BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 16, Number 1 January 2010

Germany strengthens its Data Protection Act and introduces data breach notification requirement

By Jorg Rehder, Counsel, and Mauricio F. Paez, Partner, Jones Day.

In July 2009, the German legislature passed various controversial amendments to the *Bundesdatenschutzgesetz* (BDSG), Germany's *Federal Data Protection Act*.[1] While these amendments were not as extensive as many had initially hoped or feared, a few will undoubtedly have an immediate impact on companies doing business in Germany.

The amendments cover a range of privacy and business issues, including marketing use of data lists, administration of employee data, and contractual provisions in data transfer agreements. They also increase the maximum fines for violating data protection laws and grant greater powers to data protection authorities (DPAs). The most significant change, however, is a new requirement to provide notification for data breaches, a generic term encompassing any event that results in the compromise of the security or integrity of personal data. This requirement is similar in scope to state statutes in the United States, where 45 states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information, although the triggers for and the recipients of any notification vary on a state-by-state basis.[2]

Jorg Rehder *is of counsel in the Frankfurt office of the global law firm Jones Day. His practice focuses primarily on outbound and inbound corporate investments between Germany and the United States, specifically licensing and data privacy matters and general corporate, employment, and distribution issues. He can be contacted at: jrehder@jonesday.com.* **Mauricio F. Paez** *is a partner in the New York office of global law firm Jones Day. His practices focuses on technology, intellectual property and international corporate transactions, advising global clients in Asia, Europe, Latin America and the United States. He can be contacted at: mfpaez@jonesday.com.*

The BDSG

The BDSG prohibits the collection (the acquisition of data on the data subject)[3], processing (the storage, modification, transfer, blocking and erasure of personal data)[4], and use (any utilisation of personal data other than processing)[5] of "personal data", unless the affected individual (the data subject) expressly consents to the activity, or German law specifically authorises it.[6] Under the BDSG, "personal data" is broadly defined as any information concerning the personal or material circumstances of a natural person.

By contrast, California (like many other US states) more narrowly defines "personal information" as a prescribed combination of specific categories of data. Under the *California Computer Security Breach Notification* Act, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social Security number;

- driver's license number or California Identification Card number;
- account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account;
- medical information; and
- health insurance information.[7]

The "list privilege" exception

One of the widely disputed activities permitted by the BDSG is the "list privilege" exception. Under the previous "list privilege" exception, personal data such as a person's name, address, job title and year of birth may be used for a company's own advertising and marketing purposes and transferred to third parties (such as direct marketing companies) for similar purposes without the prior consent of the data subject, provided that such data is pooled in a list covering a group of people.

Under Section 28, paragraph 3, it is legal to transfer or use personal data for purposes of marketing and advertisement if the data, compiled in lists or otherwise combined, concern members of a group of persons and are restricted to:

- the data subject's membership of this group of persons;
- occupation or type of business;
- name;
- title;
- academic degrees;
- address;
- year of birth; and
- if there is no reason to assume that the data subject has a legitimate interest in his data being excluded from transfer.

Data subjects are entitled to object to such activities (under Section 6, paragraph 1 and Section 28, paragraph 4), but they rarely do. Many privacy advocates believe that this exception allows for large volumes of personal data to be sold at relatively low prices, particularly over the internet.[8] Accordingly, the amended BDSG requires the individual or legal person who is collecting, processing or using personal data (the "data controller")[9] to obtain consent from data subjects when engaging in any of these activities for the purpose of marketing or selling personal data (Section 28, paragraph 3), unless certain relatively simple conditions are met.

Consent is not required if the data is necessary for:

- marketing the data controller's own goods and services;
- advertising in a business context, eg for professional services; and
- advertising for charitable donations.

Aggregated personal data, eg data lists, can also be transferred without consent if:

- both the sender and the recipient keep records of the transfer for two years; and
- the advertisement clearly identifies the original collector of the data (*BDSG* Section 28 paragraph 3 and Section 34 paragraph 1a).

In recent years, Germany experienced a dramatic increase in data breaches and scandals involving the illegal trade of address lists and bank account information. For example, Deutsche Telekom lost personal data for about 17 million T-Mobile Germany customers in the spring of 2006 when thieves got their hands on a storage device containing personal data, such as names, addresses, cell phone numbers, birth dates and email addresses (including some for high-profile German citizens). T-Mobile Germany said it has taken multiple steps to shore up its security since the breach, including tighter restrictions on who has access to information, more complex passwords, and increased monitoring of security systems.[10]

In addition, some of the largest German companies in key industries, including transportation, finance, automotive, retail and healthcare, have been accused of encroaching on employees' constitutional rights to privacy,[11] eg by monitoring the personal data and activities of their employees. Some of these activities include:

- screening the workforce for corruption and automatic filtering, deletion and control of private emails of employees;
- spying on employees by compliance teams; and
- illegal storage and transfer of medical data of employees.[12]

Media coverage of these developments sparked widespread public interest among politicians, trade unions, and consumers on the mishandling of personal data. Consequently, a number of legislative proposals earlier this year centred on a complete abolition of the "list privilege."

However, in the face of looming German federal elections (held on September 27, 2009), many lawmakers were hesitant to institute any major legislative changes. Certain interest groups also claimed that data protection limitations on direct marketing would seriously harm entire industry sectors and lead to a higher unemployment rate, which was politically unacceptable. As a compromise, the German legislature passed the amendments to impose tighter restrictions on the commercial use of personal data while keeping the "list privilege" mostly intact. Most noteworthy among the amendments is the introduction of a data breach notification requirement.

   ISSN 1473-3579

Data breach notification

Under the amendments, data controllers must notify data subjects and DPAs of any unauthorised access or unlawful transfer of personal data, if the incident "threatens significant harm" to the rights and protected interests of the data subject (*BDSG*, Section 42a). The Act does not specifically define "significant harm," which means that companies are given a certain amount of leeway to determine whether an unauthorised or unlawful activity meets this threshold.

Nonetheless, if significant harm is threatened, then notification must be provided "immediately" after measures have been taken to secure the data and ensure that criminal investigations will not be adversely affected. This notice requirement is limited to a breach of certain kinds of data or data elements, such as bank or credit card information, "sensitive information," or information that is subject to professional or official confidentiality protections. The Act defines "sensitive information" as any information concerning an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, membership in a trade union, health or sex life (*BDSG*, Section 3, paragraph 9).

By contrast, in the United States, notification is typically triggered by unauthorised access or use of a data subject's name along with another identifying element, such as government-issued Social Security number, certain banking information, personal health information or other personal information that can be used to commit identity theft.[13] Thus, the German amendments require only a single trigger for notification while most US state statutes require two.

The amendments also provide guidelines for delivery of data breach notifications. For example, in cases where individual notification of an incident that affects a large number of data subjects is too burdensome, notice must be made via at least a half-page advertisement in at least two daily national newspapers or by other means that would provide similar exposure (*BDSG*, Section 42a). This requirement is similar to the substitute notice requirements under many US state statutes. Companies should carefully consider the reputational and public relations impact of making such a notification via newspaper or other media before doing so.

The costs of data breach notification

Although public disclosure of data breaches in Germany will probably bring to light many objectionable activities that may otherwise go unreported, the new notification requirement will add costs to companies operating in Germany or maintaining data that falls under German jurisdiction. In 2008, the average cost of a data breach in Germany was more than €2.41 million (approximately $3.5 million) per breach and €112 (approximately $165) per compromised record, which includes the average cost of notifications at €80,000 per breach or €4 per record. Data breaches with mobile devices are more expensive: lost or stolen laptop costs averaged €123.63 per data record compared with €106.85 for other data breaches.

The average cost is a composite of cost factors, which include:

- outlays for breach detection, escalation, notification, and response;
- fees for legal, investigative, and administrative services;
- losses due to customer defections, opportunity cost, and reputation management; and
- expenses associated with customer support, such as information hotlines and credit monitoring subscriptions.[14]

These figures are low relative to data breach costs in the United States because the previous *BDSG* did not require notification to data subjects or publication of data breaches. In the United States, where the majority of states require some form of data breach notification, the average cost of a data breach in 2008 was more than $6.6 million (approximately €4.5 million) per breach and $202 (approximately €137) per compromised record.[15] These costs are expected to grow in future years, particularly in connection with the anticipated increase in data protection or privacy litigation. Since 2005, the cost of a data breach has grown by nearly 40 per cent or more than $64 on a per-victim basis. In general, the US legal obligations and industry best practices related to a data breach – eg notification to individuals and state agencies, legal and reputational risk containment, and technical remediation – have proven to be more costly to businesses than other data protection and privacy safeguards required by US law. Such differences between the two countries suggest that the costs associated with a data breach in Germany, at least those related to providing notification, are likely to rise under the new *BDSG*.

A Europe-wide movement?

Further, it is important to note the possibility of a domino effect that Germany's data breach notification requirement may have on the European Union and its member states. The history of data breach notification requirements in the United States began when one state, California, enacted a data breach notification law in 2003.[16] Since then, a majority of US states have followed suit, and the U.S. Congress is now considering a national breach notification statute.[17]

While the implementation of the *EU Directive on Data Protection*[18] by individual member states has made the European Union one of the most highly regulated jurisdictions in the world with respect to protecting personal data, the European Union still has no general data breach notification requirement. There is evidence, however, that the European data protection landscape may be changing. The EU Council is in the process of amending its telecommunications directives to include an industry-specific data breach notification obligation for communication services providers.[19] Some neighbouring non-EU jurisdictions, such as Norway, already have laws requiring notice to DPAs of data breaches.[20]

The United Kingdom has a *de facto* notification law im-

posed through the UK independent data protection agency's recommendation that companies notify it of "serious" breaches. The Information Commissioner's Office does not specifically define what constitutes a "serious" breach but provides general guidelines and examples for making such an assessment; important factors for determining a "serious" breach include potential of harm to individuals and the volume and sensitivity of compromised data.[21] This may explain why there is ongoing debate on whether to adopt legislation[22] and the UK Parliament has considered such laws but declined to pass them.[23]

These conditions, along with Germany's recent amendments to its *BDSG*, suggest that EU member states, or the European Union as a whole, may be moving toward a more comprehensive data breach notification regime.

Other amendments to the BDSG

Protection of employee data

Any processing of employee data is permissible only if the processing is necessary for the administration, ie establishment, maintenance or termination of the employment relationship (*BDSG*, Section 32). For the purposes of investigating employee offenses, employee data can be collected only where:

- the data substantiates the suspicion that the employee has committed an offense in the context of employment;
- the collection, processing, and use of the data is necessary for the investigation; and
- the type and scope of the collection, processing and use of the data is proportional to the employee's protected rights and the circumstances of the investigation.

Contractual requirements for outsourcing

If a company outsources its direct marketing to a third party, the contracting entities must enter into a written agreement concerning the processing of the personal data. This agreement must meet ten new conditions to be valid and legally enforceable (*BDSG*, Section 11, paragraph 2). These conditions include, for example, scope, purpose, security measures, obligations, subcontracting rights, return or disposal of data and the requirement to audit the third party. Failure to conclude such a contract exposes each of the parties to a potential fine (BDSG Section 43, paragraph 1).

Practitioners believe that DPAs are likely to enforce this provision quite vigilantly because:

- the German public consistently expresses concern about direct marketing activities in Germany; and
- DPAs can quickly determine whether parties are in compliance with this requirement.

Protection of the data protection officer

A company's internal data protection officer (DPO), who ensures the company's compliance with Germany's data protection laws and acts as a contact person for employees on privacy matters, may be dismissed only for cause (*BDSG*, Section 4f, paragraph 3). The Act requires the following companies to appoint DPOs:

- all companies that have more than nine individuals regularly involved with automatic data processing;
- all companies involved in the commercial transfer of personal data; and
- companies involved with the commercial transfer of personal data for market research or opinion research purposes.

Special protection for the DPO extends until one year after the end of employee's term as the company's DPO, unless management has "important grounds" for terminating the DPO. Companies must also permit and finance the continued education and training of their DPOs on data protection matters. A natural, though probably unintended, consequence of this new provision is that many companies will invariably prefer an external DPO over an internal DPO. External DPOs are specifically permitted under the Act (BDSG, Section 4f, paragraph 2) and are less cumbersome to remove.

Increased power of DPAs

DPAs can order companies to remediate compliance, technical or organisational failures relating to the collection, processing and use of personal data (*BDSG*, Section 38, paragraph 5). Depending on the circumstances of the violation, they can also implement special data processing procedures or prohibit companies from collecting, processing or using personal data.

Stricter punishments

The maximum fine for failure to comply with data protection laws is now:

- **€50,000 (previously €25,000):** for ordinary offenses, eg failing to appoint a DPO, encrypt a data transfer or ensure that a third-party service provider meets the technical or organisational measures prescribed by the Act (*BDSG*, Section 43, paragraph 1); and
- **€300,000 (previously €250,000):** for serious offenses, eg accessing, collecting or processing data that is not publicly available, processing or using data beyond the scope of their authorised purpose, or failing to inform data subjects of a breach that may cause them "significant harm" (*BDSG*, Section 43, paragraph 2).

Moreover, if the data controller made profits that exceed €50,000 or €300,000, respectively, by violating data protection rules, then the authorities may raise the fine proportionally.

These revisions became effective September 1, 2009, although data collected prior to this date for marketing

   ISSN 1473-3579

purposes will be subject to a transition period under which the previous rules are effective until August 31, 2012.

Conclusion

Europe, like the United States and other countries around the world,[24] may be developing a trend for adopting data protection laws that include a general obligation to notify government agencies, individuals, or both of the unauthorised access or use of personal data. The amendments reflect a growing awareness of data protection issues among the European public and the potential for increased enforcement of data protection laws by European DPAs. For example, in September 2009, nearly 25,000 people took to the streets of Berlin to demand better protection of personal data,[25] and Germany's new coalition government has declared that it intends to pass legislation specifically concerning data protection for employees and in the workplace. These activities suggest that any infringement of data protection rules will become riskier.

To ensure compliance with the amendments and likely future legislation in the European Union, companies should at minimum:

- establish standard policies and operating procedures for data breach investigations, remediations and notifications related to personal data, which include data beyond that which would trigger notification under US law;
- assess and restructure the use or transfer of data lists and other personal data; and
- review and consider renegotiating service, employment and other data-related contracts.

In making these changes, companies may want to take advantage of the opportunity to evaluate their overall data protection practices and consider implementing a more holistic approach to data protection compliance that anticipates subsequent legislation in this area. To avoid business risks, including fines, audits and reputational damage associated with legal noncompliance, companies must properly focus their compliance efforts. Companies should consult with legal counsel for assistance in handling these matters.

NOTES

[1] *Bundesdatenschutzgesetz* [Federal Data Protection Act], December 20, 1990, BGBl. I at 2954, as amended.

[2] States with no data breach notification law are Alabama, Kentucky, Mississippi, New Mexico and South Dakota. State Security Breach Notification Laws, National Conference of State Legislatures, available at: http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotification-Laws/tabid/13489/Default.aspx.

[3] BDSG Section 3, paragraph 3

[4] BDSG Section 3, paragraph 4

[5] BDSG Section 3, paragraph 5

[6] BDSG Section 4, paragraph 1

[7] Cal. Civ. Code Ann. Section 1798.82(e) (2009).

[8] Jochen Lehmann, *Amendments to Federal Data Protection Law: Analysis*, Cecile Park Publ'g, Aug. 2009, available at: http://www.goerg.de/uploads/tx_kbgoerg/DPLPaugust09lehmann.pdf.

[9] Similar to the *EU Data Protection Directive*, the *BDSG* defines "data controller" broadly to refer to any person or body collecting, processing, or using personal data on his or her own behalf or commissioning others to do the same (*BDSG* Section 3 paragraph 7).

[10] "T-Mobile Lost 17 Million Subscribers' Personal Data," *Information Week*, October 6, 2008, available at: http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=210700232.

[11] *Grundgesetz* [Constitution of the Federal Republic of Germany]. Sections 1 and 2 of the German Constitution provide for the respect for "human dignity" and "personal freedoms" that have been interpreted by German courts to include the right to be free of employer monitoring, unless specifically provided for under the employment contract.

[12] *Privacy and Data Protection Law: European Developments*, Ernst & Young, July 2009.

[13] See, eg *California Computer Security Breach Notification Act*.

[14] See *Cost of Data Beach, Germany 2008 Annual* Study, Ponemon Institute, available at: http://www.encryptionreports.com/costofdatabreach.html.

[15] See *Cost of Data Beach, United States 2008 Annual Study*, Ponemon Institute, available at: http://www.encryptionreports.com/costofdatabreach.html.

[16] *California Computer Security Breach Notification Act*, Cal. Civ. Code Ann. Section 1798.82, *et seq.* (2009).

[17] S. 1490, 111th Cong. (2009) (entitled, "A bill to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information").

[18] Council Directive 1995/46, 1995 O.J. (L281) 31 (EC), at: http://ec.europa.eu/ justice_home/ fsj /privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[19] Resolution on the Common Position Adopted by the Council with a View to the Adoption of a Directive of the European Parliament and of the Council Amending

Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No. 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws, Eur. Parl. Doc.

(TA 360) 6 (2009), available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P6-TA-2009-0360.

[20] *Personal Data Act 2000*, Section 27 (Nor.), available at: http://www.legislationline.org/download/action/download/id/1102/file/2e3d6bb37cf550acba8549d9759d.pdf.

[21] See Information Commissioner's Office, Notification of Data Security Breaches to the Information Commissioner's Office, Mar. 27, 2008, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf.

[22] See, eg Tom Espiner, "Data Breach Law: IT Managers Say 'No,' " ZDNet UK, June 5, 2008, available at: http://community.zdnet.co.uk/blog/0,1000000567,10008370o-2000331828b,00.htm.

[23] See, eg House of Commons Justice Committee, First Report, 2007-08, H.C. 154 (recommending data breach reporting requirements under the Data Protection Act 1998), available at: http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf.

[24] Outside of the United States and the European Union, countries such as Australia, Canada and Japan have laws directly imposing data breach notification obligations. Alana Maurushat, *Data Breach Notification Law Across the World from California to Australia*, Univ. of New S. Wales L. Research Series (Paper No. 11), Apr. 2009, available at: http://law.bepress.com/cgi/viewcontent.cgi?article=1153&context=unswwps.

[25] "25,000 March for More Privacy from Authorities," *The Local: Germany's News in English*, at http://www.thelocal.de/society/20090913-21897.html.