

## **Information on the tasks and responsibilities of employees for protection of personal data**

Within the framework of the implementation of the new European Data Protection Regulation ("GDPR") end of May 2018, in our group of companies a new data protection policy and a new data protection management system was introduced, which defines standards and processes to ensure that the processing of personal data in our companies meets our own high requirements and the legal requirements for data protection and data security, thus, permitting also a secure data exchange between the companies in our Group and between us and our partners across national borders.

In order to guarantee these data protection and data security standards and processes, the company relies on the cooperation of the employees; compliance with these requirements is, therefore, essential. Lack of compliance may lead to damage as well as to criminal and civil liability on the part of employers and employees.

In view of this, all staff are requested to read this information sheet carefully and to subsequently abide with the regulations contained.

### **Which personal data we process in our company:**

In our company, we process personal data concerning employees, customers and suppliers.

This includes first names, last names, birth dates, employee gender and language information, e-mail addresses, telephone numbers, tax numbers, images, bank details, credit card numbers, postal addresses, passwords, professional qualifications, performance evaluations, salaries, travel data, access data at entrances with access control, insurance data, data from surveillance cameras, company figures and sales data from partners.

### **Purposes of the processing of personal data:**

We need to process this information to enable smooth business operations, protect our IT communications system, manage our working relationships, enable collaboration with our customers and suppliers and fulfill the respective contracts.

### **Data processing method:**

The data protection regulations apply equally to processing of personal data by automated or non-automated means.

The term "data processing" is to be interpreted in a broad way including the collection, recording, organization, arrangement, storage, adaptation or modification, reading, querying, use, disclosure by transmission, disclosure or any other form of provision, comparison or linking, restriction, erasure or destruction.

### **Duties and obligations of staff members for the protection of personal data**

The new data protection regulations stipulate that the processing of personal data is only permitted for specified explicit purposes for which those data were collected. Accordingly, all employees are required to use and process personal data, which they can view or process to perform their tasks and responsibilities exclusively for the intended purposes.

The new rules further provide that only those employees may have access to personal data, which require such access in order to perform their tasks and responsibilities. Accordingly, all employees

are required not to disclose personal data to unauthorized persons (inside and outside the company) or to inform them in any other way about those data.

We endeavor to prevent unauthorized access to personal data and the disclosure of such data to unauthorized persons as far as possible by technical means. However, this is only possible to a limited extent. Therefore, it is essential that all employees stay up to date and comply with the IT security regulations as well as the user rules and instructions applicable in the company and available in the respective quality management documentation on the intranet, as well as the applicable rules for the storage and administration of documents in paper form; the general access security and locking regulations. Further, it is essential that any technical and organizational gaps which may exist in the protection of those data are not abused by staff for any unauthorized access, processing or unauthorized access.

In this context, we would like to point out that, in recent months, phishing attacks have been a growing problem for companies across the world, where hackers try to obtain employees' passwords through malicious emails in order to gain access to e-mail accounts and other IT systems. In order to respond to this threat, we are continuously improving our filter and security measures. In order to counter this threat we are constantly improving our technical filtering and security precautions. In addition, it is imperative that all staff are cautious when opening Email attachments, do never obey with any email instruction to disclose credentials, notify apparent phishing emails to the IT department and, in general, pay great attention to the protection of mechanical and electronic keys and passwords in everyday behavior.

The new regulations stipulate that management must always have a precise overview of where, how and for what purpose personal data are saved, stored and processed in the company in order to be able to provide information or implement restrictions within a few hours in the event of instructions to this effect; accordingly, all employees are required to create new collections of personal data only in consultation with their respective superiors and, in the case of electronic data, with the IT department.

The new regulations stipulate that personal data may be processed only for specified limited time periods and then deleted. This means that all employees are required to adhere to the specified deletion deadlines and deletion processes.

The new regulations stipulate that particular attention must be paid to the accuracy of the data in the processing of personal data. Therefore, all employees are required to ensure that such data are correct and, if necessary, to initiate corrections.

The new regulations provide for far-reaching duties to provide information and implement restrictions for data subjects. Therefore, all employees are required to cooperate swiftly and carefully in the processing of such inquiries and orders.

### **Controller of the processing of personal data, data exchange and data processing on behalf of Controllers**

Your employer is the Controller of the processing of personal data in our company and, thus responsible for it. In order to facilitate smooth business processes and exploit synergies, certain personal data must also be exchanged and processed across companies in our group of companies. As a consequence, all employees are required to process personal data processed for partner companies with the same care and with respect of the same rules as those of the employer.

### **Further information on data protection**

Further information on our company's data protection regulations and the rights and obligations arising therefrom may be found on our intranet under the heading Data protection and in the data protection notice on our company website.

For any further question, which staff members may have, they are free to contact the data protection coordinators under the contact addresses indicated in the Data Protection Contact List.