RailSync GmbH, St. Annenufer 2, 20457 Hamburg, Germany, ensures compliance with legal standards and internal company guidelines as part of the RailSync website and cloud-based software solution (hereinafter referred to as "RailSync", "we", "us"). Accordingly, we would like to inform you about the collection, processing and use of personal data in the context of the use of our RailSync application in accordance with Art. 13, 14 of the General Data Protection Regulation (GDPR). We process personal data only in accordance with the applicable legal and data protection regulations, which result in particular from the GDPR and the Federal Data Protection Act (BDSG).

RailSync has set itself the goal - combined in one solution - of simplifying and making more efficient the administrative effort involved in coordinating rail-based logistics between all players. We focus on an efficient user experience and the protection of your data, because this is extremely important to us.

RailSync has taken extensive data security precautions to protect your data. Compliance with applicable data protection mechanisms is a matter of course for us.

We only process, store and share the information and data with our partners that is necessary for the provision of our services.

This information applies to the processing of personal data when using the cloud-based software solution RailSync and the website.

Note: For better readability, the generic masculine is used in this privacy policy. Unless otherwise indicated, the personal designations used in this document refer to all genders.

# Contents

# 1. Responsible person, contact data protection officer

RailSync GmbH, St. Annenufer 2, 20457 Hamburg, Germany, is responsible for processing your data in RailSync. If you have any questions regarding data protection, you can also contact us at any time at the following e-mail address:privacy@railsync.app . Our data protection officer can be contacted via RailSync GmbH or the above e-mail address.

# 2. Categories of personal data

The following categories of personal data may be processed by us in connection with our services:

- Master data: First name, surname, self-created password and password changes (not visible to RailSync), company, role, user ID.
- Communication data: E-mail address, communication content (e.g. from e-mails, contact forms or use of the integrated instant messaging service), telephone number (optional)
- Software usage data: Time stamps for certain actions, contractual partners, order data (e.g. container data)
- Technical data: Operating system version , browser, IP address with location
- Voluntary information: This includes personal data that you provide to us on a voluntary basis without us explicitly asking for it, such as suggestions for improvement or responses to a survey.

# 3. Legal basis and purposes of data processing at RailSync

## 3.1. Usage data

When you visit our websites, so-called usage data is temporarily evaluated on our web server for statistical purposes as a log in order to improve the quality of our websites. This data record consists of

- the name and address of the requested content,
- the date and time of the query,
- the amount of data transferred,
- the access status (content transferred, content not found),
- the description of the web browser and operating system used,
- the referral link, which indicates from which page you came to ours,
- the IP address of the requesting computer, which is shortened so that a personal reference can no longer be established.

The aforementioned log data is only analyzed anonymously.

The legal basis for the processing of usage data is Art. 6 para. 1 sentence 1 lit. f GDPR. The processing is carried out in the legitimate interest of providing the content of the website and ensuring a device- and browser-optimized display.

## 3.2. Contact us via the contact form

**Purposes of the processing**

If you send us inquiries via the contact form, your details from the inquiry form, including the contact details you provide there, will be stored by us for the purpose of processing the inquiry and in the event of follow-up questions.

**Legal basis for the above processing**

This data is processed on the basis of Art. 6 para. 1 lit. b GDPR if your request is related to the performance of a contract or is necessary for the implementation of pre-contractual measures. In all other cases, the processing is based on our legitimate interest in the effective processing of the inquiries addressed to us (Art. 6 para. 1 lit. f GDPR)

## 3.3. Newsletter

**Purposes of the processing**

If you subscribe to the newsletter, the data in the respective input mask will be transmitted for processing. Subscription to the newsletter takes place in a so-called double opt-in procedure. This means that after registration, an email is sent to the email address provided for registration. This email is used for verification purposes and asks you to confirm your registration. This confirmation is necessary so that no one can register with other people's e-mail addresses. When registering for the newsletter, the user's IP address and the date and time of registration are stored. This serves to prevent misuse of the services or the e-mail address of the person concerned. The data is not passed on to third parties. An exception is made if there is a legal obligation to pass on the data. The data is used exclusively for sending the newsletter. The newsletter is used for information purposes and only for direct advertising for our own similar goods or services. Subscription to the newsletter can be canceled at any time. Consent to the storage of personal data can also be revoked at any time. There is a corresponding link for this purpose in every newsletter.

**Legal basis of the above processing**

The legal basis for the processing of data after registration for the newsletter by the user is Art. 6 para. 1 lit. a) GDPR if the user has given consent. The legal basis for sending the newsletter as a result of the sale of goods or services is Section 7 (3) UWG

## 3.4. Setting up a RailSync account

**Purposes of the processing**

In order to obtain the status of a registered and verified user and thus have the possibility to use the services of RailSync including (and possibly) those of operators of logistics locations (e.g. terminals), the creation of a RailSync account via the relevant registration page ("Registration") is required.

Surname, first name, e-mail address, company incl. company type and role are mandatory for registration, subsequent verification and the use of RailSync services. The data is stored in the user account in RailSync. Optionally, the telephone number can also be stored.

Registration with the above data already provides limited access to RailSync functionalities and allows you to get an impression of the "look and feel". Access to the functionalities

assigned to the role is enabled after successful verification in accordance with the approval process.

Upon registration, we check whether registrations already exist with the registration information provided (e-mail address and, if applicable, telephone number) and possibly the plausibility of the information entered based on criteria previously defined for each "activated" company (e.g. via the e-mail domain).

After clicking on Submit and successfully checking the plausibility of the information entered, a registration link is sent to the specified email. By clicking on the confirmation link, the registration is completed and the coordinator assigned to the specified company or role is notified of the new registration. Until verification is complete, the status of the user account is set to "pending".

Notes: Every registered user can manage their own user data in their user account and is responsible for updating it themselves. RailSync can only intervene here in cases of particular hardship and at the user's separate request. A change of e-mail address always requires confirmation via a confirmation link and subsequent verification by the responsible coordinator (see below).

**Legal basis of the above processing**

Art. 6 para. 1 sentence 1 lit. b) GDPR

The processing of the data is necessary for the fulfillment of the contract and enables users to obtain a limited overview of the app. Furthermore, we ensure that multiple registrations of users are avoided.

## 3.5. Verification or activation of registration and role assignment by the administrator

**Purposes of the processing**

The verification of the registration and the role assignment of a user is carried out by the "responsible" coordinator assigned to the respective user.

These are:

| **Users** | **Responsible coordinator** |
|---|---|
| Terminal Coordinator<br>*Each additional terminal coordinator* | RailSync Admin<br>*Already verified other terminal coordinator* |
| 1. coordinator (the terminal partner)<br><br>*Each additional coordinator (the terminal partner)* | Terminal coordinator (in each case for cooperating companies)<br>*Already verified other coordinator (the terminal partner)* |
| Other roles Terminal employee | Respective terminal coordinator |
| Other terminal partner roles | Respective coordinator |

For verification purposes, the coordinator receives access to the user account information in order to carry out the verification. During the verification process, the coordinator appointed by each company confirms that they are authorized persons for the respective company. The responsible coordinator also assumes the function of managing the respective user roles

Note: If no responsible coordinator has been verified at the time of registration, verification is not possible. The status of the user account is set to "pending" until verification has taken place.

Once verification has been completed, the user receives an e-mail with a notification that verification has been completed, including information on which coordinator carried out the verification. The user account is set to "active" and the assigned role, including approved functionalities, can be executed.

Note: The coordinator also has the option of setting a user account to "inactive". The user is informed of every change to a role or deactivation by email, including information on which coordinator made the change

**Legal basis of the above processing**

Art. 6 para. 1 sentence 1 lit. b) GDPR

The processing of the data is necessary for the contract fulfillment . Furthermore, we ensure that only authorized persons have access to relevant functions and only to information intended for them.

## 3.6. Re-verification of the account at regular intervals

At regular intervals (usually 12 months after the last verification and after a longer period of inactivity), a re-verification link with a deadline will be sent to the e-mail address stored in the user account. After clicking on the link, the user account will be marked as still "active".

If there is no response, the first re-verification email will be followed by two further reminder emails, each with a deadline. If there is still no response, the account will be set to "inactive", access to functionalities will be restricted (read authorization) and the coordinator responsible for the company will be informed.

The coordinator then has the opportunity to check the inactivity. Furthermore, after logging in again (if the user account has not yet been deleted), the user must apply for verification via the user account again. The coordinator assigned to the user (see above) will be informed of this and can carry out the verification again. The user account then receives the status "active".

**Legal basis of the above processing**

Art. 6 para. 1 sentence 1 lit. b) and c), 32 GDPR

The processing of the data is necessary for the fulfilment of legal technical and organizational protection obligations in order to protect critical infrastructures from criminal acts and to increase security for the operators of logistics locations (e.g. terminals) and users.

## **3.7.** Visibility for cooperating companies

**Purposes of the processing**

Active users (with the exception of users who only have read authorization) can be viewed by the assigned, cooperating companies with their respective role, function, contact information and status (e.g. availability) in a contact list and in an integrated instant chat messenger. This

visibility is given as long as the respective user account is active, not archived or not deleted and a link/cooperation of the respective companies is active/established in RailSync.

**Legal basis of the above processing**

Art. 6 para. 1 sentence 1 lit. b) GDPR

The processing of the data is necessary for the fulfillment of the contract.

## 3.8. Slot booking

To book, change or edit a slot for handling orders at logistics locations, the user uses the corresponding function within the software environment. As part of the slot booking or management, RailSync stores the booking or processing user (contact information such as company, name, e-mail address and, if applicable, telephone number) in the respective slot. (Verified and active) employees (except those with read rights) of the companies involved in the booking or processing (terminal and relevant terminal partners) can view this information. Any changes to the booking can be viewed in the change log and by the parties relevant to the handling of the respective slot. Slot bookings are only possible between companies for which a link/cooperation between the companies is active/set up in RailSync.

The coordinator of a company can make the setting for the respective company that a central contact information (telephone and/or e-mail address) is stored instead of the respective user information.

Note: Personal information that is stored and processed as part of a slot booking or management (including changes) remains stored as booking-related information for 10 years in accordance with the statutory periods.

**Legal basis for the above processing**

Art. 6 para. 1 sentence 1 lit. b) GDPR

The processing of the data is necessary for the fulfillment of the contract.

## 3.9. (Temporary) blocking of user accounts of partner companies

**Purposes of the processing**

In the event of violation of applicable law, disregard of instructions from the operators of logistics locations or, for example, misuse of functionalities in RailSync, reasons for this can be stored, which are associated with a (temporary) blocking of access or restriction of use

The entry is made in a free text field by the operator of the logistics location (e.g. terminal) and can only be viewed by the operator. RailSync itself has no access to the encrypted information and can only see the existence of a block or usage restriction.

To clarify: The blocking of a user account is not a general blocking of the user account, but a restriction that an operator of a logistics location can impose on certain users to protect its own facilities. The block or restriction only affects the link between the initiating terminal and the respective user of a partner company, i.e. the blocked user can no longer perform any functions (e.g. slot booking) for the initiating terminal.

**Legal basis for the above processing**

Art. 6 para. 1 sentence 1 lit. f) GDPR

The legitimate interest in the storage of violations that lead to the (temporary) blocking of user accounts arises from the right of the operators of the logistics locations to take measures for building and plant security, measures for business management and measures to prevent criminal offenses.

## 3.10. Instant messaging service

**Purposes of the processing**

Direct and smooth communication between all stakeholders involved is an essential element in achieving the goals pursued by RailSync, such as a significant increase in efficiency in the coordination of train dispatching, and raising the communication channels from analog processes to a digital level in which all stakeholders can find the information they need in one central location.

In addition to the other functionalities, the instant messaging service Pusher from Pusher Limited has been implemented for this purpose. This enables a communication exchange in the form of a chat on certain events (e.g. slot booking) at any time, comprehensibly and centrally. Furthermore, important and general information can be made available in a traceable manner and in real time via push notifications, e.g. to its partner companies.

The user ID, name and e-mail address are transmitted to Pusher for use. This is mandatory for the integration and use of the service

**Legal basis of the above processing**

Art. 6 para. 1 sentence 1 lit. b) GDPR

The processing of the data is necessary for the fulfillment of the contract and is intended to ensure that support requests can be processed efficiently and in a structured manner and thus the best possible user experience can be achieved.

## 3.11. Support function

**Purposes of the processing**

RailSync strives to provide its users with the best possible user experience, which is why RailSync also strives to support its users efficiently and as needed, should they have concerns, need support or, contrary to expectations, have problems using functionalities within the software environment. In addition to telephone and direct contact during business hours, RailSync offers the use of the digital e-mail support service Freshdesk from Freshworks Inc. In each case, a ticket is opened in Freshdesk for a support request so that these can be processed efficiently, prioritized and, if necessary, chronologically. Contact information that is personal data (?) (e.g. e-mail signatures) can be stored in the Freshdesk software environment. Furthermore, tickets can also be created in JIRA (Atlassian. Pty Ltd) on the basis of support requests if required. Individual personal information can be assigned to the tickets in order to enable reliable and traceable processing.

**Legal basis of the above processing**

Art. 6 para. 1 sentence 1 lit. b) GDPR

The processing of the data is necessary for the fulfillment of the contract and is intended to ensure that support requests can be processed efficiently and in a structured manner and thus the best possible user experience can be achieved.

## 3.12. Other integrated services and collection of technical data

**Purposes of the processing**

When you access our app, we process data to enable you to use the app, monitor and optimize its performance and, if necessary, take the technical measures required to keep the system stable. In the event of malfunctions, the information is also used to analyze and rectify errors

The following services are integrated for this purpose:

- SRedis: We use the Redis service provided by AWS to temporarily store (cache) application data in the backend. This is a high-performance in-memory data store that is used to temporarily store data in order to improve system performance and response speed. Redis is used in particular for fast read and write accesses in the backend. As part of Redis use, personal data is processed to a limited extent, in particular the user ID of the user together with the timestamp of the last online access. This data is only stored temporarily and is used to control simultaneous processing operations (e.g. to avoid data conflicts) and to display the user's online activity in the system. Processing is carried out for session control, optimization of user interaction and technical control of editing processes in the system. The storage is only temporary in the context of caching and is regularly deleted or overwritten.

- Grafana (Raintank Inc.): We use the external tool **Grafana** to visualize system and application metrics. Grafana is a visualization and monitoring tool that is used to display performance data from various sources (e.g. databases, infrastructure, external monitoring services such as New Relic). It is used to monitor system resilience and display the performance of the application in real time. As a rule**, no personal data** is stored or processed in Grafana. Grafana is used exclusively to visualize technical metrics and aggregate data without direct reference to individuals.

- New Relic (New Relic Inc.): We use the New Relic service from New Relic Inc. to monitor and analyze the performance of our application and system infrastructure. The integration takes place via a plugin in Grafana, which displays performance data visually and makes it analyzable. New Relic is an external monitoring tool for monitoring the performance of applications, databases and infrastructures. It supports the identification of bottlenecks, errors and unusual behavior in the system. As part of the integration of New Relic, the user ID may be processed. This can be processed in the system for two reasons:
    - Visualization of user data via a read-only database account:
      A read-only database user who accesses tables with user data is used to display database statistics in Grafana. This allows key figures to be displayed aggregated by user group, for example.
    - Collection in log data: Request or error logs transmitted to New Relic for analysis may in certain cases contain the user ID - especially if an error occurs in direct connection with a user action.

The processing takes place exclusively for error analysis, performance optimization and quality assurance of our system. Evaluation for other purposes or disclosure to unauthorized third parties does not take place . Personal data is not processed or stored.

- Firebase Google Analytics (Google LLC): We use the Google Analytics service, provided by Google LLC, to analyze the use of our web application and to optimize the user experience. Google Analytics is an external web analytics service that helps us understand user behavior on our website, measure usage and identify opportunities for improvement in the application. The aim is to continuously optimize the user-friendliness and efficiency of the application. The following data may be processed when using Google Analytics:
    - User activities within the web application (e.g. page views, click behavior)
    - Geographical data (e.g. country, city or region)
    - System information (e.g. operating system: Mac/Windows/Linux; device type: desktop/mobile/tablet; browser type)
    - Language settings of the browser
    - IP address (is usually stored anonymously)
    - Session information, including duration, number of page views and bounce rate

  This data is collected pseudonymously and does not allow to identify the data subject. The data collected is used exclusively for statistical and analytical purposes, in particular to:

    - Analysis of visitor behavior on the website
    - Measurement of website traffic and usage patterns, e.g:
        - Number of visitors, sessions, page views, unique visitors
        - Dwell time, bounce rate, pages per session
    - Evaluation of access sources:
        - Direct access, organic search results, referrals, social media platforms
    - Examination of entry and exit pages as well as search queries within the site

  Data processing is carried out to improve the user experience and to further develop the web application.

- Freshworks: In order to efficiently manage support requests and ensure smooth communication with our users, Freshdesk, a product of Freshworks Inc., is used in support and customer service. As part of its use, the name, e-mail address, telephone number, ticket content and any other information provided by users may be stored. This data is used exclusively to process support requests and to improve our customer service. Freshdesk processes data in accordance with the applicable data protection regulations. Further information on data processing by Freshdesk can be found in the Freshworks privacy policy on their website.

- Pusher: We use the external service **Pusher** to provide real-time communication in our system. This makes it possible to exchange messages and notifications in real time between our system and the users. When using Pusher, we only transmit the

**user ID** of the authenticated user who is currently logged in. This information is transferred to Pusher under the relevant fields. The personal data transmitted is used exclusively to:

- Send real-time messages to users via Pusher Channels.
- Provide push notifications via Pusher Beams.
- perform authentication in so-called *presence channels* to determine which users are online or offline.

This authentication is necessary so that the front-end components of our system can interact securely and reliably with the Pusher service.

- AWS : As part of our system, we use various services from Amazon Web Services (AWS) to ensure the functionality, security and user-friendliness of our platform. Personal data is only processed to the extent necessary and used exclusively for specified purposes:

  - Sending emails via AWS SES: We use the Amazon Simple Email Service (SES) to send system-related notifications (e.g. account activations, password resets, system information). Only the email address of the data subject is transmitted. Data processing is carried out for the purpose of communicating with users in the context of contract fulfillment and to ensure system operation.
  - User management via AWS Cognito: We use Amazon Cognito to register, manage and authenticate user accounts.
    The following personal data is processed and stored as part of the account creation process: e-mail address, first name, last name. This information is used to create and manage the user account and to display the user name in notifications (e.g. in the event of password changes). The data is stored in the attribute fields provided for this purpose within AWS Cognito.
  - Data storage in AWS RDS (PostgreSQL database): Our central system database is operated via Amazon Relational Database Service (RDS). Personal user data is stored in a structured manner in this database. The following data is processed: User ID, e-mail address, first name, last name. This information is required for various system functions, e.g. to identify users when they log in, to display names in the user area and to document user actions within the system (e.g. creating shift reports or change logs).

  All AWS services used are operated exclusively within the EU or in countries that ensure an adequate level of data protection, unless expressly agreed otherwise. Processing is carried out in accordance with the applicable data protection laws, in particular the General Data Protection Regulation (GDPR).

- Jira and Confluence (Atlassian Pty Ltd.): Jira and Confluence are products of Atlassian Pty Ltd. Jira serves as a ticket and project management system that is mainly used for developing new features and managing technical tasks. Confluence is a platform for documentation and collaboration within our team. In principle, no

personal data of users is stored in Jira or Confluence. However, there is a limited exception:

- If a user creates a support ticket (e.g. in the event of a technical problem or a reported error), personal data such as name, e-mail address or ticket content provided by the user may be stored in the system.

All data processed via Jira or Confluence is stored on Atlassian's servers. Atlassian uses data centers in the EU and globally distributed cloud servers for this purpose. The support ticket data stored in Jira is used exclusively to analyze and resolve problems. The information is not used for advertising or other commercial purposes. Access to this data is strictly limited to authorized members of our support and development team. The information contained in the tickets is not automatically analyzed or further processed, except for the purpose of troubleshooting and further development of the software. No automated user profiles are created on the basis of this data.

**Legal basis of the above processing**

Art. 6 para. 1 sentence 1 lit. b) GDPR (for the services Redis, Grafana, New Relic, Jira, Freshworks and AWS); for all other services mentioned, Art. 6 para. 1 sentence 1 lit. f) GDPR applies

The processing of the data is necessary for the performance of the contract (provision and use of the app) in order to keep our app available (i.e. stable and secure), to optimize it, to develop it further and thus to offer our customers the best possible services and to increase customer satisfaction.

# 4. Categories of recipients

**Logistics site operator**

There is a contractual relationship with the respective logistics site operators to which you (can) request access, in which we act as a processor for the logistics site operator. As processors of the logistics site operators, we are subject to confidentiality and are contractually obliged to transfer your personal data to the respective operators for a specific purpose and to comply with data protection regulations.

**Cooperation company**

The following information can be viewed by cooperation companies and their users in RailSync in the contact list or slot booking information, provided that a link is active/established between the companies: Surname, first name, email address, telephone number if applicable

**Coordinators**

For verification purposes, the relevant coordinator receives a one-off verification request with the personal data required to check whether the person is an authorized person from their

company. In addition, the respective coordinators of the companies have access to the user information of the registered colleagues at all times.

**Service provider / processor**

To process your data, we sometimes use specialized service providers who in turn work for us (e.g. IT and software service providers, hosting providers, data centers, payroll service providers, etc.). Our service providers are carefully selected and regularly monitored by us. They only process personal data on our behalf and strictly in accordance with our instructions on the basis of corresponding order processing contracts. The data passed on may only be processed by the respective processor on the basis of agreements in accordance with Art. 28 para. 3 sentence 1 GDPR. The processors are subject to confidentiality and are contractually obliged to maintain data protection through the order processing contract

**Other**

In addition, there may be further legal obligations to transfer data in individual cases, but these may only arise in specific individual cases and not in general. This also includes cooperation with investigating authorities and the transfer of data in this context in compliance with data protection law.

Data processing generally takes place in the EU/EEA. Processing of data outside the EU/EEA is permitted under the conditions of Art. 44 et seq. of the GDPR

# 5. Duration of storage

Unless we have already informed you in detail about the storage period, we delete personal data if it is no longer required for the aforementioned processing purposes and there are no legitimate interests or other (legal) reasons for storage that prevent deletion or anonymization. In the case of statutory retention obligations, erasure or anonymization will only be considered after the respective retention obligation has expired. Until deletion or anonymization, the data will be stored in blocked form.

**Access logging (log files, technical data)**

- Data (database ID and operating system version) is completely deleted or anonymized after 3 years at the latest

**Other activity data**

- Activity data (e.g. gate access) is deleted or anonymized after 3 years at the latest if it is not billing-relevant data
- Location data is anonymized before storage

**Billing-relevant data**

- Storage period in accordance with the applicable provisions of the HGB: 10 years

**User account (inactive)**

- After one year of inactivity, the user is informed of the inactivity and informed that a lack of interaction leads to the deletion or anonymization of the data
- Without interaction, the user account is automatically deleted or anonymized after 3 years at the latest

**Request for deletion of the user account**

- If the deletion of the user account is requested, the account will be blocked
- E-mail address and telephone number will be anonymized immediately after the request for deletion of the user account
- All further data will be stored for 3 years after the request for deletion; after that, all personal data will be deleted or anonymized.

# 6. Information about your rights

The following rights are available to you under the applicable data protection laws:

- Right to information about your personal data stored by us;
- Right to rectification, erasure or restriction of processing of your personal data;
- Right to object to processing which serves our legitimate interest, a public interest or profiling, unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing serves the establishment, exercise or defense of legal claims;
- Right to data portability;
- right to complain to a supervisory authority.

You can revoke your consent to the collection, processing and use of your personal data at any time with effect for the future. You can find more information on this in the respective sections above, where data processing based on your consent is described.

If you wish to exercise your rights, please address your request to:

RailSync GmbH, St. Annenufer 2, 20457 Hamburg, or to the e-mail address:

privacy@railsync.app