The new § 32 of the Federal Data Protection Act - More Than Just Clarification of Existing Law?

Amendment of Data Protection Law

The handling of employee data by some companies has recently triggered a political and public debate about the need for stricter employee data protection laws and for the creation of a separate employee data protection act.

On July 3, 2009 the German *Bundestag*, with votes from the coalition parties, passed the "Act for Amendment of Data Protection Laws", which will take effect on September 1, 2009. On July 10, 2009, the law was also passed by the German *Bundesrat*. The new law, for now, involves the "*de minimis* solution" preferred by the government coalition. Foregoing -- at least preliminarily -- a separate employee data protection act, the legislature added a fundamental employee data protection provision (FDPA § 32 (as amended)) to the Federal Data Protection Act (*Bundesdatenschutzgesetz* – "FDPA"). In addition, FDPA § 4f, a provision introducing special protection from termination for data protection officers, was added.

In the course of the legislative process, it was emphasized that the new FDPA § 32 merely summarizes the employment-related data protection principles developed by German courts in the past, but is not intended to change these principles. A closer look however reveals that the new law can, in part, quite readily be interpreted as an expansion of the scope of protection afforded to employee data.

In the past, the collection, processing or use of personal data for employment purposes was in essence governed by FDPA § 28 (1). In the future, employers will also have to comply with FDPA § 32 (as amended), whose applicability has priority over that of FDPA § 28.

FDPA § 32 (1) Sent. 1 (as amended) - Data Protection in the Employment Context

According to paragraph 1 of FDPA § 32 (as amended), personal data of employees may be collected, processed or used for employment purposes (only) if this is "necessary" for the formation of an employment contract or for the performance or termination of an employment contract after formation.

When applying FDPA § 28 in the past, courts predominantly held that the collection, processing or use of data must always be "necessary," although this was not expressly stated by the (old) statutory provisions. This view has now become the letter of the law.

As examples of the (continued) permissibility of collecting data, the legislature cited questions about professional skills, know-how and experience during the pre-hiring phase or questions about information or circumstances of employees that are, for example, necessary for payroll purposes.

FDPA § 32 (1) Sent. 2 (as amended)- Data Protection During Measures Designed to Detect Criminal Offenses by Employees

The new law completely revises the provisions governing the circumstances under which personal data of employees may be collected and used to detect criminal offenses (FDPA § 32 (1) sentence 2 (as amended)). To begin with, the collection, processing or use of personal data to detect criminal offenses committed within the scope of employment is permitted only if there are "documented actual indications" that a criminal offense has been committed by an employee. The purpose of this rule is to preclude routine investigations in the future that are conducted without any suspected wrongdoing.

In addition, the collection, processing or use of employee data for the purpose of detecting a criminal offense must be "necessary." Finally, the collection or use of data may not be in conflict with any prevailing protected interests of the employee. In particular, the collection and use of data must be reasonable taking into consideration the interests of employer and employee.

It is noteworthy that the new law introduces a sort of "documentation obligation" with respect to the facts providing grounds for suspecting that a criminal offense has been committed. It is however unclear how this documentation must be handled if the suspicion that a criminal offense has been committed later turns out to be unfounded. It is to be expected that conflicts will arise with respect to the deletion or destruction of such documentation.

It is also unclear what rules apply if an employer wishes to follow up on a suspicion that an employee has breached duties under his employment contract, where such breach falls short of a criminal offense. It seems at least plausible that the general provision of FDPA § 32 (1) sentence 1 (as amended) and the necessity standard established by this provision would apply in such cases. This result however appears very questionable, because an employer would then face lower data protection hurdles for a less serious breach of contract than in the case of a criminal offense!

FDPA § 32 (2) – FDPA § 32 (1) (as amended) Also Applicable to Non-Automated Processing

FDPA § 32 (2) (as amended) provides that FDPA § 32 (1) (as amended) also applies if personal data are collected, processed or used by non-automated means, or if personal data are processed or used in or from a non-automated file or are collected for processing or use in such a file.

This provision expands the scope of applicability of the Federal Data Protection Act compared to the old law. Cases involving non-automated data collection or processing were in the past frequently resolved by courts without applying the Federal Data Protection Act, in consideration of the legal rights and interests involved -- in particular the employee's general right to privacy. In the future, the processing of data for employment purposes will -- generally regardless of the way in which data are processed -- be subject to the limitations of FDPA § 32 (as amended). Some legal commentators have already noted that even the simple monitoring or questioning of an employee (= data collection) by a superior may require justification under data protection law by showing that such measures are necessary.

FDPA § 32 (3) Employee Participation Rights

Finally, FDPA § 32 (3) (as amended) clarifies that the participation rights of employee representatives, in particular those of the works council, remain unaffected. This provision introduces no changes to existing law.

FDPA § 4f (as amended) - Special Protection from Termination for Data Protection Officers

FDPA § 4f now affords data protection officers with special protection from termination. Under this provision, a data protection officer may be terminated only if there is a good cause justifying termination without notice. If a data protection officer is removed from office, the officer enjoys protection from termination for one additional year. In addition, FDPA § 4f (as amended) provides that data protection officers are entitled to paid participation in training and education courses to the extent they provide training necessary for the duties of the officer.

Practical Advice

The changes to German employee data protection law must be seen as a political response to the "data protection scandals" that have plagued a number of large corporations in the recent past. The parties in power (*grosse Koalition*) apparently felt compelled to act before the political summer break.

As a result of the new law, companies are now confronted with an even more difficult dilemma than before: They are required -- in part, by other laws -- to establish mechanisms designed to prevent or detect violations of law by employees. In particular in recent years, numerous companies have therefore created well-staffed, well-equipped compliance departments. The trend of employee data protection law as we foresee it raises doubts as to whether compliance departments will, in light of the rising data protection hurdles, still be able to effectively carry out their tasks. The new law passed by the legislature fails to adequately take into consideration the interests of companies and appears to be a premature, unrefined "shot from the hip" motivated by the public debate and upcoming election.

It remains to be seen to what extent the German legislature will continue to pursue the topic of employee data protection after the *Bundestag* election. As the Committee on Internal Affairs noted in its recommendation for passage of the new law, FDPA § 32 neither obviates the need for a separate employee data protection act nor does it have any prejudicial effect on the contents of a future employee data protection act. Thus, it appears that the last word has not yet been spoken. When we will hear the next word will to a large extent depend on the legislative majorities emerging from the *Bundestag* election.

Contact

Dr. Henning Reitz (h.reitz@justem.de)
Dr. Thilo Mahnhold (t.mahnhold@justem.de)
www.justem.de