BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

German Legislation

Employment Privacy

New German Employee Privacy Proposal is a Mixed Blessing

BY KARIN G. RETZER

The German government has approved a bill that would substantially amend the country's framework data protection law, the Bundesdatenschutzgesetz ("BDSG"), with a focus on human resources data.[1] The bill follows Chancellor Angela Merkel's promise to revise the BDSG after a wave of corporate breaches of employee privacy. High profile German companies, including a supermarket chain and an automobile manufacturer, were found to be in breach of the law, and the government-owned railway

Karin Retzer is Of Counsel in the Brussels office of Morrison & Foerster LLP and a member of the Technology Transactions Group. Her practice focuses on the legal aspects of electronic commerce and data protection, technology licensing, and intellectual property law.

[1] The Bill (in German only) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_Beschaeftigtendatenschutz.pdf?__blob=publicationFile.

Background paper (in German only) http://www.bmi.bund.de/cae/servlet/contentblob/1286174/publicationFile/95296/pressepapier_beschaeftigtendatenschutz.pdf.

 ISSN 1538-3423

company Deutsche Bahn AG was issued the largest ever fine given for noncompliance with the BDSG. These scandals led to significant concern that the law was not being appropriately enforced and that changes needed to be made.

A proposal was made by the Ministry of the Interior to amend the BDSG by adding provisions that specifically addressed data protection in employment relationships. Current German employee privacy is variously regulated by general provisions in the BDSG, by provisions in the Works Council Act, by guidance from regional data protection authorities (''DPAs''), and finally by rather inconsistent case law emanating from the labor courts.

When they reviewed the bill prior to it being adopted by the government ministers in cabinet, the German DPAs, as well as Sabine Leutheusser-Schnarrenberger, the German Justice Minister known as a strong civil libertarian and privacy advocate, reduced the rights of employers and strengthened the protection of employees. These modifications amounted to significant changes to the Ministry of the Interior's initial draft.

The bill is now being discussed in the Bundesrat, the Parliament's chamber representing Germany's federal states. A vote is expected for October, after comments are received from the different legislative committees currently examining the bill.[2] The bill is then expected to undergo substantial changes in the Parliament's general assembly, the Bundesrat, before the final vote. Both the Bundestag and the Bundesrat need to agree on the final text. There is no set timetable for review in the Bundestag, although the bill could still become law in 2010.

The bill, as approved by the government, now goes before the German Parliament, where it is expected to undergo further substantial changes, although it could still become law in 2010.

The main elements of the bill are as follows:

Employee Consent: Consent to the collection, processing, and use of employee data is invalid unless expressly permitted by the new provisions on employee privacy. The bill permits consent only in very limited circumstances, *e.g.*, to legitimize certain types of background checks on applicants.

In the past, the German authorities had questioned the validity of employee consent unless employees had real freedom to say ''no'' (*i.e.*, it would not jeopardize their employment position). However, as a result of the bill, employee consent would be invalid even where previously recognized, for example, for data processing related to stock options plans, or for limited monitoring of the use of communication devices. If this provision remains unchanged, employers will need to (re)structure all of their employee data processing to comply with the statutory permissions and will be precluded from processing any data that is not otherwise permitted by a statutory exception.

Works Council Agreement: A new provision confirms earlier interpretations that an agreement with the Works Council may provide an alternative to consent or a statutory basis for legitimizing the processing of employee data. In other words, where an agreement with the Works Council permits certain processing of data, such processing is deemed legitimate. Language in the bill seems to suggest that an agreement may derogate some of the restrictions foreseen by statute, a point previously disputed by the authorities. As a result, Works Councils will have an even stronger say in Germany about employers' use of workforce data.

Applicant Background Check: Data may be collected from applicants only where strictly necessary to determine whether they are suitable for a particular position. Publicly available data may be collected without consent if the individual is notified. However, any collection of data from third parties (other than from public sources) will require consent from the applicant. This provision would directly affect background check providers.

In addition, background checks often contain ''sensitive data'' on racial or ethnic origin (for US-style equal opportunities compliance), religious or philosophical beliefs, disabilities, sexual identity, health, financial background, criminal investigations or court findings. According to the bill, these data may only be collected where use of such information is permissible under the German Equal Treatment Act, *i.e.*, where it is required for the position in question, and where decisions based on such information are legitimate, proportionate, and result from genuine requirements for the position.

Social Networks: The bill would explicitly prohibit potential employers from using social networking sites such as Facebook when conducting background checks and screening candidates/employees. Rather, employers should limit their searches to information on the internet that is ''publicly available,'' *i.e.*, not from social networking sites where membership is necessary to access that information. Searching on professional online networks such as LinkedIn or Xing would still be permitted where ''required'' and ''proportionate.''

In practice, it will be difficult in some cases to distinguish between the professional social networks that the bill deems ''primarily used for the presentation of professional qualifications,'' which may be consulted by employers, and other, purely social networks, use of which is prohibited in this context. In addition, information on member-only social networks is often ''publicly available'' because search engines may show content from protected web pages.

Medical Checks: Medical checks for candidates are permitted where ''important'' and ''essential'' for a particular position, and where consent has been obtained. The results may be shared with the applicant, but the potential employer may only receive information on whether the applicant is medically fit for the position (or not). Other tests on applicants are permitted under similar conditions, but only where they are based on scientific methods.

Employee Files: Employee data (unless provided by the applicant/employee without solicitation from the employer) may only be collected, processed, and used where proportionate and required for: (i) establishing the employment relationship; (ii) compliance with contractual or statutory requirements; or (iii) exercising employers' rights, including for the purposes of perfor-

[2] For further information on the timing and process, see (in German) http://www.bundesrat.de/cln_161/nn_6906/SharedDocs/Beratungsvorgaenge/2010/0501-600/0535-10.html?__nnn=true.

  PVLR ISSN 1538-3423

mance reviews. All third party recipients must be notified that they may only process data for the specific purposes for which the data were transferred.

Internal Investigations: Employee data may be collected for investigating criminal acts or serious breaches that would allow the employer to immediately terminate the employment relationship, but only where there is concrete suspicion and/or supporting evidence of criminal activity. Employers would generally be required to notify employees after collecting potential evidence. Without concrete suspicion against a particular employee or group of employees, the bill suggests that automated data verification programs should be used and only anonymous or pseudonymized data may be processed.

Any data collected during internal investigations that relate to an employee's private life may not be collected, processed or used. If collected, these data should be deleted immediately.

The bill would severely limit an employer's ability to conduct internal audits into misconduct that violates the employer's policies (as opposed to a criminal statute) or to monitor employee activity utilizing data loss prevention software or any other tools. Moreover, the functioning of internal audit or compliance departments may be seriously hampered.

CCTV/Video Surveillance: The bill provides detailed rules on the purposes for which video cameras may be installed in areas that are not publicly accessible, such as storage facilities or production plants. Here cameras would only be allowed for specific reasons (such as access control, protection of property, quality checks, or employee or facility security concerns), and where required for ''important operational reasons.'' Files must be deleted immediately, *i.e.*, without undue delay. There should also be ''appropriate measures'' to inform employees that cameras are installed. Covert video surveillance of employees of any kind would be prohibited. In all areas where the personal lives or privacy of employees may be affected, such as dormitories, locker rooms or washrooms, cameras are banned.

Mobile Devices: Employers would be able to process location data where required for the security of employees or for planning/coordinating staff. Tracking of location data would only be permitted where employees are notified of it in detail and only during working hours.

Tracking of location data would further be permitted to protect movable property. Tracking for this purpose would however not be allowed where the employee legitimately uses or possesses the property, but would allow employers to try to locate, for example, stolen company cars.

Monitoring the Use of Communication Devices: The bill confirms current interpretation and case law by the labor courts. Unfortunately, the bill fails to regulate monitoring where personal/private use of communication infrastructures is permitted, either expressly or implicitly and either continuously or on an occasional basis (as in many organizations).

Current interpretation provides that where private or personal use is permitted, the employer acts as a ''telecommunications services provider'' for employees and is thus subject to the even stricter data protection rules of the German Telecommunications Act, as well as telecommunications secrecy rules and regulations. As a result, where private use is permitted, the employer may not access private or work-related e-mails, nor any work related e-mails unless private and work-related e-mails can be clearly separated, e.g., through separate e-mail accounts.

Where an organization prohibits the personal use of its communication infrastructure, the bill differentiates between monitoring phone calls, and monitoring e-mail and internet use. The bill allows traffic and content data from e-mail and internet use to be collected, processed, and used, where necessary, for data security, for billing, for occasional performance controls, or where required for business continuity during absences or changes, but only if there is no overriding privacy interest of the employee to the contrary. Employees must be notified about any monitoring, and the details must be documented.

Telephone calls may be monitored only where there is specific notice in each case and only where there is consent from all parties on the phone call. When making telephone calls is one of the most important tasks of an employee, *e.g.*, for call center agents, monitoring is permitted without specific notice to the employee for occasional checks, provided there is general up-front notice, and the other party has agreed to the monitoring, *e.g.*, via a telephone script.

By permitting some limited monitoring only where employers prohibit personal use, the bill fails to address a commonplace situation in many organizations. Many employers prefer to allow some personal use of workplace communication infrastructures in order to accommodate their employees. However, in practice, under the bill, organizations operating in Germany would be well advised to prohibit any personal use of telecommunication devices. For this situation, technology use policies and labor contracts should clearly set forth that employees may not use their work e-mail account for any personal use and may not research the internet for private purposes. Ironically, the bill does allow monitoring for purposes of ensuring that the tools are not used for private purposes. The approach taken in the past of permitting personal use of telecommunication infrastructures in exchange for the employee consenting to some limited monitoring will no longer be available to employers since the bill clearly rules out consent.

Breach Notification: Different from the general breach requirements which apply to specific data such as sensitive personal data or credit card data only, under the proposed bill, employers will need to notify any affected employees of a breach (even if it involves only the employee's name or employee's work-related e-mail). The data protection authorities need to be notified in cases of serious breaches of an individual's rights and interests.

Conclusion:

As many of the concerns about the BDSG raised over the last few months are addressed in the bill, it is not surprising that it has been welcomed by the German Federal Data Protection Commissioner Peter Schaar as an ''acceptable compromise for both employees and employers and a substantial improvement'' on the status quo for the handling of employee data. Conversely—but also not surprisingly—the business community has called the bill disappointing: despite in-

troducing some reasonable and acceptable provisions, it has failed to provide detailed, practical guidance. Several of the provisions are insufficiently clear; others fail to address important practical problems. For example, most employers do allow their employees to use workplace e-mail and phone for occasional private use, and the bill fails to address this situation. One may hope that the language of the text will be improved before it is adopted by the German Parliament.

  PVLR ISSN 1538-3423