Data protection and data security at Wir Packen's

We are pleased to be able to guarantee the best possible data protection and data security to all our partners. This applies to new customers with the highest security requirements as well as to our existing customers. Wir Packen's deals with a lot of data: Starting with those of its own employees, it continues from the data of applicants and service companies to those of our clients and their customers. This includes highly sensitive data that require a very high safety profile in dealing with them. To protect this data, we need to ensure their security. These include the issues of confidentiality, integrity, availability, commitment, accountability, and more recently the sanctity of appliances.

In addition to meeting the legal requirements of data protection and the installation of an external data protection officer, we take the protection and security of all in our accumulated data so serious that our security concept and the resulting measures go far beyond what is required.

Wir Packen's sets high security standards in all areas

How do you manage to guarantee this level of data security? With our data protection officer Manfred Pastuska we have developed, and put in writing, a tailor-made data security concept for us and our customers and business partners. In addition, we have developed quite a lot of information, forms and guidelines that we provide for our staff. We ask our employees to confirm in writing that they are aware of their obligations and that they comply with the guidelines:

- Wir Packen's safety manual,
- Booklet for staff information about the BDSG
- Consent according to § 4 section 2 and in connection with § 4a BDSG
- Formal obligation to preserve the secrecy of telecommunications in accordance with § 88 Telecommunications Act (TKG)
- Formal obligation to ensure data secrecy in accordance with § 5 BDSG
- Formal obligation to maintain postal secrecy in accordance with § 39 Postal Services Act (PostG),
- Security policy for fixed and mobile information and communication technology as well as for internal and external computer networks.

Moreover, our concept consists of a large number of individual technical and organizational measures.

Inner and outer security

The entire facility is protected by a variety of technical means. Obviously, for security reasons we cannot describe these measures in detail. But to at least give an idea of how important security is to us, we can say that we have installed alarm systems that are connected to an external security firm, all the checks of the premises and the building facilities will be logged and our entrances are protected by technical installations. Visitors are identified and are not allowed to move unaccompanied in the building, maintenance and

cleaning personnel are supervised. Even within our building, we provide protection for particularly sensitive areas. They include, among other things, the spatial separation of work areas, additional safety equipment as well as access restrictions and controls.

Security in data processing

We have laid down rules for the allocation and management of access permissions comparable to the security policy for fixed and mobile information and communication technology as well as for internal and external computer networks. They prevent unauthorized persons from using data processing systems.

Our security measures ensure that employees, who use the data processing systems, may only work with the data which they have permission to access. We also protect personal data in the processing, use and after storage, and the electronic transmission, in their transportation or their storage on disk in such a way that it cannot be read, copied, altered or removed. Further, we ensure and check whether and by whom data is entered into the system, altered or removed and at which points transmissions are planned.

We guarantee that personal data handled on behalf of clients can only be processed according to the instructions of those clients. We carefully ensure that these data are protected against accidental loss or destruction. Data collected for different purposes are processed separately.

At Wir Packen's, data security is daily common practice. We feel committed not only to our customers but also to our employees and applicants. As data protection policies, laws and regulations are subject to constant change, continuous revisions and refinements are necessary. They are integrated into our everyday work, because through new media, storage facilities, etc., the conditions, under which data have to be dealt with, keep changing.

The Federal Data Protection Act (BDSG)

It is not a recent revelation that all of us have to be protected from the misuse of our data. As early as 1977, the Federal Data Protection Act was passed, in order to "... through the protection of personal data against abuse in storage, transmission, modification and deletion, counteract interests worthy of protection against any impairment."

The first two articles of the Basic Law form its foundation:

> Article 1, paragraph 1: „Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority."
>
> Article 2, paragraph 1: "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law."

They shall protect the general personality right which the Federal Constitutional Court described as the "right to informational self-determination", because

> "A social order, by which citizens can not know who knows what when and on which occasion about them and a legal system that would support this, are incompatible to the right to informational self-determination."

Privacy and security measures

All technical, organizational and personnel measures that ensure the right to informational self-determination are to be used. The Appendix to § 9 of the BDSG describes the technical and organizational measures, the so-called eight commandments of data security, which have to be taken by any company to guarantee the execution of the provisions of relevant legislation on data protection:

1. Access control
2. Admission control
3. (Electronic) access control
4. Transfer control
5. Input control
6. Order control
7. Availability control
8. Control of the separation of purposes.