PRIVACY POLICY

Updated: 05/2018

Version: 1

I. OBJECTIVE

The shipping company undertakes to observe data protection as part of its corporate social responsibility. This privacy policy guarantees a uniform and high level of protection of personal data. To this end, this policy sets out basic rules for the handling of personal data and establishes an organisation for data protection.

II. SCOPE

The privacy policy applies to the shipping company F. Laeisz G.m.b.H. (hereinafter referred to as "shipping company"). It covers all processing of personal data of employees, suppliers and customers.

III. PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

1. Lawfulness

When processing personal data, the individual rights of the data subject must be respected. Personal data must be collected and processed in a lawful manner.

2. Purpose limitation

The processing of personal data may only take place for the legitimate purposes established prior to the collection of the data. Subsequent changes to the purposes are only possible to a limited extent and require a justification.

3. Transparency

The data subject must be informed about the handling of their data. In principle, personal data should be collected from the data subject themselves. When collecting the data, the data subject must at least be able to know the following or be informed accordingly of:

- the identity of the controller of the data file,
- the purpose of the data processing,
- third parties or categories of third parties to whom the data may be transmitted.

4. Data minimisation

Personal data must be reasonably and substantially limited to the purpose and extent necessary for the purpose of the processing.

5. Deletion

Personal data that is no longer required after the expiry of statutory or business process-related retention periods must be erased.

6. Factual accuracy and up-to-date data

Personal data must be stored correctly, completely and—if necessary—up to date. Appropriate measures must be taken to ensure that inaccurate, incomplete or outdated data is erased, corrected, supplemented or updated.

7. Confidentiality and data security

Personal data must be treated confidentially in personal dealings and kept secure through appropriate organisational and technical measures against unauthorised access, unlawful processing or disclosure, as well as loss, alteration or destruction.

IV. DEFINITIONS

- **Personal data** means any information relating to an identified or identifiable natural person. A person is identifiable, for example, if any relation to the person can be established by a combination of information with randomly available additional knowledge (examples: surname, first name, birthday, address data, e-mail content).
- **Special personal data** means data on racial and ethnic origin, religious or philosophical beliefs, trade union affiliations or on the health or sexuality of the data subjects.
- **Processing of personal data** means any operation performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, alteration, retrieval, use, disclosure, transmission, dissemination or combination and reconciliation. This also includes the disposal, deletion, and blocking of data and data carriers.
- **Transmission** means any disclosure of protected data by the data controller to third parties.
- **Consent** means a voluntary, legally binding declaration of consent to data processing.
- **Data subject** within the meaning of this privacy policy means any natural person whose data is processed.
- **Data protection incidents** mean any event in which there are reasonable grounds to suspect that personal data were unlawfully viewed, collected, altered, copied, transmitted or used. This may relate to actions by third parties as well as employees.
- **Data controller** means any person or body that collects, processes or uses personal data for themselves, or commissions others to do so on their behalf.

V. ADMISSIBILITY OF DATA PROCESSING

The collection, processing and use of personal data is only admissible if any of the following grounds for permission exist. Grounds for permission are also required if the purpose for the collection, processing and use of the personal data is to be changed from the original purpose.

1. Consent

Data processing may occur with the consent of the person concerned. Declarations of consent must be given voluntarily. Involuntary consent is ineffective. When obtaining consent, the person concerned must be informed that they can revoke their consent at any time with future effect. In principle, the declaration of consent must be obtained in writing or electronically for reasons of evidence.

2. Data processing to fulfil a contract or to carry out pre-contractual measures

Personal data of the supplier, customer or contract partner may be processed to establish, implement and terminate a contract or a pre-contractual business relationship.

Personal data necessary for establishing, executing and terminating an employment contract may be processed for employment purposes. The personal data of job applicants may be processed during the initiation of an employment relationship. After rejection, the applicant's data must be deleted, taking into account the deadlines for evidence, unless the applicant has consented to further storage for a later selection process. Consent is also required for the data to be used for further application procedures or before the application is passed on to other group companies. In existing employment relationships, data processing must always be related to the purpose of the employment contract. If collecting further data about the job applicant from a third party is necessary during the initiation of an employment relationship or during an existing employment relationship, the respective statutory requirements must be followed. In case of doubt, the data subject's consent must be obtained. The processing of personal data in the context of employment that does not, however, serve the fulfilment of the employment contract must have a legal justification. These can be statutory requirements, collective agreements with employee representatives, the employee's consent or the legitimate interests of the company.

3. Data processing to fulfil a legal obligation

The processing of personal data is admissible if national legislation requires, prescribes or permits it. The nature and extent of the data processing must be in line with what is necessary for the legally admissible data processing and is governed by these statutory provisions.

4. Data processing to protect vital interests

The processing of personal data is lawful insofar as this is necessary to protect the vital interests of the data subject or another natural person.

5. Consideration of legitimate interests

A legitimate interest in the processing of personal data includes the legal, factual, economic or moral interest of the shipping company, which must be weighed up comprehensively, in particular in light of the purpose of the data processing and the nature and content of the data concerned. The interests or fundamental rights and freedoms of the data subject must not outweigh this.

6. Processing of special categories of personal data

The processing of special categories of personal data for employment purposes is permitted if it is necessary for the exercise of rights or for the fulfilment of legal obligations arising from employment law, social security and social protection law and if there is no reason to assume that the data subject's legitimate interest in the exclusion of the processing prevails.

VI. COMPANY DATA PROTECTION OFFICER

The shipping company has appointed a company data protection officer (DPO) in accordance with the GDPR.

The DPO performs the tasks assigned to them by law and under this Directive with the application of their expertise free from instructions.

The DPO alone is responsible for reports, information, etc. to the data protection supervisory authorities. The specialist departments shall provide the information, documents, etc. required for this. The same applies to inquiries, complaints or access requests.

Any shipping company employee can contact the DPO directly with information, suggestions or complaints.

VII. OBLIGATION TO MAINTAIN DATA CONFIDENTIALITY

Every shipping company employee who is involved in the processing of personal data must be bound in writing to data confidentiality and compliance with this policy when taking up their duties.

VIII. TRANSMISSION OF PERSONAL DATA

The transmission of personal data to recipients outside the shipping company or to recipients within the F. Laeisz Group is subject to the conditions of admissibility of the processing of personal data under Section V. The recipient of the data must be obligated to use it only for the specified purposes.

IX. DIRECTORY OF PROCESSING ACTIVITIES

The processing directory serves to ensure transparency about the processing of personal data. The shipping company is obligated to keep a record of processing activities. The directory summarises the essential information on data processing activities, in particular information on the purpose of the processing and a description of the categories of personal data, the data subjects and the recipients.

X. DATA PROTECTION IMPACT ASSESSMENT

A data protection impact assessment must always be carried out when special personal data is processed or the data processing is intended to evaluate the personality of the person concerned, including their abilities, performance or behaviour. In these cases, the DPO examines the particular risks inherent in the procedure for the rights and freedoms of the data subject and at the end of this examination gives an opinion on the legality of the data processing.

XI. RIGHTS OF DATA SUBJECT AND ASSERTION

Every data subject can exercise the following rights. Any exercise of these rights must be immediately handled by the responsible department of the shipping company and must not result in any disadvantages for the data subject.

1. Rights

a) The data subject can request in writing information about if and which personal data of which origin is being stored about them for which purpose. Any further rights enshrined in the employment relationship according to the respective employment law to access documents held by the employer (e.g. personnel file) remain unaffected.

b) Information must also be provided about the identity of the recipient or categories of recipients if personal data is transmitted to third parties.

c) The data subject may request incorrect or incomplete data to be corrected or supplemented.

d) The data subject is entitled to request erasure of their data if there is no legal basis for processing the data or if the legal basis no longer applies. The same applies if the purpose of the data processing is no longer valid because it has expired or for any other reason. Existing data retention requirements and any interests warranting protection contrary to erasure must be observed.

e) The data subject has the right to receive the personal data concerning them in a structured, common and machine-readable format.

f) The data subject has a fundamental right to object to the processing of their data, which must be taken into account if, due to special personal circumstances, their interest warranting protection outweighs the interest in processing the data. This does not apply if the processing is mandatory due to a legal requirement.

2. Assertion (procedure)

When a data subject exercises their right of access, the information to be provided must be made available to them without delay and in any event within one month of receipt of the request. In complex cases, this period may be extended by two months. The data subject must be informed of any extension of the deadline, stating the reasons for the delay, within one month of receipt of the application. The information may be provided in writing, electronically or verbally at the request of the data subject. If the information is provided verbally, the identity of the data subject must, however, be proven by other means. If the data subject applies for information electronically, the information to be made available must be made available in a common electronic format (e.g. as PDF).

XII. SECURITY OF THE PROCESSING OF PERSONAL DATA

Personal data must be protected at all times against unauthorised access, unlawful processing or disclosure, as well as against loss, falsification or destruction. This applies regardless of whether the data processing is done electronically or in paper form. Before the introduction of new data processing procedures, especially new IT systems, technical and organisational measures to protect personal data must be defined and implemented. These measures must regard the state of the art, the risks arising from processing and the protection requirements of the data. The technical and organisational measures to protect personal data are part of information security and must be continuously adapted to technical developments and organisational changes.

XIII. DATA PROTECTION CHECKS/DATA PROTECTION TRAINING

Compliance with the privacy policy and the applicable data protection laws are regularly checked through data protection audits and other checks. The DPO is responsible for implementation. In addition, the DSPO conducts regular training courses to raise awareness among the shipping company's employees.

XIV. NOTIFICATION OF DATA PROTECTION VIOLATIONS

In the event of a breach of the protection of personal data, the breach must be reported to the competent supervisory authority without delay, if possible, within 72 hours after the breach became known. A report can be dispensed with if the breach of the protection of personal data is not likely to pose a risk to the rights and freedoms of natural persons. If there is a high risk to personal rights and freedoms, those affected must also be informed. To be able to comply with these obligations to report or inform, the breach of personal data protection must be detected, the facts of the case must be forwarded to the DPO and subsequently assessed by them. The following information must be reported to the responsible supervisory authority:

- Type of violation of the protection of personal data (categories, number of persons concerned)
- The nature of the breach of personal data protection (categories, number of persons concerned)
- Description of the likely consequences
- Description of the measures taken or proposed
- If necessary, measures to mitigate the adverse effects