General Data Protection Regulation - Protection of Employee Data

Phillip Raszawitz

The General Data Protection Regulation (GDPR), which is intended to unify protection of personal data in all EU member states, will go into effect throughout Europe next year. The Regulation will be directly applicable and take priority over domestic law, but it will also leave national lawmakers the discretionary leeway required to enact their own provisions as long as they are not inconsistent with those contained in the GDPR. Germany's legislature has availed itself of this option and adopted the Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 as well as changes in the current version of the Federal Data Protection Act (*Bundesdatenschutzgesetz* – BDSG). The revised version of the Federal Data Protection Act was announced on 5 June 2017. The new provisions will take effect as of 25 May 2018 along with the GDPR.

A complete presentation of the changes in the GDPR and the changes in legislation governing data protection that affect employment relationships would exceed the scope of this bulletin. The presentation below is therefore intended to provide an overview of changes regarding the protection of the personal data of employees, in particular as regards the provisions contained in § 26 of the Federal Data Protection Act (new version), as well as to show what companies and employees can expect in this regard in the future.

Introduction

The GDPR primarily reinforces the rights of individuals when their data are processed and, for example, Art. 13 and 14 of the GDPR contain expanded duties to provide data subjects with information that also apply as regards employees. In the future, the right of data subjects to obtain information on whether and how their personal data are being processed will be significantly expanded under Art. 15 of the GDPR. Although the GDPR is intended to provide a uniform level of data protection, it contains many different mandatory and optional escape clauses that require or allow national legislatures to determine the actual form of implementation in certain areas. In the area of protection of the personal data of employees, Art. 88(1) of the GDPR allows the member states to regulate the processing of personal data of employees in the context of national legislation governing employment. The jurisdictional competency of the national legislatures is, however, limited to "more specific" rules. National legislatures will not have the right to deviate from the GDPR by lowering or raising the level of protection. The option of national legislatures to adopt more specific rules in respect of the protection of employee data pursuant to Art. 88 (1) of the GDPR will also not be unlimited. In fact, Art. 88(2) of the GDPR allows only measures that are suitable and adequately safeguard the fundamental rights and legitimate interests of the respective data subject.

In Germany, § 26 of the Federal Data Protection Act (new version) will replace the current § 32 of the Federal Data Protection Act as the central provision governing the protection of employee data. It is obvious that the legislature has modeled the revision of § 26 of the Federal Data Protection Act (new version) on the main regulatory structures, mechanisms and provisions of the previous § 32 of the Federal Data Protection Act.

Employee data protection pursuant to § 26 of the Federal Data Protection Act (new version)

Grounds

As already allowed in the past, the first sentence of § 26(1) of the Federal Data Protection Act (new version) allows employers to process the personal data of their employees where "necessary" to establish, maintain or terminate an employment relationship. Pursuant to the second sentence of § 26 (1) of the Federal Data Protection Act (new version), it will also still be possible to process data for the purposes of criminal investigation under special circumstances. In addition, it will still be possible to process data when necessary to enable representatives of the interests of employees to exercise their rights or fulfill obligations under the law or a collective agreement. It will also most likely be possible to process the personal data of employees for purposes other than those re-

lated to the employment relationship on the basis of the consent provisions contained in Art. 6(1) or Art. 9(2) of the GDPR.

Necessity of data processing

It is also possible to infer from the explanatory memorandum on § 26 of the Federal Data Protection Act (new version) that it can be considered necessary to process personal data of employees only if such processing is suitable for achieving the purposes of the employment relationship, is the least invasive of all equally efficacious options available to the employer and, finally, is not outweighed by any legitimate interest an employee may have in refusal to consent to such processing. In line with the previous case law of the Federal Labor Court, the fundamental legal positions of the employer and employees must be weighed against one another and reconciled by means of a practicable agreement.

Collective agreements

§ 26(4) of the Federal Data Protection Act (new version) makes it clear for the first time that what are referred to as collective agreements, i.e., wage agreements, works council agreements or enterprise agreements for public servants, constitute legal provisions within the meaning of the Federal Data Protection Act and accordingly can constitute a suitable legal basis for processing employee data. These agreements must therefore now also meet the requirements and standards contained in Art. 88(2) of the GDPR. Collective agreements must therefore include suitable and specific measures to safeguard the human dignity, legitimate interests and fundamental rights of data subjects. In particular, they must contain measures to ensure transparency as regards the processing of data. Appropriate measures must be taken insofar as works council agreements also involve the transfer of personal data within a group of undertakings or a group of companies engaged in a joint economic activity. The same applies accordingly to works council agreements on workplace monitoring systems.

It is important to bear in mind that neither § 26 of the Federal Data Protection Act (new version) nor the GDPR makes provision for exceptions for “old” cases. Existing collective agreements, in particular works council agreements that govern the processing of personal employee data, must now meet the same standards. In that regard, the question already arises as to whether these agreements must be identified as a “permissive rule” for the purposes of application of legislation governing data protection. In addition, agreements must be examined with an eye to determining whether the standards of Art. 88(2) of the GDPR have been met, whether the principles of legislation governing data protection pursuant to Art. 5(1) of the GDPR have been satisfied and whether the duty to provide information pursuant to Art. 12 of the GDPR has been implemented and a data protection impact assessment carried out. In the event shortcomings should become apparent in the course of such a review, the respective agreements must be modified accordingly.

Voluntary consent

In the past, the question as to whether the consent of an employee was a valid ground for processing that employee's personal data was a matter of dispute in the context of the protection of employee data, but § 26(2) of the Federal Data Protection Act (new version) now expressly qualifies consent as a possible ground for processing an individual’s data. In addition, the new provision makes it clear that voluntary consent can exist despite the dependency inherent in an employment relationship if, for example, a legal or economic benefit accrues to the employee or both parties to an employment contract pursue similar interests. The explanatory memorandum cites “the introduction of company healthcare management to promote employee health” and the “permission for personal use of company IT systems” as typical examples.

Before they can give their consent, data subjects must be informed of the purpose for which their data are to be processed and their right to withdraw consent pursuant to Art. 7(3) of the GDPR. If special categories of personal data within the meaning of Art. 9(1) of the GDPR are to be processed with the consent of the data subject, the data subject must also be expressly informed of the possibility of withdrawing his or her consent in such cases. Any consent form should be carefully formulated to keep the possibility of invalidity of the consent to a minimum.

After revision, § 26(2) sent. 3 of the Federal Data Protection Act (new version) will still contain a written-form requirement that will apply except under special circumstances that justify a different form.

Application to "analog" data processing

With § 26(7) of the Federal Data Protection Act (new version), the legislature will continue to allow application of the provisions of legislation governing data protection in cases in which data processing is not automated and analog means are used instead.

Expanded sanction

The pending changes and new standards contained in the GDPR are already attracting considerable attention due to the fact that the economic risks associated with violations of legislation governing data protection will be significantly greater in the future. For example, the authorities responsible for data protection will be able to impose much higher fines. Art. 83 of the GDPR calls for fines of up to € 20 million or up to 4% of total worldwide turnover.

Conclusions

Data protection, particularly when data of employees are involved, has become increasingly topical in corporate practice due to the pending changes in the Federal Data Protection Act and the GDPR, which will go into effect in May next year. One reason for this can be found in the higher fines for violations of legislation governing data protection. Many questions still remain unanswered in this context. Despite the shift in focus from the national level to the European level due to the GDPR and thorough revision of the Federal Data Protection Act, and in particular its § 26, much will remain unchanged as regards the protection of employee data. Although the changes in the area of protection of data of employees may seem minor, the work that may be required should not be underestimated. For example, the more stringent requirements in terms of documentation and information on data processing that companies will generally face in the future will also apply in the employment area. As regards employee data protection in particular, companies and employee representatives may find themselves faced with numerous new duties due to the possible need to review and revise collective agreements that are already in effect or will be concluded in the future. The latter would therefore be well advised to review their current collective agreements for compliance with the GDPR and the new Federal Data Protection Act on a timely basis and initiate talks to adapt existing arrangements to new requirements.

Note

Our Offices

GÖRG Partnerschaft von Rechtsanwälten mbB

BERLIN
Kantstraße 164, 10623 Berlin
Phone +49 30 884503-0, Fax +49 30 882715-0

COLOGNE
Kennedyplatz 2, 50679 Köln
Phone +49 221 33660-0, Fax +49 221 33660-80

FRANKFURT AM MAIN
Neue Mainzer Straße 69 – 75, 60311 Frankfurt am Main
Phone +49 69 170000-17, Fax +49 69 170000-27

HAMBURG
Dammtorstraße 12, 20354 Hamburg
Phone +49 40 500360-0, Fax +49 40 500360-99

MUNICH
Prinzregentenstraße 22, 80538 München
Phone +49 89 3090667-0, Fax +49 89 3090667-90