Information on data processing during the guest/visitor entering process in the seat/business premises of KNORR-BREMSE Vasúti Jármű Rendszerek Hungária Kft.

Dear Visitor!

Welcome to the seat/business premises of KNORR-BREMSE Vasúti Jármű Rendszerek Hungária Kft. (Seat: H-1238 Budapest, Helsinki út 105.) In connection with personal data process hereby informs you about the followings:

Please read this leaflet carefully and at the end of this leaflet, please make a statement considering the processing of your personal data by marking the appropriate sections.

Thank you for your cooperation!

General Privacy Policy

KNORR-BREMSE Vasúti Jármű Rendszerek Hungária Kft. (Seat: H-1238 Budapest, Helsinki út 105.; Company Registry Number.: 01-09-464653; Tax number: 12089675-2-44, Phone number: +361-289-4100 hereinafter: Data Controller) is committed to ensure the protection of the personal data of persons wishing to enter its seat / business premises (hereinafter: Data Subjects), and attaches great importance to ensuring and respecting the right of self-determination of those concerned.

Only authorized person may enter the territory of KNORR-BREMSE Vasúti Jármű Rendszerek Hungária Kft. The necessary condition for entry is the use of the entry card provided by the Data Controller. Person who do not have a permanent entry card are obligated to request a guest card at the main entrances. Entry cards are issued by the Data Controller's security service after the verification of identity and made available free of charge.

In accordance with the pertaining legal provisions, we provide information on the processing of personal data that may arise in connection with the entry into the seat / business premises as follows:

Data Controllers: KNORR-BREMSE Vasúti Jármű Rendszerek Hungária Kft. (Seat: H-1238 Budapest, Helsinki út 105.; Company Registry Number.: 01-09-464653; Tax number: 12089675-2-44) and KNORR-Bremse Systeme für Nutzfahrzeuge GmbH (Seat: Germany, 80809 München, Moosacherstrasse Str. A 80.; Tax number: DE129395680; Company Registry Number: HRB 91181)
Representative of the Data Controller: László Veres managing director; Phone number: +36 70 320 6327; e-mail address: laszlo.veres@knorr-bremse.com

Description of data processing:

Authorization of the entry of the Data Subjects, identification of entering persons and the devices they intend to bring in, recording of the entry and exit data as well as internal movement data takes place in the computer system of the Data Controller. Recording of the data and the scope of the recorded data depend on whether or not the Data Subject's entry is subject to a separate permit under the internal regulations. For ease of transparency, each data treatment was recorded in a tabular form. Please note that the scope of the data processing depends on the type and circumstances of the access(es), not all data processing may be carried out for all Data Subjects.

During the entries, we distinguish three types of entry person:

Guest		For example, an official person (eg National Tax Authority, police), a job interview, a person entering for signing a contract, a language teacher, a trainer, etc.
Permission required guest		Person entering the seat and business premises of KNORR-BREMSE Vasúti Jármű Rendszerek Hungária Kft., arriving for non-work purposes.
Service Partner (and its employees)		Person working at the seat/business premises based on an ad hoc engagement agreement on behalf of a contractual partner who does not own a card in his / her own name.

1. Pre-registration of hospitality

Guests may only visit the seat/premise at the invitation of a Knorr-Bremse employee (Host employee). Not later than three working days prior to entering the seat/ business premise the host is obliged to request prior registration via the TopDesk IT system. The same rules apply to the reception of contractual partners who do not have a permanent entry card.

Pre-registration ensures the internal authorization process and facilitates / accelerate the registration of the entry, because at the actual entry the pre-recorded data can be retrieved from the system and the necessary documentation and entry card are prepared in advance. In the absence of pre-registration, access may be refused by the security service, exceptionally with the permission of the Security Manager, when this data will be recorded at the time of actual entry.

Description of data processing:	Scope of processed data	Purpose of data processing	Legal basis of data processing	Source of data	Recipients of processed data
Pre-registration of VIP hospitality	• name • number of an identity document • • purpose and date of the visit • company name • identification of thew host employee	Tracking of hospitality, internal allowance of entry and the facilitation and acceleration of entry	Legitimate interest: tracking of hospitality, internal allowance of entry and the facilitation and acceleration of entry	Host person	Security service provider as data processor
Pre-registration of guests and contractual partners	For guests: • Name • Company name • Date of arrival/departure	Tracking of hospitality, internal allowance of entry and the	Legitimate interest: tracking of hospitality, internal allowance of entry and the facilitation	Host person	Security service provider as data processor

	• Name and telephone number of host For Contractual Partner: • Host name and telephone number • Company name	facilitation and acceleration of entry	and acceleration of entry		

Pre-registration data will be retained from the time of registration until entry. In the absence of entry, the pre-recorded data will be deleted the day after the scheduled entry date.

2. Registration of entry and identification

Guest/ Service partners

Entry registration and identification is carried out at the main gate. If the pre-registration of VIP Guests has taken place before the entry, then the signing of the completed documentation and the receipt of the pre-prepared entry card is required only on the part of the guest.

In the case of guests and service partners who do not have a permanent entry card, all persons entering the premises are required to prove their identity by placing their identity document onto the MRZ code reader device (the documents are not recorded in any form, only certain data will be stored for identification purposes). Only the name, mother's name, date and place of birth, document number and expiration date are kept during the entry procedure.
During the entry, the entering guest views, acknowledges and accepts as binding the Labor Protection, Fire Protection, Property Protection and IT Security Regulations applicable to the Data Controller, the fact of which is confirmed by acknowledging them in the online surface.
In the event of a repeated visit – in case of previous consent for data processing -, Data Subjects are not required to any further registration.
The data of the IT device (manufacturer, type, serial number) that the entrant may want to bring in are also recorded in the same system and during the same process electronically or by filling in a paper-based import permission.
Upon entry, the person entering receives an entry card that secures and tracks their entry and traffic.

Permission required guests

Contractual partners (and their employees) who come to the Company's seat/business premises for the purpose of regular business may be issued with a permanent entry card. In such a case of need, a permanent entry card will be issued to the concerned party in accordance with internal procedures, which will enable the person concerned to enter the Company's seat/business premises through the turnstiles at the main gate or the turnstile at the street front by activating the entry card. If a person whose card has

been blocked by the system or a "red" signal is given due to a card failure wants to enter, access is only possible via the main gate.
In the event that a contractor forgets his/her entry card at home, he/she will not be allowed to enter the factory premises until the security service has checked in the system that he/she has a permanent entry card and has been issued with a temporary entry card for this purpose. Entry is only possible after this card has been scanned.

Description of data processing:	Scope of processed data	Purpose of data processing	Legal basis of data processing	Source of data	Recipients of processed data
Entry registration - in case of a guests/service quests Personal identification, access to identification document data	• name • place and date of birth • mother's name • number of an identity document • picture on the document • date of validity of the document • purpose and date of the visit • company name • identification of the host employee	Personal identification Tracking of hospitality and ensuring that only authorized persons are present at the seat / business premises	Legitimate interest: verification of the identity of person entering, tracking of hospitality and ensuring that only authorized persons are present at the seat / business premises	Data subject	Security service provider as data processor
Entry registration – - in case of a permission required guest	• name • photo suitable for face identification (in case of permanent card) • entry card number • organizational unit designated for contact • HR code number • registration number	Tracking of hospitality and ensuring that only authorized persons are present at the seat / business premises	Legitimate interest: tracking of hospitality and ensuring that only authorized persons are present at the seat / business premises	Data subject	Security service provider as data processor
Data of the electronic entry card – Permanent entry card	• name • photo suitable for face identification • entry card number • HR code number • registration number • department and manager • company name, address telephone number of the Partner • card validity • exact time of entry / exit • movement data within	Tracking entry and exit, where applicable, traffic within seat / business premises	Legitimate interest: monitoring of entry and exit and, where appropriate, monitoring of traffic at the seat / business premises	Data subject	Security service provider as data processor

	the seat / business premises ((passing through doors with card reader (terminal)) • where applicable, parking entitlement and parking entry and exit details				
Data of the electronic entry card – Single entry card	• name • purpose and date of visit • place and date of birth • mother's name • company name, if applicable • identification of the visiting employee • Card number • Exact date of entry/exit	Tracking entry and exit	Legitimate interest: monitoring of entry and exit	Data subject	Security service provider as data processor
Registration of devices brought in	• manufacturer • type • serial number	Tracking of electronic devices brought in	Legitimate interest: tracking of electronic devices brought in	Data subject	Security service provider as data processor
Entry registration for future occasions,	• name • place and date of birth • mother's name • number of an identity document • picture on the document • date of validity of the document • purpose and date of the visit • company name • identification of the host employee	Facilitating entry	consent	Data subject	Security service provider as data processor
Register of persons banned	• name • place and date of birth • mother's name	Tracking of hospitality and ensuring that only authorized persons are present at the seat / business premises	Legitimate interest	Data subject	Security service provider as data processor

We will keep your entry and personal identification data, as well as the movement data of your entry cards for three days, in case of consent twelve months from the date of leaving.
The data of the device brought in is retained until exit.

3. Registration of exit

If the visitor (who does not have a permanent entry card) is about to leave the seat/premise, he / she can exit with a card reader located at the main gate, which saves the exact time of exit (day, hour, minute) to the login data.

When checking the exit of a visitor who does not have a permanent entry card, the personal device declared at the time of entry is checked (no other data processing is carried out) by logging in the data recorded at the time of entry.

The exit of a permission required guest is checked as follows:
A random selection function is programmed on the card readers at the turnstiles. If the system gives a green signal to the person who is to exit, he/she can continue the exit process and, after providing a voluntary access to the contents of his/her bag, leave the factory premises without further control. If the person reporting for exit does not consent to the inspection of his/her bag, he/she will be escorted by the Security Service to the X-ray examination, which will allow the exit process to continue.

If the person wishing to exit receives red feedback from the system, in which case the exit will not take place, the person has to walk to the interior of the gate, where his/her bag or coat must be placed on the inlet roller line for X-ray package inspection. While the bag, jacket, and other belongings of the person selected for inspection is passing through the baggage screening, the inspected person must pass through a metal detector screening gate. If during the inspection neither the passage through the metal detector gate, nor the X-ray inspection of the package gives a reasonable suspicion that the inspected person tries to bring out items, devices and products belonging to the Company without permission, then the person selected for inspection may continue to exit through the internal rotating fork located in the room.
If, during the X-ray inspection of the package, there is a serious suspicion as to the content of the bag or jacket, the person selected for inspection shall be escorted by the security service to a separate camera-monitored room where he or she will be asked to empty his or her bag. If the attempted theft is proven, the security service will complete a theft report and immediately notify the Chief of Security, who will make a police report on the matter.
If no suspicion has been raised during the X-ray inspection of the package, but there is a continuous signal when passing through the metal detector gate, the security service will continue the investigation with a manual metal detector. If there is still an alert, the person selected for the check will be escorted by the security service to a separate room monitored by the camera, where he or she will be asked to empty his or her clothes. The abovementioned inspection is recorded in each case. If the attempt of theft is proven, the security service will complete a theft report and immediately notify the Chief of Security, who will make a police report on the matter.

In the event of suspicious behavior or the use of a bag larger than normal, the security service may instruct anyone to perform the X-ray examination, regardless of the result of system response.

Upon exit, the guest / contractual partner is obliged to present to the security service his / her own device or, in the case of a company device, the corresponding export license, and its identification data of which are verified by the security service. The control is carried out by inspecting the device data recorded at the time of entry, during which no personal data is processed. If the exiting person intends to bring out an asset that is not his or her property or a company asset for which he or she did not have an export license, the security service will keep a record about it and at the same time notify the Chief Security Officer.

Description of data processing:	Scope of processed data	Purpose of data processing	Legal basis of data processing	Source of data	Recipients of processed data
Exit registration	• exit time (day, hour, minute)	Tracking of entries and exits	Legitimate interest: monitoring of entry and exit, and ensuring that only authorized persons are present at the seat / business premises	Data subject	Security service provider as data processor
Recordkeeping in case of illegality	• name of the client company • date and description of the event • name of the guard acting • name and position of the person concerned and the name of his or her supervisor/ name of the company • data of witnesses • names and signatures of signatories	Tracking of entries and exits	Legitimate interest: monitoring of entry and exit, and ensuring that only authorized persons are present at the seat / business premises	Data subject	Security service provider as data processor

Exit time data is attached to and stored with the entry registration data. Device inspection shall be limited to the duration of the inspection, except in case of illegal exports. Recordkeepings of extraordinary events are retained for 5 years.

4. Possible checks during entry, exit and during the stay at the seat / business premises

It is forbidden to bring in to the seat/premise devices and items according to the information posted at the entrance of the facility. It is also forbidden to enter or stay under the influence of alcohol. Taking away of Knorr-Bremse-owned equipment and materials from its seat is also prohibited. Compliance with import and export restrictions and alcohol-free status may be monitored by the security services at both entry and exit and throughout the stay. Random checks of alcohol-free status are carried out among permission required guests in the entry card system. If the automated entry control system selects an entrant, the entrant shall be required to submit to an alcohol test. As part of the inspection, in case of suspicion, the security service may invite the person concerned to present the contents of his or her package or the trunk of his or her vehicle, and, in case of suspicion of alcohol consumption / intoxication, an alcohol may be initiated. Only a refusal to test or a test with a positive result is recorded.

Description of data processing:	Scope of processed data	Purpose of data processing	Legal basis of data processing	Source of data	Recipients of processed data
Checking of work ability conditions – possible record taking	• date • place of inspection • name, identification (if any), year of birth, position • test result, statements related to the inspection of the inspected person • name and identification of the person performing the inspection • data of the present witnesses • signatures	Checking of work ability conditions	Legitimate interest: ensuring personal and property security	Data subject	Security service provider as data processor
Checking of alcohol influence regarding contractual partner with permanent entry card – drunkenness inspection book	• registration number • date of inspection • name, year of birth, position of the inspected person • name and position of the person performing the inspection • test result (positive, negative)	Recording and monitoring of relevant inspections concerning alcohol-free status and drug use	Legitimate interest: ensuring personal and property security	Data subject	Security service provider as data processor
Clothing and package check registers, and	• date of inspection • name, identification (if any), signature of the inspected person • test result (positive,	Monitoring compliance with import and export	Legitimate interest: ensuring personal and	Data subject	Security service provider as data processor

recordkeeping	negative • name of the person performing the inspection	prohibitions	property security		
Inspection of car trunk, glove-compartment with introspection (only in case of recordkeeping)	• date of inspection • name, identification (if any), signature of the inspected person • test result (positive, negative) • name of the person performing the inspection	Monitoring compliance with import and export prohibitions	Legitimate interest: ensuring personal and property security	Data subject	Security service provider as data processor
Checking the contents of lockers in the premises (only if a record has been made)	• date of inspection • Name, identification (if any) of the inspected person or contracting partner • if he/she was present during the inspection, his/her comments and signature, • Name of the person performing the inspection	Monitoring compliance with import and export prohibitions	Legitimate interest: ensuring personal and property security	Data subject	Security service provider as data processor

We retain the alcohol test records and registered data for 5 years.
Package inspection records will be retained for 1 year.

5. Entry and exit of freight transport, related checks

During working hours, there is a continuous flow of lorries in and out of the Company's seat and business premises. The security service checks all unsealed vehicles entering and leaving the premises and compares the data on the delivery note with the material on the vehicle. During the inspection of lorries, the Company checks the identity of the driver int he An Guard software by reading the MRZ code on the personal identity card.
All lorries entering the territory of the Company must be subject to the AEO seven-point vehicle check.

The Security Guard checks in the presence of the driver the following:

- The driver's cab, the areas next to, in front of, under and between the seats
- Glove compartment
- The contents of compartments and boxes in the cab
- Open the trunk (for passenger cars)
- Exterior tool and other compartments of the vehicle
- The underside of the vehicle
- Spot check the engine compartment of the vehicle
- The integrity of the tarpaulin cover

- The integrity of the tarpaulin
- Integrity of the seals

The inspection itself does not involve the processing of personal data, but a record will be made if the goods to be exported are found to be different or if an infringement is suspected.

Description of data processing:	Scope of processed data	Purpose of data processing	Legal basis of data processing	Source of data	Recipients of processed data
Inspection documentation - Goods discrepancies report	• Check time • Identification of the vehicle being checked, • Inspection result (discrepancies with the consignment note) • Name of person carrying out the check • Signature of the driver	Recording of export discrepancies	Legitimate interest: investigating export discrepancies	Data subject	Security service provider as data processor
Checking the trunk and glove compartment of the vehicle, taking a report in case of infringement	• Check time • Identification of the vehicle checked • Result of check Name of person carrying out the check • -Driver's signature (in the absence of a signature, the fact that the signature has been withheld)	Monitoring compliance with import and export bans	Legitimate interest: ensuring the safety of persons and property	Data subject	Security service provider as data processor
Identifying the driver of lorry	• name • place and date of birth • mother's name • number of an identity document • picture on the document • date of validity of the document	Tracking of hospitality and ensuring that only authorized persons are present at the seat / business premises	Legitimate interest: ensuring the safety of persons and property	Data subject	Security service provider as data processor

6. Handling of found and retained objects, lockers

Description of data processing:	Scope of processed data	Purpose of data processing	Legal basis of data processing	Source of data	Recipients of processed data
Records of found objects	• name of the person recording the registration • name of the finder • object • exact location of reported event • name of other person concerned (possessor of found object)	Lawful treatment of found objects	Legitimate interest	Data subject	Security service provider as data processor
Records of retained objects	• name and date of birth of the person who owns the object, • position, • name of immediate superior • shift manager to be notified • employment status • name of employer • length of service	Protection of the Company's assets	Legitimate interest	Data subject	Security service provider as data processor
Checking the contents of lockers	• name of the locker user • any personal data according to the contents of the locker • names of persons involved in the service	Protection of the Company's assets	Legitimate interest	Data subject	Security service provider as data processor

The Company shall store the Found Objects for 30 days from the date of possession, after which it will arrange for their destruction. Thus, personal data are also kept in the relevant records for 30 days and then manually deleted, together with the corresponding record in electronic format.
The retained objects are stored from the moment of taking possession until their ownership is clarified, after which they are either returned to the competent territory of the Company or to the person concerned, at the

same time as the personal data are manually deleted from the register, together with the record in electronic format.
The objects found in the lockers shall be stored by the Company for 30 days from the date of taking possession of them, after which the Company shall arrange for their destruction. Thus, personal data will also be kept in the relevant records for 30 days and then manually deleted, together with a record in electronic format.

7. Complaint Handling

Any person entering the Company's premises, whether a Knorr-Bremse employee, other form of employment, contractor or visitor, has the right and opportunity to make a report to the Knorr-Bremse Security Manager.

Description of data processing:	Scope of processed data	Purpose of data processing	Legal basis of data processing	Source of data	Recipients of processed data
Proper investigation of complaints	• name • Position, • cost centre • workplace contact details	Proper investigation of complaints, improving the work of the guard service	Data subject's consent	Data subject	Security service provider as data processor

8. Providing parking possibilities for Service Partners

The Company provides parking facilities for its Service Partners in two external areas. Access to the parking places is possible with entry card along with the registration of the license plate. The license plate data is processed in the IT system of the Security Service.

Description of data processing:	Scope of processed data	Purpose of data processing	Legal basis of data processing	Source of data	Recipients of processed data
Provision of parking places	• name • license plate number • company name	provision of parking places	Data subject's consent	Data subject	Security service provider as data processor
Provision of parking spaces - electronic registration	(in addition to the access card system data recorded above) • license plate number • parking entry and exit data	provision of parking places	Data subject's consent	Data subject	Security service provider as data processor

9. Transmission of data of person acting on behalf of Service Partners to Service Partner

In the case of some of our Service Partners, the time of entry and exit (and internal movement) as personal data of the persons acting on behalf of the Service Partner between Knorr-Bremse as customer and the Service Partner as contractor / agent will be transferred to the Service Partner in order to validate the provided services which is the basis of the calculation pf remuneration of the Service Partner.
Accordingly, the entry and exit data of the person acting on behalf of the Service Partner and, if necessary, their internal movement data are transmitted to the Service Partner on a monthly basis.
With regard to the transmitted data, the Service Partner acts as an independent Data Controller, moreover, the Service Partner informs the persons acting on its part about the scope of the transmitted data, as well as about its own data processing purposes and its own data processing.

Description of data processing:	Scope of processed data	Purpose of data processing	Legal basis of data processing	Source of data	Recipients of processed data
Transmission of entry and exit (movement) data of person acting on behalf of a Service partner	• name • card number • actual monthly entry and exit as well as movement data	Ensuring settlement between the Data Controller and the Service Partner	Legitimate interest: fulfillment of the contract between the Data Controller and the Service Provider partner	Data subject	Security service provider as data processor Service partner as an independent Data Controller

For this purpose, the Data Controller will retain the data for six months, after which it will be automatically deleted.

10. Camera recordings

Only authorised persons may be present at the Company's headquarters and premises. The Company has a legitimate interest in ensuring that the Company's intellectual property and assets are properly protected. Outdoor and indoor cameras are installed at the Company's headquarters and premises as set out in the Camera Regulations. The surveillance of the camera system is carried out by the Security Service Provider on a 0-24 hours basis. Camera recordings are automatically deleted after a maximum of 30 days if they are not used. The recordings are stored on a dedicated internal server set up by the Company for this purpose, with appropriate IT protection, and access to the recordings is restricted and logged. Recordings may be kept for longer than 30 days in exceptional

cases, the fact of which shall be recorded in writing in all cases. The use of recorded images, sound or images and sound recordings and other personal data as evidence in judicial or other official proceedings shall be considered as use.

A person whose right or legitimate interest is affected by the recording of his or her image, sound or image and sound recording or other personal data may, within the erasure deadline, request that the data not be destroyed or erased by the controller by providing evidence of his or her right or legitimate interest. Thereafter, at the request of the court or other authority, the recorded image, sound, image and sound recording and other personal data shall be sent without delay to the requesting court or authority. If no request is made within thirty days of the request not to destroy, the recorded image, sound and image and sound recordings and other personal data shall be destroyed or erased.
The camera system is also capable of real-time monitoring.

The Company will place special notices in the affected areas to inform about the use of the cameras.

Description of data processing:	Scope of processed data	Purpose of data processing	Legal basis of data processing	Source of data	Recipients of processed data
Outside and inside Camera recordings	• the image and movement of the data subjects in the camera footage	Protection of persons and property, facilitating the investigation of incidents	Legitimate interest: The Data Controller has a legitimate interest in recording, being informed of, and taking the lawful and necessary measures to record events that deviate from normal operations on the factory premises it operates.	Data subject	Security service provider as data processor If used, the relevant authority (Police, Prosecutor's Office, Court)
Special Camera recordings (by fix position cameras and occasionally by body camera) at dispatcher centre and reception desks at the premises	• the image, voice and movement of the data subjects in the camera footage	Protection of persons and property, facilitating the investigation of incidents	Legitimate interest: The Data Controller has a legitimate interest in recording, being informed of, and taking the lawful and necessary measures to record events that deviate from normal operations on the factory	Data subject	Security service provider as data processor If used, the relevant authority (Police, Prosecutor's

			premises it operates.		Office, Court)
Internal call centre for notification of incidents	• provided personal data during the call: name, voice others.	Protection of persons and property, notification and facilitating the investigation of incidents	Legitimate interest: The Data Controller has a legitimate interest in recording, being informed of, and taking the lawful and necessary measures to record events that deviate from normal operations on the factory premises it operates.	Data subject	Security service provider as data processor If used, the relevant authority (Police, Prosecutor's Office, Court)

Recipients of processed data: During data processing, we use a data processor as follows:
Security Service: Securimaster Protect Plusz Kft. (Seat: H-1221 Budapest Duna utca 1-3, Company Registry Number: Cg: 01-09-324643; Phone number: 06-76/511 100, e-mail address: info@securimaster.com). The Data Processor acts in accordance with the instructions of the Data Controller, and shall not use the data for its own purposes or transfer them to other persons.
In addition to the above, the registration systems of KNORR-BREMSE Vasúti Jármű Rendszert Hungária Kft. - considering from the fact that the Company is part of an international group of companies – designed so that the parent company is entitled to access the data stored in the electronic systems. This is due to the fact that the parent company provides the software system at KNORR-BREMSE Vasúti Jármű Rendszert Hungária Kft. and the necessary servers and other IT conditions, so it shall be deemed as a joint Data Processor.

Retention times:

- detection and investigation of occupational accidents, traffic accidents: 5 working days,
- Detection and investigation of unlawful acts affecting the property of the Company and the property of employees, contractors, students and other visitors: 8 working days,
- Protection of the Company's trade secrets: 5 working days,
- Identification of employees, contractors, students and other visitors entering the company's seat/premises: 3 working days,
- Investigation of incidents, accidents, security breaches and disputes between persons at external and internal Company sites: 3 working days,
- During the qualitative and quantitative inspection of goods, raw materials and finished products received at the Company's seat/premises, the Company uses cameras to handle and prove subsequent complaints and quality objections: 30 days.

Your Rights in connection with the process of your personal data:

Your right to access: You have the right to request information on whether the Processor processes your data, and if there is such ongoing data procession you have the right to access personal data and information set out in acts. Based on it, you have right to contact the Processor and request information about your processed data and ask for access to your data.

Your right to rectification: You have the right to the correction of your personal data if it changes with announcing the right data at any time.

Your right to erasure ('right to be forgotten'): In cases when the data processing is not necessary anymore for the original purpose it has been collected, or when the data processing is against the law or when the cancellation of data is prescribed by law you are entitled to indicate the data cancellation to the Processor.

Your right to the restriction of processing: You have the right to indicate the restriction of processing if the data processing is against the law, and if the Processor does not need the data for data processing purposes but you intend to use them for a legal claim. The restriction of processing means that the data can be only stored until the cancellation of restriction, and it can be used only for submitting legal claims.

Your right to object: You have the right to object to the processing of your personal data for reasons connected to your own state at any time. In such cases the Processor examines individually whether there is any well-founded reason which justify the necessity of data processing or not.

Your right to data portability: You have the right to obtain personal data from the Processor pertaining to you in an articulated, commonly used form which can be read by machines. Moreover, you are entitled to transfer the abovementioned data to other processors without the inhibition of the Processor. Provided that it is technically achievable, during the exercising of the right of data portability you are entitled to indicate the direct transmission of personal data among processors.

Your right to lodge a complaint: You have the right to lodge a complaint to the Hungarian National Authority for Data Protection and Freedom of Information. (Contact information: H-1055 Budapest, Falk Miksa u. 9-11., +36-1-391-1400, ugyfelszolgalat@naih.hu)

Enforcement of claim in front of the court: You have the right to refer to the court if in your view the Processor or the Controller commissioned by the Processor process your personal data with an infringement of regulations pertaining to data processing.

Data safety

Data Controller ensures the safety of personal data. In respect of this, Data Controller performs the technical and organizational arrangements and forms procedural regulations which are necessary for the enforcement of precedent law, data and secret protection. Data Controller protects personal data from unauthorized access, alteration, transmission, disclosure, delete or destruction, as well as from involuntary destruction and damage, as well as from becoming inaccessible due to the change of applied new technology, with proper arrangements. Data Controller ensures the enforcement of the rules of data protection with the help of internal regulations, orders, procedural methods (among other things) which are stand apart from the General Privacy Policy and the information document herein. Data Controller while stipulating and applying the arrangements serving the safety of personal data, consider the all-time development of technology and out of several possible data processing methods, chooses the one which ensures the highest protection of personal data except if it causes disproportioned difficulty.

If you have any question regarding the processing of your personal data, contact us in the following e-mail address rudolf.gerendai@knorr-bremse.com . Our detailed Privacy Policy is also available at the seat of our Company and will be made available upon request.