BUHLMANN
TUBE SOLUTIONS

# Data Protection Guidelines

# Forward

Ladies and Gentlemen,

As a globally operating company it is our aim to comply with the legal requirements associated with the collection and processing of personal data, because data privacy is personal privacy.

In our Data Protection Guidelines, we have defined strict requirements for the processing of personal data of our customers, prospects, business partners and employees. It complies with the requirements of the European Data Protection Directive and ensures compliance with the principles of applicable national and European data protection laws. As a benchmark, we have defined seven privacy principles

– including transparency, data economy and data security.

Our executives and employees are required to adhere to these Data Protection Guidelines the respective data protection legislation.

I am pleased to be your contact at BUHLMANN for any questions relating to data protection and data security.

Sven Ladewig

Data Protection Officer

# Contents

# I. Aim of the Data Protection Guidelines

These Data Protection Guidelines applies to all BUHLMANN Group companies worldwide and is based on globally accepted basic data protection principles. The protection of privacy, among other things, forms the basis for trusting business relations and the reputation of the BUHLMANN Group as an attractive employer.

As one element of its social responsibility, the BUHLMANN Group is committed to international compliance with data protection laws.

These Data Protection Guidelines guarantees the appropriate level of data protection for international data traffic, as demanded by the European Data Protection Directive and other national laws, even in those countries in which there is no appropriate level of legal data protection.

# II. Scope of the Data Protection Guidelines

The Data Protection Guidelines applies to all BUHLMANN Group companies, i.e. to *BUHLMANN Rohr-Fittings-Stahlhandel GmbH + Co. KG* and all its dependent group companies, as well as affiliated companies and their employees. The Data Protection Guidelines encompasses the processing of personal data. In countries where the data of legal entities are protected in the same way as personal data, these Data Protection Guidelines applies equally to the data of legal entities. Anonymised data, for example for statistical analyses or investigations, are not subject to these Data Protection Guidelines.

The most recent version of the Data Protection Guidelines can be found under the Data Protection Guidelines notes on the BUHLMANN Group website at www.buhlmann-group.com.

# III. Applicability of National Law

These Data Protection Guidelines is based on the principles of data protection practised worldwide without replacing existing national law. It supplements the respective national data protection legislation. The respective national law is applicable if it requires deviations from these Data Protection Guidelines or if it makes more stringent demands. The contents of these Data Protection Guidelines must be observed even if there is no corresponding national law. The data processing reporting obligations under national law must be observed.

Every BUHLMANN Group company is responsible for complying with these Data Protection Guidelines and the legal obligations. If there is reason to believe that the legal obligations conflict with the obligations of these Data Protection Guidelines, the group company concerned must immediately inform the Data Protection Officer. In the event of a conflict between national legislation and the Data Protection Guidelines, BUHLMANN R-F-S will work with the affected group company to seek a workable solution in line with the Data Protection Guideline's objectives.

# IV. General Principles

## 1. Data Avoidance and Data Economy

Prior to processing personal data, whether and to what extent they are necessary in order to achieve the intended purpose of the processing must be examined. If it is possible to achieve the purpose, and the effort is proportionate to the intended purpose, anonymous or statistical data shall be used. Personal data may not be stored for future potential use unless this is either required or permitted by national law.

## 2. Confidentiality and Data Security

Personal data is subject to data secrecy. They must be treated confidentially in personal dealings and secured by appropriate organisational and technical measures against unauthorised access, unlawful processing or disclosure, as well as against accidental loss, alteration or destruction.

## 3. Dedicated Purpose

Personal data may only be processed for the purposes set out prior to data collection. Subsequent changes in the purpose are only possible to a limited extent and require justification.

## 4. Fairness and Legality

When processing personal data, the personal rights of the data subject must be respected. Personal data must be collected and processed legally and fairly.

## 5. Transparency

The data subject must be informed about the use of personal data. In principle, personal data must always be collected from the data subject. When collecting the data, the data subject must at least be able to recognise the following or be informed accordingly:
- The identity of the responsible agency.
- The purpose of data processing.
- Third-parties or categories of third-parties to which the data are transmitted.

## 6. Data Accuracy and Relevance

Personal data are correct, complete and – as far as necessary – up-to-date. Appropriate measures must be taken to ensure that any inaccurate, incomplete or outdated data is erased, corrected, supplemented or updated.

## 7. Deletion

Personal data that are no longer required after expiry of legal or business process-related retention periods must be deleted.

# V. Data Processing Legitimacy

Personal Data

Personal data are individual details about personal and factual circumstances of a particular or an identifiable person. This includes information such as your real name and surname, your address, your telephone, telefax and mobile phone numbers, email address or your birthday and any other data. Information that is not directly associated with you, such as the number of users of a website, on the other hand, is not personal data.

The collection, processing and use of personal data is only permitted if one of the following authorisations exist. Such authorisation is also required if the purpose of the collection, processing and use of the personal data is changed compared to the original purpose.

## 1. Customer Data

### 1.1 Data Processing for Contractual Agreements

Personal data of the prospect or customer may be processed for the establishment, implementation and termination of a contract. This also includes support of the contracting party, if this is in connection with the purpose of the contract. In the run-up to a contract – that is, during the contract preparation phase – the processing of personal data for the preparation of offers, the preparation of purchase requests or for fulfilling any other wishes of the prospective customer aimed at completing the agreement is allowed. Prospects may be contacted during the agreement preparation process using the data they have provided. Any restrictions expressed by prospects must be observed.

### 1.2 Data Processing for Advertising Purposes

If the data subject approaches a BUHLMANN Group company with a request for information (e.g. requesting the sending of information material on a product), data processing is allowable in order to fulfil this request.

### 1.3 Consent to Data Processing

Data processing can take place on the basis of the consent of the persons concerned. Prior to giving consent, the data subject must be informed in accordance with IV.3. of these Data Protection Guidelines. For the purpose of evidence, the declaration of consent must always be obtained in writing or electronically. In some circumstances, e.g. in the event of telephone advice, consent may also be given verbally. Granting of the consent must be documented.

### 1.4 Data Processing Based on Legal Permission

Processing of personal data is also permissible where national legislation demands, requires or authorises such data processing. The nature and extent of data processing must be necessary for legally permissible data processing and are governed by such legislation.

### 1.5 Data Processing Based on Legitimate Interest

Personal data may also be processed inasmuch as this is necessary for the realisation of a legitimate BUHLMANN Group interest. Legitimate interests are generally legal (e.g. enforcement of outstanding claims) or economic (e.g. to prevent contractual disputes) in nature. Personal data may not be processed based on a legitimate interest if, in individual cases, there is an indication that the interests of the data subject that are worthy of protection outweigh the interest in processing. The interests worthy of protection must be examined for each processing instance.

### 1.6 Processing of Particularly Sensitive Data

Particularly sensitive personal data may only be processed if this is legally required or the data subject has expressly consented to this. Processing such data is also permissible if it is absolutely necessary in order to assert, exercise or defend legal claims against the data subject. If the processing of particularly sensitive data is planned, the Data Protection Officer must be informed in advance.

### 1.7 User Data and the Internet

If personal data is collected, processed and used on websites, the concerned persons must be informed about this in the Data Protection Guidelines. The privacy notices must be integrated in such a way that they are easily recognisable, immediately accessible and constantly available to those affected.

## 2. Employee Data

### 2.1 Data Processing for Employment Purposes

Personal data may only be processed for employment purposes if they are necessary for the creation, implementation and termination of the employment contract. When preparing for an employment relationship the applicant's personal data may be processed. Following rejection, the applicant's data must be deleted, taking into account evidence-related periods, unless the applicant has consented to further storage for a later selection process. Consent is also required to use the data for further application procedures.

In an existing employment relationship, data processing must always be based on the purpose of the employment contract, unless one of the subsequent authorisations for data processing acts.

If, during preparation for the employment relationship or in an existing employment relationship, further information about the applicant must be collected from a third party, the respective national legal requirements must be taken into account. In case of doubt, the consent of the data subject must be obtained.

Legal legitimation is necessary to process personal data related to the employment relationship, but not originally intended to fulfil the employment contract. This may involve legal requirements, the consent of the employee or the legitimate interests of the company.

### 2.2 Data Processing Based on Legal Permission

Processing of personal employee data is also permissible where national legislation demands, requires or authorises such data processing. The nature and extent of data processing must be necessary for legally permissible data processing and are governed by such legislation. If there is legal room for manoeuvre, the employee's interests worthy of protection must be taken into account.

## 2.3 Consent to Data Processing

Employee data processing can take place on the basis of the consent of the persons concerned. Declarations of consent must be voluntary. Involuntary consent is thus void. For the purpose of evidence, the declaration of consent must always be obtained in writing or electronically. In exceptional cases consent can also be given verbally. Granting of consent must always be correctly documented. In the event of an informed voluntary disclosure of data by the data subject, consent may be accepted if national law does not require explicit consent. Prior to giving consent, the data subject must be informed in accordance with IV.3. of these Data Protection Guidelines.

## 2.4 Data Processing Based on Legitimate Interest

Personal employee data may also be processed inasmuch as this is necessary for the realisation of a legitimate BUHLMANN Group interest. Legitimate interests are usually legal in nature (e.g. the assertion, exercise or defence of legal claims).

Personal data may not be processed based on a legitimate interest if, in individual cases, there is an indication that the interests of the employee that are worthy of protection outweigh the interest in processing. Any interests worthy of protection must be examined for each processing instance.

Control measures that require employee data to be processed may only be performed if there is a legal obligation or there is reason to do so. Even if there are reasonable grounds, the proportionality of the control measure must be examined. The legitimate interests of the company in carrying out the control measures (for example, compliance with legal provisions and internal company regulations) must be weighed against any legitimate interest of the employee affected by the measure to be excluded from the measure and may only be implemented where appropriate. The legitimate interest of the company and the possible legitimate interests of the employee must be determined and documented prior to each measure. In addition, any additional requirements under national law (e.g. information rights of the persons concerned) must be taken into consideration, where necessary.

## 2.5 Processing of Particularly Sensitive Data

Particularly sensitive personal data may only be processed under certain conditions. Data that are particularly worthy of protection are data on racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union affiliations or the health or sexual life of the data subject. Additional data categories may be classified as eligible for protection under national law or the content of the data categories may be differently defined. Similarly, data concerning offences may often only be processed under specific conditions defined under national law.

Processing must be expressly allowed or required by national law. In addition, processing may be permitted if necessary to enable the responsible agency to fulfil its rights and obligations under employment law. The employee may voluntarily expressly consent to processing.

If the processing of particularly sensitive data is planned, the Data Protection Officer must be informed in advance.

### 2.6 Telecommunications and the Internet

Telephone systems, email addresses, Intranet and Internet are primarily provided by the company to perform tasks defined by the company. They are employment tools and a corporate resource. They may be used within the scope of applicable laws and corporate policies. In the case of permitted use for private purposes, telecommunications secrecy and the respective national telecommunications law must be observed, as far as they are applicable.

General monitoring of telephone and email communications or Intranet and internet usage is not permitted. To guard against attacks on the IT infrastructure or on individual users, protective measures, which block technically damaging content or analyse the patterns of attacks, may be implemented at the interfaces into the BUHLMANN Group network. For reasons of security, the use of telephone systems, email addresses, the Intranet and the Internet, as well as internal social networks may be logged for a limited period of time. Personalised analyses of these data may only be carried out in the case of a concrete and reasonable suspicion of a violation of the law or BUHLMANN Group guidelines. These examinations may only be carried out by means of investigating departments, while respecting the principle of proportionality. The respective national laws must be observed, as well as existing BUHLMANN Group regulations.

## VI. Transfer of Personal Data

Transfer of personal data to recipients outside or inside the BUHLMANN Group is subject to the admissibility requirements for the processing of personal data under Section V. The recipient of the data must be obliged to use them only for the specified purposes.

In the case of a data transfer to a recipient outside the BUHLMANN group in a third country, the latter must ensure a level of data protection equivalent to these Data Protection Guidelines. This does not apply if the transfer is a result of a legal obligation. Such a legal obligation may arise from the law of the country of incorporation of the company transferring the data, or if the law of the country of incorporation recognises the objective of the transfer of the data pursued by the legal obligation of a third country.

In the case of data transmission from third parties to companies in the BUHLMANN Group, it must be ensured that the data may only be used for the intended purposes.

If personal data are transmitted from a group company domiciled in the European Economic Area to a group company located outside the European Economic Area (third country), the company importing the data is obliged to cooperate with the supervisory agency responsible for the company exporting the data and to observe the findings of the supervisory agency with regard to the transferred data. The same applies to data transfers by group companies from other countries.

## VII. Order Data Processing

Order data processing occurs when a contractor is commissioned with the processing of personal data without being given responsibility for the associated business process. In these cases, an order data processing agreement must be concluded both with external contractors and between companies within the BUHLMANN Group. The commissioning

company retains full responsibility for the correct data processing execution. The contractor may only process personal data in accordance with the client's instructions. When placing the order, the following requirements must be met; the commissioning department must ensure their implementation.

1. The contractor shall be selected according to their suitability to guarantee the necessary technical and organisational protection measures.
2. The contract shall be awarded in written form. The data processing instructions and the responsibilities of the client and the contractor must be documented.
3. The contract standards provided by the Data Protection Officer must be observed.
4. The client must be satisfied prior to commencing data processing that the contractor adheres to their obligations. Compliance with the data security requirements can be demonstrated by a contractor, in particular by submitting appropriate certification. Depending on the risk involved in data processing, the audit may need to be repeated regularly during the contract period.
5. In cross-border order data processing, the respective national requirements for the transfer of personal data abroad must be met.

# VIII. Rights of the Data Subject

Each data subject may exercise the following rights. Their assertion must be processed immediately by the responsible department and must not lead to any disadvantages for the data subject.

1. The data subject can request information about the origin and purpose of the stored personal data. If, according to the employment law affecting the respective employment relationship, further rights of inspection of documents held by the employer are granted (for example personal file), these rights remain unaffected.
2. If personal data are transmitted to third parties, information must also be provided on the identity of the recipient or on the categories of recipients.
3. If personal data is incorrect or incomplete, the data subject may request their correction or supplement.
4. The data subject is entitled to request the deletion of his data if there is no legal basis for processing the data or the legal basis has been removed. The same applies in the event that the period of the purpose of data processing has expired or is absent for other reasons. Existing storage requirements and protection against deletion if this would harm the protected interests of the data subject must be observed.
5. The data subject has a fundamental right of objection to personal data processing, which must be taken into account if the protected interest outweighs the interest in the processing as a result of a special personal situation. This does not apply if there is a legal obligation to carry out the processing.

In addition, any data subject may utilise the rights furnished in No. III. Para. 2, IV., V., VI., IX., X and XIV. Para. 3, as third party beneficiaries if a company that has undertaken to comply with the Data Protection Guidelines fails to comply with its requirements and they thereby are injured in their rights.

## IX. Data Processing Confidentiality

Personal data are subject to data secrecy. Unauthorised collection, processing or utilisation is prohibited to employees. Any processing performed by an employee without being expressly entrusted with and entitled to perform in the course of normal duties is unauthorised. The *needtoknow* principle applies: Employees may only access personal information if, and to the extent, necessary for their respective duties This requires the careful division and separation of roles and responsibilities as well as their implementation and maintenance in the context of authorisation concepts.

In addition, all Human Resource Department and Legal Department data are encrypted.

Employees may not use personally identifiable information for their own private or business purposes, transmit it to unauthorised persons or make it accessible in any other way. Supervisors must inform their employees about the duty to maintain data secrecy when starting their employment. This obligation continues even after termination of employment.

## X. Processing Security

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 data processing is done digitally or in paper form. Before introducing new data processing techniques, in particular new IT systems, technical and organisational personal data protection measures must be established and implemented. These measures must be based on best practice, the risks posed by processing and the need for data protection. The technical-organisational personal data protection measures form part of Group-wide information security management and must be continuously adapted to technical developments and organisational changes.

## XI. Data Protection Controls

Compliance with Data Protection Guidelines and applicable privacy laws is regularly reviewed through audits. Implementation is the responsibility of the Data Protection Officer or commissioned external auditors. The results of the data protection audits must be reported to the data protection officer. Management shall be informed about significant results within the scope of the respective reporting obligations. The results of data protection audits will be made available to the relevant data protection supervisory agency on request. The relevant data protection supervisory agency may also carry out its own audits of compliance with the provisions of this Directive, within the limits of its powers under national law.

## XII. Data Protection Breaches

Each employee should immediately report violations of these Data Protection Guidelines or other personal data protection legislation to their respective supervisor or the Data Protection Officer. The responsible executive is obliged to inform the responsible Data Protection Officer immediately about any data protection incidents.

In cases of:

» unlawful transfer of personal data to third parties,

» unlawful access to personal data by third parties, or

» the loss of personal data,

the notifications provided for within the company must be made without delay in order to ensure that the reporting obligations of data protection incidents under state law can be met.

## XIII. Responsibilities and Sanctions

The managements of the Group companies are responsible for data processing in their areas of responsibility. This obliges them to guarantee that data protection requirements specified in the Data Protection Guidelines and in law are taken into account (e.g. national reporting obligations). It is an executive management duty to guarantee proper data processing while observing data protection by organisational, personnel and technical measures. The respective employees are responsible for the implementation of these specifications. The Data Protection Officer must be informed immediately of data protection audits by government agencies.

## XIV. Data Processing Directory

BUHLMANN Group will maintain a directory of all processing operations that collect, process or store personal data. In each department, at least one person will be responsible for collecting the required information from the department concerned and sending it to the Data Protection Officer.

The latter will collect the information and document it in a processing list in accordance with the requirements of Art. 30 DS-GVO.

The company will make the directory available to the competent supervisory agency on request. In agreement with management, the data protection officer is responsible for this and cooperates with the supervisory agency.

## XV. The Data Protection Officer

BUHLMANN Group has appointed a company Data Protection Officer in accordance with Article 37 DS-DVO.

The Data Protection Officer, as an internal, non-technical body, works towards compliance with national and international data protection regulations. The Data Protection Officer is responsible for data protection and monitors compliance. The Data Protection Officer is appointed by BUHLMANN Group management.

Any data subject may contact the Data Protection Officer with suggestions, requests for information or complaints in connection with data protection or data security issues. Enquiries and complaints are treated confidentially on request.

If the Data Protection Officer cannot remedy a complaint or stop a violation of the Data Protection Guidelines, management must be engaged.

The contact details of the BUHLMANN Group Data Protection Officer are: BUHLMANN Rohr-Fittings-Stahlhandel GmbH + Co. KG

Data Protection Officer

Arberger Hafendamm 1, 28309 Bremen, Germany

Email: Datenschutzbeauftragter@buhlmann-group.com