fraud prevention, support)

FAIRTIQ Ltd.

Aarberggasse 29

3011 Bern

Switzerland

UID: CHE-370.720.489

feedback@fairtiq.com

Data Protection Officer

FAIRTIQ Ltd.

Data Protection

Aarberggasse 29

3011 Bern

Switzerland

app.privacy@fairtiq.com

Data controller for pilot analytics and surveys (travel analysis in the pilot; sending and evaluating personalised surveys)

The Data Controller

Northern Trains Limited

George Stephenson House

Toft Green

York

YO1 6JT

Data Protection Officer

The Data Protection Officer

Northern Trains Limited

dataprotection.officer@northernrailway.co.uk

B. Data controllership and applicable law

This privacy notice applies to the "Mobile Pay As You Go" trials on the railway line Sheffield - Doncaster with the FTQ Lab App.

FAIRTIQ Ltd. («FAIRTIQ» or «we») is the operator and controller for data processing steps in connection with the core functionalities of the FTQ Lab App («application»).

Northern Trains Ltd. ("Northern Trains") is the controller for data processing steps in connection with travel and public transport usage analysis and surveys.

Personal data is processed in accordance with

- the UK or relevant Data Protection laws, if the customer obtains services in the United

Kingdom;

- the Federal Act on Data Protection (FADP) where personal data is processed in Switzerland or where the processing activities have an effect 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.

C. Processed personal data for core purposes

General customer information

- First and last name,
- 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: discount level;
- Deposited railcard details (optional);
- User ID;
- IP address and device ID;
- Information on abusive or other fraudulent behaviour;
- Interactions with customer care.

Means of payment data

- Payment method;
- Partially anonymised payment method details.

Travel data

- Tracking (location) and activity data (based on a motion sensor, if active);
- Registered electronic tickets (ticket data);
- 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.

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.

D. Processed personal data for pilot analytics and surveys

The trial is being overseen by the Department for Transport, who have engaged Ipsos UK to carry out surveys of trial participants for analytical purposes. This work may involve the use of limited personal data and is covered by a separate Privacy Policy which can be found at <https://www.northernrailway.co.uk/legal/digital-pay-you-go-policy>

E. Processing purposes and modalities

This time-limited trial on the railway line Sheffield – Doncaster route is intended to validate that FTQ Lab can issue real, valid tickets and correctly detect, price and settle journeys in everyday conditions. The trial also assesses operational performance (reliability, fraud prevention, support) and overall customer experience to inform a potential wider roll-out.

Personal data transferred **by the customer to FAIRTIQ** via the application are processed by FAIRTIQ for the following **core 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 **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 anonymised form for this purpose.
- To **analyse and understand user behaviour, app usage patterns and consumption behaviour** in order to assess and improve application usability, navigation, and functionality. Where consent has been provided by the customer, this includes collecting aggregated usage and interaction data through the analytics tool PostHog, and the transfer of results of the analysis of public transport journeys and spending in personalised form to third parties.
- 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 our services to existing customers, and surveys concerning the use of FAIRTIQ and mobility in general.
- 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**.

Personal data transferred by the customer to Northern Trains Limited via the application and / or by taking part in surveys are processed by Northern Trains Limited on behalf of the Department for Transport (DfT). More information can be found at <https://www.northernrailway.co.uk/legal/digital-pay-you-go-policy>.

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

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 application 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 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 analysis of customers' travel behaviour and the customers' answers provided via surveys in personalised form is based on consent. Contacting customers for requesting participation in surveys and consenting to personalised travel analysis is based on legitimate interest.

The legal basis for the processing of personal data of customers within the European Union is Art. 6 (1) (a), (b), (c), (e), (f) GDPR. The processing of special category data is further based on Art. 9(2)(b) 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 **FAIRTIQ** and its **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 Switzerland, Germany, Austria, and Portugal,.

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**: The registration of the means of payment in connection with the application is directly arranged by the payment provider 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 **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 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 analyzes the user'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 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 **Northern Trains Limited**: FAIRTIQ forwards the required personal data to Northern Trains Limited to fulfil the customer care, to combat abuse, and to communicate with customers, and for payment and accounting purposes. In this context, Northern Trains acts as an independent controller for the personal data processing.

If consent is provided by the customer, travel data and answers to surveys may be transferred by FAIRTIQ as a processor to Northern Trains as a controller in personalised form for the analysis of consumption and usage behaviour.

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).

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 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 unsubscribe link or the instructions in each message that FAIRTIQ sends to the customer.

L. Data retention period

Data processed for core purposes

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 or **until the end of the FTQ LAB app trial plus three months** (whichever comes first) 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 customer information shall be retained for the purpose of combating abuse, for the means of communication with the customer and for commercial purposes **a) for two years** from the last journey or from joining a campaign (depending on what occurs later) or **b) until the end of the FTQ LAB app experiment plus three months** ((a) or b) - whichever comes first) and then deleted.

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).

Data processed for analytics purposes

The retention period for personal data used by for Survey and Analytics purposes is covered at <https://www.northernrailway.co.uk/legal/digital-pay-you-go-policy>

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.

M. 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.

N. 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 the section [Processed personal data](#) directly in the app.

Modifications are not possible during an ongoing journey.

O. 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.

P. 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) (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.

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

R. 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/hubfs/ftq-lab_privacy-notice_uk-trial.pdf

S. 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

T. 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/hubfs/ftq-lab_privacy-notice_uk-trial.pdf

U. Accessibility and download of the privacy notice

The current version of the privacy notice can be viewed and printed at

https://fairtiq.com/hubfs/ftq-lab_privacy-notice_uk-trial.pdf

This Privacy Notice comes into effect on 27 October 2025 and remains valid until replaced or updated.