Privacy Policy

1 Introduction

The protection of personal data is an important concern for our company. For this reason, we process the personal data of our employees, customers, business partners, service providers, public authorities and other third parties exclusively in accordance with the applicable legal provisions regarding the protection of personal data and data security.

In order to underline this concern, company management hereby adopts this Privacy Policy for our company. This Policy is intended to present the organisation, responsibilities and goals in the area of data protection in our company in a clear and concise form.

2 Scope of application

The Policy applies to VPL Coatings GmbH & Co KG as a whole and extends to all current and future business locations of the company. It is aimed at all current and future employees of the company. This Policy obliges all employees of the company to independently comply with the rules and duties laid down here, and to fulfil the formulated responsibilities in their area of activity.

3 Organisation of data protection

Company management bears the overall responsibility for data protection and the processing of personal data. Company management provides sufficient time, financial resources and personnel resources to meet the requirements of data protection legislation.

This includes the appointment of a data protection officer for the company. The data protection officer performs the tasks pursuant to Art. 39 GDPR and advises management and the employees involved in the planning and implementation of data protection and processes in the company in compliance with data protection.

It must be ensured that the data protection officer is involved at an early stage in the planning and introduction of new processes in connection with which personal data is also processed. The same applies to changes to existing processes.

The data protection officer is assigned a direct contact person as the data protection coordinator. Such person acts as the first point of contact for matters of data protection and internally accompanies, supports and drives forward the planning, implementation and evaluation of measures for data protection compliance. The data protection officer advises the data protection coordinator.

4 Responsibilities

4.1 Company management

Company management assumes overall responsibility for data protection in the company. It ensures that sufficient time, financial resources and personnel resources are available. It also authorises the data protection coordinator to plan and after consultation implement appropriate measures to achieve, maintain and improve the level of data protection.

4.2 Data protection officer

The data protection officer is the contact person for the topic of data protection in the company. He or she performs his or her tasks in accordance with Art. 39 GDPR and advises, monitors and supports company management, the data protection coordinator and the employees with regard to the processing of personal data within the company.

In accordance with Art. 37 GDPR, the following person has been appointed as data protection officer:

Dr. Andreas Melzer
kelobit IT-Experts GmbH
Tel.: 0345 132553-80
E-mail: dsb@kelobit.de

4.3 Data protection coordinator

The data protection coordinator acts as the primary contact person for the data protection officer in the company. The following person has been appointed as data protection coordinator:

VPL "Data Protection Team"
Tel.: 03496 68-636
E-mail: office@vpl-coatings.de

He or she consults with management and the data protection officer to support the implementation of the measures recommended by the data protection officer for achieving, maintaining and improving the level of data protection in the company. He or she also meets with the data protection officer at regular intervals to discuss the progress of the planned measures.

The data protection coordinator continues to process requests from data subjects and receives notifications of data breaches or suspected data breaches. Where necessary, he or she coordinates further action in these matters with management and the data protection officer.

4.4 All employees

Each employee contributes independently to ensuring data protection in the company by working in compliance with data protection regulations. In doing so, all employees are obliged to follow and comply with this Policy – in particular the principles listed below for the processing of personal data – and the other policies regarding data protection. If questions or ambiguities arise on specific points, employees are to seek advice from the data protection coordinator.

Where there are uncertainties or doubts as to the lawfulness of individual processing operations, in particular as regards the transfer or disclosure of data, the data protection coordinator is to informed and his or her advice is to be sought before the processing operation is carried out.

If obvious or at least possible violations of data protection are discovered in the course of everyday work, every employee is obliged to report such incidents and other disturbances in data processing immediately and directly to the data protection coordinator.

If persons contact individual employees with questions or concerns regarding data protection in the company, such persons are to be referred to the data protection coordinator or the data protection officer. The independent provision of information and other actions are not permitted.

For employees with special tasks listed below, the regulations laid down there also apply.

4.5 IT manager

The IT manager ensures the security of electronic data processing by planning, procuring, implementing and monitoring appropriate technical protection measures. The necessary budget for this is provided by company

management. He or she coordinates measures that have an impact on the security of data processing with the data protection officer and ensures that the existing protective measures are adequately documented.

4.6 Administrators

The administrators carry out the technical measures in coordination with the IT manager, document their activities and contribute to the optimisation of the security of data processing and data protection by making suggestions for improvement.

4.7 Supervisors with personnel responsibility

Supervisors with personnel responsibility ensure that the persons working in their area of responsibility are adequately informed of data protection issues and work in compliance with data protection regulations and are obliged to maintain data protection and confidentiality. Furthermore, they take measures that enable the persons working in their area of responsibility to work in compliance with data protection regulations.

4.8 Project or process managers or division managers

Project or process managers or division managers involve the data protection officer at an early stage in the planning of projects with an impact on the processing of personal data, in order to ensure compliance with data protection regulations.

When commissioning external service providers or suppliers, project or process managers or division managers are obliged to select them carefully with regard to data protection. Furthermore, the existence of the processing of an order is to be reviewed upon commissioning and, if necessary, a corresponding order processing contract is to be concluded. Even if this does not comprise order processing, a contract must include provisions to protect data protection and confidentiality. The assistance of the data protection team may be called upon for such reviews.

4.9 Suppliers, external service providers and other contractors

Suppliers, external service providers and other contractors are to be obliged by separate agreements to comply with and provide evidence of the data protection requirements that affect them. If they process data on behalf of the company (order processing), an order processing contract is to be concluded prior to the commissioning.

5 Principles for the processing of personal data

The objective of this Policy is to ensure data protection within the company. For this purpose, the company will take the following data processing principles into account when planning, implementing and running processes.

5.1 Lawfulness

In the processing of personal data, the fundamental rights and freedoms of data subjects must be respected to the fullest extent possible. As such, personal data may only be collected and processed in a lawful manner, that is, only if there is a clear legal basis.

5.2 Tied purpose

The processing of personal data may be pursued only for the purposes established and documented prior to the collection of the data. Such purposes must correspond to the reasonable expectations of the data subjects as regards the processing activity in question. In principle, subsequent changes to the purposes are not foreseen. If the need for a change of purpose arise in individual cases, this is only possible to a limited extent and requires a documented weighing of interests after consultation with the data protection officer and approval by management.

5.3 Transparency

Data subjects affected by the processing must be informed of the processing operations envisaged on a timely basis. When collecting the data, the data subjects must therefore at least be able to recognise or be informed of the following information:

- the identity of the controller, that is to say, our company
- the contact details of the data protection officer
- the purpose and legal basis of the data processing
- the intended recipients of the data, in particular if the data is to be transferred to a third country

Furthermore, personal data must always be collected directly from the data subjects themselves. If possible, collections from third parties are to be avoided.

5.4 Data avoidance and data minimisation

Prior to the collection of personal data, whether and to what extent such data is necessary to achieve the purpose intended by the processing must always be reviewed. Only such data that is identified as necessary in the process may be collected and stored. All other data may not be collected. Furthermore, personal data may not be stored in stock for potential future use, unless this is required or permitted by state law.

Access to stored personal data is always to be restricted to those employees who consistently need it to carry out their assigned work tasks. The necessity for the continued existence of access authorisations is to be reviewed on an ongoing basis.

5.5 Erasure

Personal data may only be stored until the purpose of collection and processing has been achieved and no mandatory statutory regulations prevent erasure. After the expiry of the statutory retention periods or retention periods related to business processes, or upon request of the data subjects, such data must be erased or destroyed immediately. In doing so, care must be taken to ensure that, when data is erased or destroyed, appropriate secure destruction measures are used in accordance with the protection value of such data.

If, in individual cases, there are indications that our company has an interest in certain data that is worthy of protection, such data will remain stored in a separate area outside the active user access until the interest worthy of protection has been reviewed and, if necessary, legally clarified.

5.6 Factual accuracy and timeliness of data

Personal data must always be stored in a manner that is accurate, complete and up-to-date. Appropriate measures must therefore be taken to ensure that inaccurate, incomplete or outdated data is erased, rectified, supplemented or updated.

5.7 Confidentiality and data security

In the processing of personal data, respect for the confidentiality and integrity of the data has a particularly important role. For this reason, personal data must be treated confidentially in day-to-day dealings and, by means of appropriate organisational and technical measures, must be protected against unauthorised access, unlawful processing or disclosure, along with accidental loss, alteration or destruction.

In the specific implementation of the objectives, the protection measures taken must be economically proportionate to the need to protect the data and information processed.

6 Sanctions

A breach of this Policy may constitute a breach of duty under an employment contract and may be sanctioned accordingly.

For suppliers, external service providers and other contractors, contractual penalty arrangements for special risks are to be agreed.