BRANDI
RECHTSANWÄLTE

EMPLOYEE DATA PROTECTION – GENERAL PRINCIPLES

Information on data protection I July 2022

Introduction

Employers regularly come into contact with personal data of applicants and employees. In order to carry out the employment relationship, the employer must, for example, carry out payroll accounting, plan the deployment of employees in the company and provide the employee with a workplace and means of communication. With regard to the handling of employees' personal data, there are special requirements under data protection law. On the one hand, the processing of employees' personal data is essential for the employer; on the other hand, employees have an interest in and also a right to have their personal data collected, processed and used only in compliance with their own interests worthy of protection. As this topic is of great importance in the day-to-day work of every company, the handling of employee data is examined in more detail in this newsletter.

Contrary to various considerations in the past, there is currently no comprehensive employee data protection law. Most recently, the Data Protection Conference (DSK), the association of independent data protection supervisory authorities at federal and state level, also called again for the creation of such an Employee Data Protection Act in its resolution of April 29, 2022. The General Data Protection Regulation (GDPR) does not contain any concrete, sector-specific regulations for this particular processing situation, so that general data protection regulations must be applied in this respect. However, Article 88 (1) GDPR contains a so-called opening clause, which allows the individual EU member states to enact specific regulations for the area of employee data protection. Corresponding national provisions must comply with the content requirements of Article 88 (2) GDPR. The German legislator has made use of this opening clause and included a corresponding provision in the Federal Data Protection Act (BDSG). In addition, the other general data protection regulations must of course also be taken into account when processing employee data.

Processing of employee data

Pursuant to Section 26 (1) (1) BDSG, personal data of employees may be processed in particular for purposes of the employment relationship if this is necessary for the decision on the establishment of an employment relationship or, after the establishment of the employment relationship, for its implementation or termination or for the exercise or fulfillment of the rights and obligations of the employee representation resulting from a law or a collective agreement, a works agreement or a service agreement.

Pursuant to Section 26 (8) BDSG, the term "employees" includes not only employees but also temporary workers, trainees, applicants and persons whose employment relationship has ended.

Contrary to the GDPR, which requires automated processing or, alternatively, the at least intended storage of personal data in a file system, the regulations on the processing of data in the employment relationship pursuant to Section 26 (7) BDSG also apply if the relevant data is not to be stored in a file system. Accordingly, the requirements of Section 26 BDSG must also be observed when processing employee data in paper form.

Personnel file

Employees' personal data is usually filed or stored in the personnel file. The associated data processing operations can be based primarily on Section 26 BDSG (purposes of the employment relationship) and the fulfillment of the contract pursuant to Article 6 (1) (1) (b) GDPR. However, taking into account the principle of data minimization, the company may not collect and process any amount of data. Instead, the personnel data held must be limited to the necessary core data. Nevertheless, the personnel file contains a large amount of confidential and sometimes sensitive information about the employee that can be combined to form a profile, which is why the personnel file and the information it contains also require special protection. The required level of protection and the specific measures to be taken depend on the sensitivity and type of the different data. The same also applies with regard to the question of how long individual employee data may be stored. In this respect, blanket arrangements may be problematic from a data protection perspective; instead, each instance should be considered on a case-by-case basis. For this reason, care must always be taken to ensure that the personnel file is carefully stored, that the group of persons authorized to access it is limited to the necessary extent, and that the contents are protected from unauthorized inspection. As a rule, the possibility of inspection should be limited to the employer and the personnel administration.

Processing of special categories of personal data

Health data is also regularly processed within the scope of the employment relationship. These fall under the category of special data within the meaning of Article 9 GDPR and require special protection due to their sensitivity. Section 26 (3) BDSG further tightens the already strict requirements of the GDPR for the case of processing within the scope of the employment relationship. In this respect, the processing of particularly sensitive data is only permissible insofar as it is necessary for the exercise or fulfillment of rights and obligations arising from labor or social law and it cannot be assumed that conflicting interests prevail. In addition, health data such as illness information may not be filed or stored in the personnel file, but must always be kept separately. The group of authorized persons should also be limited to the supervisor and the HR manager.

Disclosure of employee data
If employee data is to be transferred to a service provider or to another group company, the general provisions of the GDPR on Contract Processing (Article 28 GDPR) or Joint Controllership (Article 26 GDPR) must be complied with. For example, if a company has outsourced its accounting to an external payroll office and employee data is transferred to and processed by the payroll office in order to carry out payroll accounting, it is necessary to conclude an agreement on contract processing with the service provider involved in order to safeguard these data processing operations. Furthermore, employee data may not be passed on to other companies without a corresponding legal basis. In the case of a "group-wide employment relationship", the legal basis for the transfer of data may also be the fulfillment of the contract pursuant to Article 6 (1) (1) (b) GDPR and Section 26 BDSG. This is the case, for example, if the activity agreed in the employment contract is clearly related to the group or the respective employee is deployed at various companies of the group.

Employer's information obligations and employees' obligations under data protection law

If personal data is collected, data controllers are obligated under Article 13 (1) GDPR to provide the data subjects with various mandatory data protection information. The information obligations pursuant to Article 13 GDPR apply not only to data processing processes in the context of the application procedure, but also to the processing of personal data during the employment relationship. Among other things, employees must be informed about the purposes for which the data are to be processed, the legal basis for the processing and the storage period. In addition, the data subjects must be provided with information about the various data subject rights, such as the rigt of access and the right to erasure.

In terms of time, the data protection information of the employees must be provided "at the time of collection". Insofar as employees have not already been comprehensively informed about data protection law as part of the application process, employees should be informed again separately about the type and scope of data processing on the occasion of the employment relationship, any special features and the rights to which they are entitled when they sign the employment contract or start work.

In addition, it is advisable to oblige all employees of the company to observe data secrecy at the beginning of their work. Companies are subject to the so-called "accountability" under the GDPR. This means that they must prove that they comply with the requirements of the GDPR. According to Article 24 GDPR, this also includes taking the necessary organizational measures to protect personal data. However, proof of the correct implementation of these measures will only be possible if all employees who come into contact with personal data are obligated in writing to maintain confidentiality and the applicable data protection regulations as well as the duties incumbent upon them. The obligation then continues beyond the end of the employment relationship.

Consent in the employment relationship

A possible legal basis for the justification of data processing operations is the consent of the data subject to the specific data processing pursuant to Article 6 (1) (1) (a) GDPR. For consent to be effective, it must be given by the data subject in an informed manner, for the specific case, voluntarily and unambiguously by means of a declaration or unambiguously confirming action. If data processing by the employer is to be based on the employee's consent within the meaning of Article 6 (1) (1) (a) GDPR, some special features must be taken into account. In this respect, the aspect of the voluntary nature of the consent is particularly problematic.

In the past, the view was sometimes expressed that consent under data protection law within the framework of the employment relationship was problematic and could not even be granted, as a free decision could not be assumed due to the employee's existing dependence on the employer (Gola/Schomerus, BDSG § 4a Rn. 6 with further references). In the meantime, however, case law has clarified that effective consent under data protection law can also be granted in the context of an employment relationship, as the employee may freely exercise his right to informational self-determination in this context as well (BAG, decision dated December 11, 2014, Ref. 8 AZR 1010/13). The employee's right to dispose of his or her data by consent is not taken away by entering into an employment relationship.

Nevertheless, consent in the employee relationship is generally only considered in exceptional cases and if the additional requirements of Section 26 (2) BDSG are met. According to the provision, the assessment of the voluntariness of the consent requires, in particular, consideration of the dependency of the employee in the employment relationship as well as the circumstances under which the consent was given. According to Section 26 (2) (2) BDSG, the aspect of voluntariness is to be affirmed in particular if a legal or economic advantage is achieved for the person employed, or if the employer and employee pursue similar interests. Irrespective of this exemplary list, it should nevertheless be checked in each case whether a voluntary decision by the employee can actually be assumed, as otherwise there is no effective consent and thus, as a rule, no legal basis for the data processing.

In order to protect the employee from acting hastily, and to make clear to them the relevance of their decision, as well as for purposes of proof, any consent in the context of an employment relationship must be in writing, unless another form is appropriate due to other circumstances. In addition, the employee must have the actual possibility to revoke the consent at any time and must also be informed about this possibility. In addition, it is recommended that the consent or the associated data protection information also explicitly state that refusal of consent or subsequent revocation is not associated with any adverse consequences for the employee. To avoid any legal uncertainties, it is advisable – as far as possible – to base data processing operations in the context of the employment relationship on a legal basis other than consent.

Monitoring of employees

It is often questionable to what extent existing data may be used to monitor employees' compliance with legal and contractual requirements. In this respect, the evaluation of video surveillance or telephone, e-mail and internet use is conceivable. Taking into account the principle or purpose limitation, personal data may only be processed for the purposes originally intended in the context of data processing. If video surveillance has been installed, for example, to prevent shoplifiting, the recordings may not be used without further ado for other purposes, such as compliance with break times. A change of the original purpose of the data processing is only possible under the narrow conditions according to Article 6 (4) GDPR. The covert monitoring of employees is also generally prohibited. In addition, for any form of monitoring measures, a balancing of interests between the interests of the employer and the employee must take place, by means of which it must be determined whether a measure does not excessively interfere with the rights of the employees. In any case, the relevant case law should also be taken into account.

In principle, employee data may also be processed to uncover criminal acts in accordance with Section 26 (1) (2) BDSG. However, this only applies if factual indications to be documented give rise to the

suspicion that the person concerned has committed a criminal act within the scope of the employment relationship. In addition, the data processing must be necessary to uncover the case, and in each case it must be weighed against the interests of the employee, whereby the data processing in particular must not be disproportionate with regard to the specific incident. It must also be taken into account that data processing may only be carried out by an authorized person, such as the HR or IT department, at best in consultation with the data protection officer.

Conclusion

In addition to compliance with general data protection regulations, there are a number of special requirements to be observed and additional requirements to be met when processing employee data. In German law, the latter result in particular from Section 26 BDSG.

The personnel file in particular contains a large amount of employee data and must therefore be treated confidentially. Only data that is necessary for the performance of the employment relationship may be filed or stored. If this principle is violated, this can sometimes result in substantial fines. The H&M Group, for example, was fined more than 35 million euros because managers unlawfully collected information about their emplyees' private lives and stored it in their personnel files.

If data processing within the scope of the employment relationship is to be based on the legal basis of consent, a precise examination of the individual case is generally required with regard to the legality, taking into account the respective circumstances. In particular, attention must be paid to whether the employee's consent was actually given voluntarily.

If personal data of employees is also to be used for monitoring purposes, this is only possible under very strict conditions. In any case, employees should be informed transparently and comprehensively about the circumstance of the monitoring and the respective case law should be taken into account. If a works council exists, it should be involved in the considerations and processes in order to avoid disputes.

Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

T +49 521 96535 - 890
F +49 521 96535 - 113
M christina.prowald@brandi.net