REQUIRED DOCUMENTS FOR NEW EMPLOYEES

Copies!

Bank data (BIC & IBAN)

e-Card

Registration form

ID card/Passport

Criminal record extract

Confirmation

I hereby confirm that I, Sujita Kumar Sahu have received, taken note of and understood the following documents and declare that I will – where intended – complete and sign them and will comply with and observe their specifications.

1. Information documents on IT security
2. Data Protection Initiative
3. Emergency Information
4. US Export Regulation
5. Privacy policy
6. Code of Conduct in its current version
7. Compliance Directive in its current version

Vienna, 30/04/2024	
Place, Date	**Signature**

Data protection initiative: Data transfer – Declaration of consent by employees

KONTRON TRANSPORTATION GMBH and its employees shall comply with the provisions of the Austrian Data Protection Act when processing personal data electronically or manually. In particular, this includes the obligation to ensure the accuracy and timeliness of personal data and to secure and protect it against loss or unauthorized disclosure.

Personnel data is collected and maintained both manually and electronically in connection with your employment due to legal requirements. This includes, among others, the following terms

- **Personal data**

such as date and place of birth, citizenship, marital status, home address, telephone numbers, data of spouses and children, social security numerbs

- **Data of the personal career**

such as educational background, previous professional activities, previous functions in the company

- **Income data**

such as development of income, current income data, bank details, data of dependents, other information necessary for payroll accounting

- **Personnel development data**

such as courses attended, exam results, evaluations, career plans, feedback and survey data, records regarding disciplinary actions

The disclosure of the above data shall be made exclusively in accordance with the material provisions of the Austrian legal system and the provisions of the Austrian Data Protection Act.

The employee already now expressly declares his/her consent that KONTRON TRANSPORTATION GMBH is entitled to pass on the following information to customer and customer projects in any case: name, date of birth, nationality, if necessary information regarding work permit/residence permit, education level. However, the employee is entitled to revoke this authorization at any time.

In this context, it should also be noticed that it is the obligation of each individual employee to immediately notify Human Resources of any changes in personal data, such as home address, martial status, bank details, etc., and in this way contribute to keeping the records up to date.

By signing this form, I agree that KONTRON TRANSPORTATION GMBH may, in connection with the above circumstances, transfer my personal data within the KONTRON TRANSPORTATION GMBH **both within and outside the European Union,** if necessary, provided that KONTRON TRANSPORTATION GMBH ensures that the provisions of the Austrian Data Protection Act are complied with.

30/04/2024

Date

Signature of the employee

EMERGENCY ADDRESS - EMERGENCY INFORMATION

Sujita Kumar Sahu

Employee

To notify in case of emergency:

Name:	Ajit Kumar Sahu Last Name/First Name
Relationship with Employee(s):	Brother (Spouse/s, Life Partner/s, Father/Mother, Brother/Sister, etc.)
Phone number:	Private: +918928931007 or: +919437338304 During the Day: Anytime

or:

Name:	Asha Choudhury Last Name/First Name
Relationship with Employee(s):	Spouse (Spouse/s, Life Partner/s, Father/Mother, Brother/Sister, etc.)
Phone number:	Private: +436607405433 or: During the Day: Anytime

By submitting this form, I agree to the electronic processing of the above information.

Signature employee

Export regulation

Dear Employee,

Below you will find our applicable US Export Regulations. In case of non-compliance we reserve the right to take legal action.

1. US Export Regulations

We are required by our manufacturers to comply with US export regulations. This means that deliveries to Iran, Syria, Sudan, Libya (may soon come off the list) and Cuba cannot be made or can only be made after approval from the US authorities. Violation of this would have adverse business consequences because U.S. companies could lose their export licenses for violations. The noticeable effect for us would be that US manufacturers could consider whether they still supply us.
Deliveries to non-Black Listed Countries (see the 5 above) require approval in any case if we know that it is for biological, chemical or nuclear purposes (or related customers) or to military facilities (no matter where outside EU - Europe).

2. Denied persons list

The US foreign trade authorities regularly issue updated "Denied Persons Lists". US products may not be delivered to these persons. It will hardly surprise that you will find the entire staff of Al Qaeda and similar organizations on it. But there are also European persons or companies (also 2-3 Austrian companies/persons) on this list. As soon as your customer has an Arabic name and is completely unknown to you or something else seems strange to you, please exercise appropriate caution and inform yourself before making any commitments.

3. EU - export regulations

Dual-use items must be authorized if the consignee will use them for biological, chemical or nuclear facilities or if these items are to be used for military facilities (If the consignee is located outside the EU).

4. Arab boycott

There are partial boycotts by Arab countries on Israeli products. Should you come across such a deal, please inform yourself in time.

In all of the above cases, it is mandatory to contact the legal department before initiating the transaction and such a transaction may not be concluded without the consent of the management. The first two points in particular may have a detrimental effect on our business in the event of a violation.

If you have any questions, please contact our Legal Expert.

30/04/2024
Date

Acknowledgement and signature of the employee(s)

Data protection confidentiality declaration

Completed between

Kontron Transportation GmbH
Lehrbachgasse 11
1120 Vienna

(hereinafter "**KTAT**")

and

_____
First Name, Last Name
(hereinafter referred to as "**Employee**")

For ease of reading, the term "employee" refers to both female and male employees.

PREAMBLE

Within the scope of the employment relationship, the Employee obtains knowledge of personal and/or confidential data of KTAT and its clients.

Personal data means any data that identifies or makes identifiable a natural person ("personal data"). Confidential data shall be understood to mean all data relevant to business and trade secrets ("confidential data").

In dealing with them, the following applies as agreed below:

1. Confidentiality/data secrecy

The Employee undertakes to keep confidential the personal data disclosed to him from data processing entrusted to him exclusively on the basis of his professional employment, insofar as there is no legally permissible reason for transferring the personal data entrusted or to which access has been gained. In particular, the Employee undertakes to process the data of KTAT's clients exclusively on behalf of the respective client.

The Employee hereby declares that he/she has taken note of the relevant provisions of data protection law as set out in **Annex 1.**

2. Transmission

Personal data may only be transferred under the express order of the Employer or following the written order of the Client.

3. Guidelines

The Employee undertakes to comply with internal work instructions and guidelines regarding the processing of personal data. The Employee undertakes not to carry out any further processing.

4. Use of company property for private purposes

The use of company property (laptops, cell phones, etc.) for private purposes is permitted in compliance with data protection regulations. The use for private purposes does not affect KTAT's ownership of the devices.

KTAT shall not be liable for loss of or damage to the data stored by the Employee on the devices owned by KTAT which are not related to or in connection with his employment ("private data") during the term of employment.

Upon termination of the employment relationship and return of the devices, KTAT will delete all data, including private data, which is still stored on the device. The employee has no claim to the return of the data stored on the devices after they have been returned.

5. Additional explanations

The Employee undertakes to carefully safeguard the entrusted user passwords and other access authorizations. The service user acknowledges that it is expressly prohibited to

pass on personal access authorizations. This also includes user passwords, passwords and other access authorizations transmitted by customers.

All hardware and software installations are performed exclusively by the system administrators or require at least their prior approval. Thus, the employee is also not permitted to install his/her own software or games on the computers. In exceptional cases, and then only with the prior initial approval of the supervisor and further approval by the system administrators, employees may also use their own software. However, such software may only be installed by the system administrators. Approval must also be obtained from the system administration for shareware or freeware.

Furthermore, it is not permitted to store material protected by copyright on the company network. This applies especially to media material such as music (MP3), photos, videos, etc.

6. Duration of the confidentiality obligation

The obligation to maintain confidentiality shall continue indefinitely beyond the termination of the contractual relationship between the employer and the employee.

7. Final provisions

7.1. The Employee hereby declares that he/she has been informed of the consequences of breaching confidentiality, in particular of the data protection violations and fines the Company may face under the EU General Data Protection Regulation and the Data Protection Act.

7.2. The Employee acknowledges that the violation of his duties may result in administrative criminal law and criminal law consequences within the meaning of the Data Protection Act, as well as consequences under employment law.

The present data protection confidentiality declaration shall be issued in duplicate. The Employee shall receive one copy, the second copy shall be included in the Employee's personnel file at KTAT. Should further questions arise regarding data protection law**,** the employee may contact the management of KTAT.

Vienna, 30/04/2024	
Place, Date:	**Signature of the employee:**

Attachments:
Appendix 1 "Data protection regulations

Anlage 1 DATA PROTECTION REGULATIONS

Art. 4 EU General Data Protection Regulation

Z 1
"**Personal Data**" means any information relating to an identified or identifiable natural person (hereinafter "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Z 2
"**Processing**" means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, filing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

§ 6 Data Protection Act

(1) The controller, the processor and their employees - i.e. employees and persons in an employee-like relationship - shall keep personal data from data processing entrusted to them or made accessible to them exclusively on the basis of their professional employment confidential, without prejudice to other statutory confidentiality obligations, insofar as there is no legally permissible reason for transmitting the personal data entrusted or made accessible (data secrecy).
(2) Employees may only transmit personal data on the basis of an explicit order from their employer (Dienstgeber). The controller and the processor shall, unless such an obligation of their employees already exists by operation of law, contractually oblige them to transmit personal data from data processing only on the basis of instructions and to maintain data secrecy even after termination of the employment relationship (service relationship) with the controller or processor.
(3) The Controller and the Processor shall inform the employees affected by the order about the transfer orders applicable to them and about the consequences of a breach of data secrecy.
(4) Notwithstanding the constitutional right to issue instructions, an employee shall not suffer any disadvantage as a result of refusing to comply with an order to transfer data improperly.
(5) A statutory right to refuse to give evidence in favor of a data controller may not be circumvented by making use of a processor working for the data controller, in particular by seizing or confiscating documents processed with the aid of automation.

§ 62 Data Protection Act

(1) Unless the act constitutes an offence under Article 83 of the GDPR or is punishable by a more severe penalty under other administrative penal provisions, an administrative offence punishable by a fine of up to 50,000 euros shall be committed by anyone who
1. intentionally obtains unlawful access to data processing or intentionally maintains recognizably unlawful access,
2. intentionally transmits data in violation of data secrecy (Section 6), in particular intentionally processes data entrusted to him/her pursuant to Sections 7 or 8 for other unauthorized purposes,
3. intentionally obtains personal data pursuant to § 10 under false pretenses,

4. operates an image processing system in violation of the provisions of Section 3 of Chapter 1 or
5. refuses the inspection pursuant to § 22 par. 2.

(2) The attempt is punishable.

(3) Fines may be imposed on legal persons for administrative violations under subsections (1) and (2) in accordance with section 30.

(4) The penalty of forfeiture of data carriers and programs as well as image transmission and image recording devices may be pronounced (Sections 10, 17 and 18 VStG) if these objects are related to an administrative offense under subsection 1.

(5) The data protection authority shall be responsible for decisions under paragraphs 1 to 4.

§ 63 Data ProtectionAct

Whoever, with the intention of unlawfully enriching himself or a third party, or with the intention of damaging another person's rights as guaranteed by § 1 para. 1, uses, makes available to another person or publishes personal data which have been entrusted to him or have become accessible to him exclusively on the basis of his professional employment or which he has obtained unlawfully, although the person concerned has a confidentiality interest worthy of protection, shall be punished by the court with imprisonment of up to one year or with a fine of up to 720 daily rates, unless the act is punishable by a more severe penalty under another provision.