

Privacy Notice of Rail Cargo Terminal – BILK Fejlesztő és Üzemeltető Zrt.

In effect: _____2024

Table of contents

1.	GENERAL INFORMATION.....	3
2.	UPDATING AND ACCESSING THE NOTICE.....	3
3.	SPECIFIC DATA PROTECTION CONDITIONS	3
4.	PROCESSED DATA AND PURPOSES OF PROCESSING	3
5.	PERSONS ENTITLED TO PROCESSING	8
6.	DATA SECURITY (TECHNICAL AND ORGANISATIONAL) MEASURES	9
7.	DATA PROTECTION RIGHTS AND REMEDIES OF THE DATA SUBJECTS	9

1. **GENERAL INFORMATION**

Rail Cargo Terminal - BILK Fejlesztő és Üzemeltető Zártkörűen Működő Részvénytársaság (“**Company**”) processes certain information qualifying as “personal data” within the meaning of Article 4 (1) of the EU General Data Protection Regulation No. 2016/679 (“**GDPR**”) about third parties, the contact persons of its contractual partners and other persons, e.g. consumers (hereinafter jointly: “**data subject(s)**”).

This privacy notice (“**Notice**”) provides information on the processing of personal data, as well as on the rights and remedies of data subjects related to processing.

Contact details of the Company:

Contact details of the Company:

Registered seat of the Company: 1239 Budapest, Európa utca 4.

Company registration number: Cg. 01-10-044722,

The Company is registered by the Court of Registration of the Municipal Court of Budapest.

Email address of the Company: cegkapu.rct.bilk@railcargo.com

Website of the Company: www.railcargobilk.hu

Representatives of the Company and their contact details:

Attila Czöndör Executive member of the Board of Directors

Gyula Garai member of the Board of Directors

2. **UPDATING AND ACCESSING THE NOTICE**

The Company reserves the right to amend this Notice unilaterally, with immediate effect following the amendment, at its own discretion anytime, considering the limitations contained in the legal regulations, and where required, with the prior notification of the data subjects in due time. This Notice may be amended, in particular, if necessary due to changes in legal regulations, practices of the data protection authority, business or employee needs, new activities resulting in the processing of personal data, or newly identified security risks. Upon request, the Company sends a copy of the effective Notice to the data subjects.

3. **SPECIFIC DATA PROTECTION CONDITIONS**

In certain cases, specific data protection conditions may also apply, of which the data subjects will receive separate information. For example the notice related to the operation of the electric monitoring system (cameras), and the notice concerning the cookies used by the Company on its websites.

4. **PROCESSED DATA AND PURPOSES OF PROCESSING**

The processed data, the purposes of processing, the legal basis for processing, the duration of processing and the persons entitled to access the data are detailed in the table below. If any purpose of processing is necessary for the legitimate interests of the Company or third parties, the Company provides its interest balancing test used for establishing the legitimate interest upon request submitted to any of its contact details listed above.

Where this Notice indicates a limitation period of establishing a claim as the duration of processing, the act interrupting the limitation period shall extend the duration of processing until the new expiry date of the limitation period.

Purpose of processing	Legal basis of processing	Processed data	Data retention period, access rights, recipients of data transfers
<p>Documenting corporate events, making recordings</p>	<p>Article 6 (1) (f) of the GDPR (the processing of the data is necessary for the enforcement of the legitimate interests of the Company).</p> <p>Legitimate interest: to document the events and to promote the controller and enhance its reputation.</p> <p>The consent of the data subject is not required for recording his/her likeness or voice, and for the use of such recording if made of a crowd or in a public event (Section 2:48 of Act V of 2013 on the Civil Code (“Civil Code”).</p>	<p>Taking photos and/or videos at events organised by the Company (likeness of the data subjects). With the consent of the data subject, the recordings can also be used on the Company’s intranet, external internet sites (e.g. the Company’s LinkedIn site) or on other media (e.g. corporate promotional materials).</p>	<p>Upon the data subject’s request, the recordings can be deleted at any time.</p> <p>The right to withdrawal may only be exercised completely before the publication of the materials in case of recordings disclosed to the public. For example, third parties may save or copy the disclosed recordings and the Company cannot check this.</p> <p>Before the publication of the recordings, persons entitled to have access to the recordings within the Company’s organisation:</p> <p>HR employee (as part of the financial division) Members of the Board of Directors. IT staff at the company’s seat (external partner).</p>

Purpose of processing	Legal basis of processing	Processed data	Data retention period, access rights, recipients of data transfers
<p>Sending invitations for the events organised by the Company (e.g. partner meetings) and registration of the participants</p>	<p>Article 6 (1) (f) of the GDPR (processing is necessary for the legitimate purposes of the Company).</p> <p>Legitimate interest: successful and effective organisation of events, documentation of the number and scope of participants.</p>	<p>Contact details of the data subjects intended to be invited by the Company: name of the participant and the represented organisation, other data related to participation provided by them (e.g. date of arrival, preferred presentation, etc.).</p>	<p>If the data subject does not object to the processing of his/her data, the contact data can be used in the future following the event, for sending invitation for the events organised by the company, and for communication. The Company processes the data for 5 years following the last communication with the data subject (Section 6:22 (1) of the Civil Code – claims lapse in 5 years).</p> <p>Persons entitled to have access within the Company's organisation: Persons entitled to access the data: Sales Head of customer service (customer service) Members of the Board of Directors</p> <p>Data are transferred to: Rail Cargo Hungaria Zrt., Marketing department address: 1133 Budapest, Váci út 92.</p>

Purpose of processing	Legal basis of processing	Processed data	Data retention period, access rights, recipients of data transfers
<p>Processing the data of the contact persons of contractual partners, and/or persons involved in performance / controlling performance, for the purpose of performing the contract (daily execution). This includes for example the processing of the mailing address of the contact persons, instructions of the contact persons concerning the performance of payments, or sending official notifications by using the contact data and the information related to the contractual obligations to be performed. For example: buyer contracts, supplier contracts.</p>	<p>Depending on whether the contract is signed with a data subject (e.g. sole trader) or other entities: Article 6 (1) (b) of the GDPR – performance (execution) of the contract concluded directly with the data subject / Article 6 (1) (f) of the GDPR – legitimate interest of the Company and the entity concluding a contract with the Company: performance of the contractual obligations, exercise of rights, and coordination of the economic cooperation of the parties.</p> <p>Handover of the personal data is a contractual requirement; without personal data, the Company cannot conclude and execute the contract.</p>	<p>Name and contact details of the contact persons of contractual partners, persons involved in performance and in controlling performance (email, phone, mobile phone) and any other activity and communication in relation to the contract containing any personal data (e.g. communication received from the contact person or any other natural person acting on behalf of the partner).</p> <p>The personal data are provided to the Company by the contractual partner or by the data subjects themselves.</p>	<p>5 years following the termination of the contractual relationship (Section 6:22 (1) of the Civil Code – unless the Civil Code regulates otherwise, the claims lapse in 5 years.)</p> <p>In relation to the fulfilment of tax obligations: the data retention period is 5 years calculated from the last day of the calendar year when the tax return or report should have been made, or in the absence of tax return or report, when the tax should have been paid (Sections 78 (3) and 202 (1) of Act CL of 2017 on the rules of taxation (“Taxation Act”).</p> <p>In case of financial documents: the data retention period is 8 years (Sections 168-169 of Act C of 2000 on accounting (“Accounting Act”). In practice, this is the case when the data form part of the documents supporting accounting, e.g. the data are contained in documents related to the contract concluded by the Company and the partner (e.g. in the order) or on the issued invoice.</p> <p>Persons entitled to have access within the Company’s organisation: Persons entitled to access the data: Financial Division Sales Only the authorised persons have access to the drives containing the data.</p> <p>Data are transferred to: Rail Cargo Hungaria Zrt. Chief Accountant department</p>

Purpose of processing	Legal basis of processing	Processed data	Data retention period, access rights, recipients of data transfers
<p>Processing the data of the contact persons of contractual partners, and persons involved in performance and in controlling performance, for the purpose of performing any other tasks in relation to compliance issues related to the contract or the performance of the contract, including the searching of legal remedies necessary for ensuring the contractual rights. For example: buyer contracts, supplier contracts.</p>	<p>In this case, the legal basis of processing is the Company's legitimate interest (Article 6 (1) (f) of the GDPR). Legitimate interest: handling of compliance issues in relation to the contract, performance of any other tasks in relation to the fulfilment of the contract, including the searching of legal remedies necessary for ensuring the contractual rights.</p>	<p>Name and contact details of the contact persons of contractual partners, persons involved in performance and in controlling performance (email, phone, mobile phone, telefax) and any other activity and communication in relation to the contract containing any personal data (e.g. communication received from the contact person or any other natural person acting on behalf of the partner).</p> <p>The personal data are provided to the Company by the contractual partner or by the data subjects themselves.</p>	<p>5 years following the termination of the contractual relationship (Section 6:22 (1) of the Civil Code – unless the Civil Code regulates otherwise, the claims lapse in 5 years.)</p> <p>In relation to the fulfilment of tax obligations: the data retention period is 5 years calculated from the last day of the calendar year when the tax return or report should have been made, or in the absence of tax return or report, when the tax should have been paid (Sections 78 (3) and 202 (1) of the Taxation Act.</p> <p>In case of financial documents: the data retention period is 8 years (Sections 168-169 of the Accounting Act). In practice, this is the case when the data form part of the documents supporting accounting, e.g. the data are contained in documents related to the contract concluded by the Company and the partner (e.g. in the order) or on the issued invoice.</p> <p>Persons entitled to have access within the Company's organisation departments competent according to the contract Financial division Sales</p>

5. PERSONS ENTITLED TO PROCESSING

The Company uses the following contractual partners to perform tasks related to processing operations. The contracted partner acts as a so-called “processor”: it processes the personal data specified in this Notice on behalf of the Company.

The Company may only use processors providing sufficient guarantees, in particular in terms of expertise, reliability and resources, to implement appropriate technical and organisational measures to ensure compliance with the requirements of the GDPR, including the security of the processing. The specific tasks and responsibilities of the processor shall be governed by the contract concluded by the Company and the processor. Once the processing has been carried out on behalf of the Company, the processor shall, at the Company’s option, return or delete the personal data, unless Union or Member State law to which the processor is subject requires the storage of the data.

Where the contractual legal relationship between the service provider and the Company is terminated for any reason prior to the aforesaid data retention deadlines, the service provider shall transfer the data to the Company or to another contractual partner designated by the Company.

Processor	Activity
Rail Cargo Hungaria Zrt. registered seat: 1133 Budapest, Váci út 92. <u>email address:</u> cargo.rch@railcargo.com	Personal data: In relation to accounting services: Data and contact details of contractual partners (including data of the contact person and the representative), data required for performing taxation and accounting tasks. In relation to marketing services: Data and contact details of contractual partners (including data of the contact person and the representative). Activity performed by the processor, method of using personal data: providing accounting and marketing services.
Primelink Szolgáltató Korlátolt Felelősségű Társaság seat: 2721 Pilis, Bartók Béla utca 15 e-mail: kiss.richard.it@gmail.com	Personal data: data required for the proper operation and setting of IT systems. The activity performed by the data processor, the way in which the personal data are used: Provision of IT support Method of using data: Troubleshooting problems that arise.
Őrmester Vagyonvédelmi Nyrt. Security services <u>registered seat:</u> 1142 Budapest, Ógyalla tér 8-9. <u>phone:</u> +36-1 368 2002	Personal data: data required for performing security services, data of the persons entitled to enter, security camera recordings. Activity performed by the processor, method of using personal data: Security services Method of using data: Performing the company’s security activities.

6. DATA SECURITY (TECHNICAL AND ORGANISATIONAL) MEASURES

The Company protects the processed personal information primarily by restricting access to the information, and by clearly specifying the user rights. Access to the systems and means used for processing the personal data contained herein is restricted to those persons who need to have access to the data in order to achieve the aforementioned purposes and who have the proper authorisations. For example: designated administrators or teams (e.g. the IT department for the management of user data necessary for using the corporate computer systems).

In addition to the above, the Company protects its own information systems by using state-of-the-art firewall and anti-virus software with excellent market ratings and by archiving data from its systems according to its internal contingency plan (backup to storage, backup to tape and backup replication), which describes and helps to understand the structure of the internal IT system to ensure business continuity. In the event of a failure of an IT device, the destruction of data on the device will be carried out in accordance with the Company's internal regulations. In addition to this, the Company uses password protection, encryption and backups.

With regard to the physical protection of data, electronic and printed documents, the Company has premises with access cards, lockable server rooms and archives, and ensures that only the authorised persons have access to the documents (for example: the HR department to HR data). At the Company's headquarters, the management building can only be accessed by using magnetic cards and the terminal area is only accessible to authorised passenger vehicles - the area is protected by a gate.

7. DATA PROTECTION RIGHTS AND REMEDIES OF THE DATA SUBJECTS

7.1 Data protection rights and remedies

The data protection rights and remedies of the data subjects are contained in detail in the relevant provisions of the GDPR (in particular in Articles 15, 16, 17, 18, 19, 20, 21, 22, 77, 78, 79, 80 and 82 of the GDPR). The following summary contains the most important provisions, and the Company provides information accordingly to the data subjects in relation to their rights and remedies related to processing. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The Company shall inform the data subject on the measures taken as a result of the request related to the data subject's rights (see: Articles 15-22 of the GDPR) without unnecessary delay, within one month following the receipt of the request. If necessary, taking into account the complexity of the request and the number of requests, such deadline may be extended by another two months. The Company will inform the data subject on the extension of the deadline within one month following the receipt of the request, indicating the reasons for the delay. If the data subject has submitted the request electronically, the information will be provided electronically where possible, unless the data subject requests otherwise.

If the Company does not take action on the request of the data subject, the Company shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the competent data protection authority and of exercising the right to judicial remedy.

7.2 Right of access by the data subject

- (1) The data subject shall have the right to obtain from the Company confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
 - a) the purposes of the processing;
 - b) the categories of personal data concerned;
 - c) the recipients or categories of recipient to whom the personal data have been or will be disclosed by the Company, in particular recipients in third countries or international organisations;
 - d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - e) the existence of the right to request from the Company rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
 - f) the right to lodge a complaint with a supervisory authority; and
 - g) where the personal data are not collected from the data subject, any available information as to their source.
- (2) Where personal data are transferred to a third country, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.
- (3) The Company shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Company may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

7.3 Right to rectification

The data subject shall have the right to obtain from the Company without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

7.4 Right to erasure (“right to be forgotten”)

- (1) The data subject shall have the right to obtain from the Company the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:
 - a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - b) the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
 - c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
 - d) the personal data have been unlawfully processed;
 - e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Company is subject; or
 - f) the personal data have been collected in relation to the offer of information society services.
- (2) Where the Company has made the personal data public and is obliged pursuant to the above to erase the personal data, the Company, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the

personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

- (3) Paragraphs (1) and (2) shall not apply to the extent that processing is necessary:
- a) for exercising the right of freedom of expression and information;
 - b) for compliance with a legal obligation which requires processing by Union or Member State law to which the Company is subject;
 - c) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right referred to in paragraph (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
 - d) for the establishment, exercise or defence of legal claims.

7.5 Right to restriction of processing

- (1) The data subject shall have the right to obtain from the Company restriction of processing where one of the following applies:
- a) the accuracy of the personal data is contested by the data subject, for a period enabling the Company to verify the accuracy of the personal data;
 - b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
 - c) the Company no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or d) the data subject has objected to processing pending the verification whether the legitimate grounds of the Company override those of the data subject.
- (2) Where processing has been restricted under paragraph (1), such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
- (3) A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

7.6 Notification obligation regarding rectification or erasure of personal data or restriction of processing

The Company shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Company shall inform the data subject about those recipients if the data subject requests it.

7.7 Right to data portability

- (1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Company to which the personal data have been provided, where:
- a) the processing is based on consent or on a contract; and
 - b) the processing is carried out by automated means.

- (2) In exercising his or her right to data portability pursuant to paragraph (1), the data subject shall have the right to have the personal data transmitted directly from one controller to another (e.g. the Employer and other controllers), where technically feasible.
- (3) The exercise of the right referred to above shall be without prejudice to the provisions concerning the right to erasure (“right to be forgotten”), and this right shall not adversely affect the rights and freedoms of others.

7.8 Right to object

- (1) The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on legitimate interest. The Company shall no longer process the personal data unless the Company demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- (2) Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
- (3) Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
- (4) In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, you may exercise your right to object by automated means using technical specifications.
- (5) Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

7.9 Right to lodge a complaint with a supervisory authority

Every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the GDPR. In Hungary, the competent supervisory authority: Hungarian National Authority for Data Protection and Freedom of Information (website: <http://naih.hu/>; address: 1055 Budapest, Falk Miksa utca 9-11.; mailing address: 1363 Budapest, Pf. 9; phone: +36-1-3911400; fax: +36-1-391-1410; email: ugyfelszolgalat@naih.hu).

7.10 Right to an effective judicial remedy against a supervisory authority

- (1) The data subject shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning him or her.
- (2) The data subject shall have the right to an effective judicial remedy where the competent supervisory authority does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the lodged complaint.
- (3) Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

7.11 Right to an effective judicial remedy against the Company or the processor

- (1) Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under the GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with the GDPR.
- (2) Proceedings against the Company or the processor shall be brought before the courts of the Member State where the Company or the processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence. The competence and contact details of the courts are available on this website: www.birosag.hu.