Data protection Guideline

1. Introduction

K&K social resources and development GmbH (hereinafter „K&K“) hereby adopts this guideline on data protection in our company.

As a company, we process a large number of (including personal) data in order to fulfill our tasks and obligations towards our customers, contractual partners, service providers, public bodies and other third parties.

We process data with different protection requirements. The security of information processing and the protection of personal data play an essential role in our company.

This guideline is intended to present the strategy, organization and goals of data protection in our company in a clear form.

2. Scope

This guideline applies to K&K. It extends to all K&K locations.

This guideline obliged all K&K employees to comply with the obligations set out here. The current version of the guideline is made available to employees in a suitable manner.

3. Goals

The Goal of this guideline is to ensure data protection in the company in accordance with the provisions of the General Data Protection Regulation, the Federal Data Protection Act and other applicable data protection provisions.

The graceful handling of personal data, which safeguards and promotes the fundamental rights and freedoms of natural persons, has top priority. The company undertakes to process personal data only in a manner that is compatible with applicable laws and human dignity.

For this purpose, the company will take into account the following goals in accordance with Art. 5 GDPR when planning, introducing and during the course of processes:

1. Rightfully
2. Transparency
3. Earmarking
4. Data minimization
5. Correctness
6. Storage limit
7. Availability, integrity and confidentiality, resilience
8. Intervention and processing in good faith („fainess“)
9. Accountability („Accountability-Principle“)

The consideration of these goals is specified in separate guidelines.

In the concrete implementation of the goals, the protective measures taken must be in an economically justifiable relationship to the protection requirements of the processed data and information.

4. Data protection organization

4.1 Data Protection Officer

K&K has appointed a data protection officer (DPO). The data protection officer is the contact person for the topic of data protection in the company. He advises monitors and supports the company management and employees with regard to the processing of personal data in the company. His or her other duties arise primarily from Art. 39 DSGVO.

In the area of processing personal data, care must be taken to ensure that the data protection offer is involved 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 involvement of the DPO can also take place in connection with the involvement of the DST.

A management system is set up in the company for the area of data protection. For this purpose, a process of continuous improvement is implemented in the company with the goal of coordinating the individual measures in the area of data protection in such a way that the objectives of this guideline are achieved.

4.2 Data Privacy Team (DST)

A Data Privacy Team (DST) will be formed to accompany and support the planning, implementation and evaluation of data privacy in the company. The DST will plan the policies required to implement the objectives of this Guideline, coordinate them with the company's management and regularly review their effectiveness and make adjustments as necessary. In the event that the DST disagrees on issues relating to the planning, implementation, evaluation or adjustment of guidelines, or on the assessment of factual or legal issues, the DST will bring this to the attention of the company's management. Management will then decide and initiate action as necessary.

The K&K guidelines are made binding by the company management so that they must be complied with by the respective addressees of the guideline and violations can be sanctioned if necessary.

The DST reports directly to the company management.

The company management will appoint the members of the DST.

The Data Privacy Officer is a mandatory member of the DST. Further members will be appointed by the company management in agreement with the respective persons.

The DST will discuss factual issues and report to the management on the outcome of the discussion. If the DST does not have a unanimous opinion on an issue, the opinion will be openly reported to the Executive Board.

The Executive Board may delegate decisions to the DST by issuing instructions in text form.

In such delegation, the management shall determine whether a unified decision of the DST or a majority decision is sufficient for a decision of the DST.

The DST will meet at least once a year to review the effectiveness of the data protection measures taken and to make adjustments.

The DST will otherwise coordinate on an ad hoc basis with regard to meetings or decision-making to discuss and decide on pending factual issues. Actions and decisions may also be discussed by telephone or text, i.e., conference calls, online meetings, and/or email discussions.

The DST itself can assign its own roles to members. For example, maintaining and keeping processing records or planning the conduct of data protection impact assessments may be delegated to individual members for further coordination. However, the DST acts collaboratively, and members of the DST assist each other in fulfilling their responsibilities.

Tasks and powers may be delegated to the DST by management. This can also be done by appropriate specifications in guidelines issued by K&K.

A collective e-mail address shall be set up for the DST at dst@muster.de, at which the DST can be reached electronically by all K&K employees and the company management. The e-mail address will be communicated to all employees in an appropriate manner and must be easy for all employees to find. This can be done, for example, by means of notices (analog/digital).

It is also the task of the DST to build up and maintain knowledge in the area of data protection. To this end, the DST maintains contacts with suitable working groups, committees or associations

5. Measure

The measures to implement these guidelines can take the form of technical and organizational measures. These also include guidelines, company regulations or company instructions. These must be followed by the employees.

6. Responsibility

The company management assumes overall responsibility for data protection in the company.

The responsibilities of the DPO and DST are already described above.

The IT officer implements the guidelines and other requirements for data privacy in his area of responsibility. He or she coordinates measures that have an impact on data privacy with the data privacy officer.

The administrators implement the technical measures in coordination with the IT officer and contribute to the optimization of data privacy by making suggestions for improvements.

Supervisors with personnel responsibility have the task of ensuring that the technical and organizational data protection measures taken are implemented with regard to the persons working in their area of responsibility.

All employees contribute to ensuring data protection through their conduct. All employees are obliged to comply with these guidelines and the guidelines on data protection.

To promote data protection in the company, all employees are obligated to report data protection-relevant malfunctions, security incidents and emergencies immediately and directly to the DST.

Data protection incidents must be reported to the DST by all employees immediately upon becoming aware of them.

The respective K&K guidelines apply.

Project or process owners must consult the DST on all projects affecting the processing of personal data to ensure that all data protection regulations can be met.

Supply companies, external service providers and other contractors must be required by separate agreements to comply with the data protection requirements affecting them if they process data on behalf of the company or have the possibility of becoming aware of personal data or information of the company that is not classified as public.

7. Sanctions

Violation of this guideline may constitute a breach of duty under the employment contract and be sanctioned accordingly

Contractual penalties should be agreed for supply companies, external service providers and other contractors in the event of particular risks.