MORRISON | FOERSTER

Legal Updates & News

Bulletins

German Data Protection Landscape is Changing

July 2009
by Karin Retzer

German Data Protection Landscape is Changing

PDF Version

Related Practices:

- Privacy and Data Security

Against the backdrop of widely reported data breaches, and with the September 2009 federal election drawing close, the German Parliament has voted for significant changes to existing data protection laws, including new requirements for credit checks, location tracking services, and telemarketing. Other amendments, including the introduction of U.S.-style data breach notification procedures and employee privacy rules, together with a prohibition on address trading without consent, are all under discussion. The following article summarizes recent privacy-related amendments in Germany, as well as a number of new developments that are in the pipeline.

New Rules for Scoring Techniques

With new rules on scoring techniques adopted June 12, the German Parliament has finally regulated a common practice. What is scoring exactly? The most frequently used type is a credit score or credit check that is based on a statistical analysis of a person's payment history, current income, etc. to determine the creditworthiness of that person. Banks and credit card companies use credit scores to evaluate the potential risk posed by lending money to consumers and thus mitigate losses due to bad debt. Credit scoring is, however, not limited to banks. Other organizations, such as online retailers, mail order services, mobile phone providers, employers and landlords, may use the same techniques.

To date, credit scoring had not been specifically regulated and, while very common, was carried out in a somewhat grey legislative area.

Further, despite pressure from industry and the German *Länder* (the federal states) the new rules also apply to consumer scoring techniques employed mainly for marketing purposes, such as the use of address data to customize marketing campaigns, but also to insurance providers for determining insurance eligibility and premiums.

The amendments, incorporated in the Federal Data Protection Act (the Bundesdatenschutzgesetz, or BDSG)[1] will become effective April 1, 2010.

In an effort to increase transparency, the amendments provide that individuals must be notified in advance if their data are to be used for scoring purposes. Where individuals' address data are used, the provision of notice to the individual must be documented. Upon request, individuals must be provided with detailed in-formation including the data used, an "understandable explanation" about the scoring technique employed, and the credit scores that have been recorded over the past six months. Moreover, an individual's credit score may not be lowered just because of exercising a right to access credit check information held about him or her (which is common practice in the United States).

The new rules allow financial institutions to share certain credit data with others, and in particular credit agencies, based on mere notice. Consent is no longer necessary.

The use of scoring to determine the conclusion, performance, or termination of contractual relationships, such as the eligibility for a credit, is permitted where (i) there is evidence that data pertaining to an individual can be used to conduct certain mathematically scientific probability calculations (a requirement that may be particularly problematic for marketing scoring), and (ii) general data protection requirements have been complied with. For the latter, opt-in consent may be required.

The new rules also establish, for the first time, when credit information may be used for scoring purposes. In brief, an individual's payment history information may be used and shared for scoring purposes if a previously adjudicated court insolvency order is in place, if an individual has formally acknowledged a debt, or if an individual has been provided with two or more unpaid demand letters sent over a time span of at least four weeks. Sharing of payment history information between affiliated entities is subject to the same requirements.

Substantial financial penalties for failure to comply with the new requirements have been introduced.

Opt-In for Consumer Telemarketing

The German Parliament also approved penalties amounting to €50,000 (approx. $71,000) for failure to obtain opt-in consent prior to contacting consumers by telephone for marketing purposes. According to the legislative materials, these penalties may be imposed on telemarketing agents and service providers, their customers, or any other organization engaged in telemarketing.

Under the existing Act against Unfair Trade Practices (the Unlauterer Wettbewerbsgesetz, or UWG), telemarketing to consumers is already subject to opt-in consent. The bill amending the UWG[2] requires that such consent contain "a declaration of will," and may not be determined merely based on the individual's behavior. The wording of the bill also clearly states that each and every call by telemarketers, even the very first one, would be covered by these restrictions. Telemarketing to businesses is permitted if it may reasonably be concluded that the recipient wishes to be contacted.

Further, marketers who fail to display their telephone numbers on caller ID systems may be fined up to €10,000 (approx. $14,000).

The amendments also enable consumers, who have not been appropriately informed of their right to with-draw from a service contract concluded at a distance (such as over the phone or via the Internet), to exercise this right of withdrawal, even in cases where portions of the services have already been rendered. This right would only expire when all portions of the services have been performed at the request of the consumer.

The right to withdraw could also extend to contracts concluded over the phone relating to the delivery of newspapers, periodicals, and magazines, or for gaming and lottery services. Such contracts are expressly excluded from the right of withdrawal provided for in the European Union Distance Selling Directive 97/7, but withdrawing from them looks set to become easier in Germany in the future. As so often happens, German consumer law would therefore be going further than corresponding EU law.

The German Federal Network Agency, which monitors developments in national telecommunications, gas, electricity, and railway markets, has been charged with supervising the new law. The generally held view is that these requirements will apply to telemarketing to German recipients, irrespective of the location of the provider. These amendments are expected to enter into force, without any transition period, at the end of July once published in the Official Journal.

Location Tracking Services

Amendments to the Telecommunications Act (the Telekommunikationsgesetz, or TKG)[3] which were approved recently by the German Parliament will seriously impede navigation, friend-finder, and other mobile services that require the continuous transferring of the user's location.

The amendments first require that telecommunications providers obtain "express, distinct, and written" consent from subscribers if the location of his/her de-vice is tracked and transferred to other subscribers, including to third parties (other than the value added-service provider). As a result, providers who offer sub-scribers the option of having their locations determined and forwarded (e.g., for friend-finder services or for tracking a misplaced device) will need to obtain distinct, written consent from these subscribers. Under German law, this means pen on paper or qualified digital signatures, since e-mail or click through consent is not sufficient. Moreover, the word "distinct" indicates that the consent wording may not be included in general subscriber terms and conditions, but must be separated from such text.

Second, the amendments permit providers to track a subscriber's location a maximum of five times. After the fifth time, the subscriber must be notified before further location tracking can take place (unless he/she has opted out of such notice). In addition, the law requires providers to accommodate the needs of disabled per-sons, such as by providing specific telephone tools for hearing-impaired persons.

The Network Agency has been charged with enforcing these rules, and failure to comply with the consent and notice requirements may result in penalties of up to €300,000 (approx. $420,000). Arguably, all location tracking services currently aimed at the German market are within the scope of the new requirements, including services provided by operators outside Germany.

These amendments will become effective once signed by the German president and published in the Official Journal. No transition period is provided for in the law.

Breach Notification, Strict Rules for Marketing, and Other Amendments

Designed to prevent and address recent data breaches, the German government has proposed further amendments to the Federal Data Protection Act[4] that, if approved by the Parliament, will provide for (i) the introduction of a mandatory breach notification regimen, (ii) the requirement to obtain opt-in consent for the secondary use of contact details for marketing purposes and in particular for data trading, (iii) in-creased enforcement, as well as (iv) a voluntary data protection audit scheme. However, due to the ongoing debate in Parliament and much criticism from industry, the bill amending the BDSG may not be voted into law before the summer break and the general elections. This means that under German constitutional rules the new government will have to present the bill anew.

As stated, one of the central elements of the proposal is the introduction of U.S.-style breach notification requirements in cases where any of the following sets of data are leaked: sensitive data, criminal records, bank account or credit card data, or personal data subject to legal privilege (e.g., data held by lawyers, doctors, journalists, etc.). The proposed rules only require notification in cases where the data leakages may lead to "serious impediments for privacy and other individual interests." The legislative commentary states that the types of data, as well as the possible results of the breach (such as damages or identity theft), must be taken into account when assessing whether such "serious impediments" exist. Both the data protection authorities, as well as all individuals concerned, must be notified "immediately" (as soon as reasonably possible) after containment and as soon as such notification no longer impedes law enforcement (principle of responsible disclosure). In cases where a broad public is concerned, public announcements in at least two national newspapers may replace individual notices. These announcements must be at least half a page tall. The notice should include information on the data leakage, possible results of the leakage as well as measures being taken to mitigate damages.

The breach notification requirement also extends to electronic communications providers and telecommunications operators in any case where user data (e.g., registration data obtained by a Web site operator) are leaked. Interestingly, public authorities are exempt from breach notification.

The provision of potentially greatest commercial significance is the abolition of the "list privilege," whereby contact details are traded amongst marketers. According to industry representatives, the proposed amendments would effectively kill legal trade in marketing data. Data collected prior to the entry into force of the amendments may

continue to be processed until July 2012. After that date, opt-in consent will be required, even for existing databases in which organizations may have invested significant resources, and data may need to be destroyed.

Under the list privilege system, data brokers as well as other organizations, process data lists consisting of names, addresses, dates of birth, professions, and other specified data for marketing and market research purposes, without prior opt-in consent. The draft amendments would make any processing of such data for marketing purposes, including market research, subject to opt-in consent.

The draft does provide an exception allowing processing based on opt-out consent in cases where (i) the details are used for marketing and market research purposes in relation to products or services of the data controller (which presumably excludes marketing and market research for affiliates), and (ii) all data have been collected directly from the individual. Marketing for charities as well as business-to-business (B2B) marketing seem to be exempt too, provided that the marketing is sent to the individual's work address and that it relates solely to products and services intended for commercial use. However, the wording for the B2B exception is awkward in that it restricts the exception to entrepreneurs and contractors, and does not seem to permit marketing to employees of larger enterprises. Where marketing or market research is permitted with opt-out consent, individuals must be able to opt out upon establishment of the relationship. Under existing law, opt-out options only had to be provided when follow up marketing contacts were made, not beforehand.

Where opt-in consent is required, consent must be provided in writing or through qualified digital signature. Electronic consent is permitted if documented and if individuals are easily able to retrieve the wording of their consent and or withdraw it at any point in time. Where specific circumstances render oral consent permissible, for example during a telephone conversation, the amendments now propose that such oral consent must be confirmed in writing.

Marketing consent must also be separate from other declarations (including the general data protection con-sent), and a separate signature, tick or click must be provided (and the confirmation obtained) in order to process data for marketing and market research purposes. Withdrawal of consent may not be subject to stricter requirements than those governing the entering into of the agreement. The rule under German law is that consent must be in writing, meaning pen on paper or by use of a qualified digital signature.

Last, the provision of products or services may not be made conditional upon providing consent for marketing, unless the individual may purchase similar products or services under reasonable conditions elsewhere, that is, where the provider has no monopoly and market conditions are not such that other providers impose the same requirement for consent. No further guidance is provided as to what would constitute "reasonable conditions" or "similar" products or services.

The draft also contains a number of proposals that are aimed at strengthening compliance and enforcement: Internal data protection officers (DPOs) may not be terminated during their term as DPOs, or during the 12 months thereafter, unless there is an "important cause" requiring immediate termination. Organizations must also compensate DPOs for training courses. Penalties are increased to a50,000 for failure to comply with formalities and to a300,000 for other data protection breaches (approximately $70,000 and $420,000, respectively). The draft expressly stipulates that higher penal-ties should be assessed to ensure that the penalties exceed the commercial gains that organizations may make from breaches. Further new penalties have been introduced, including for failure to comply with the restrictions on processing for marketing and market re-search purposes; or for failure to have detailed written data processing agreements in place with a data processor, irrespective of the location of that processor, and irrespective of whether the processor is an independent service provider or an affiliated entity. According to the German authorities, a master agreement between the parent and the provider is insufficient in cases where data relating to the German affiliate are processed.

Finally the amendments propose the introduction of a voluntary data protection audit with auditing and certification conducted by independent certified firms, in turn monitored by data protection authorities. The government would be charged with setting up a regulatory committee to develop guidelines for data security regulations covering private sector companies.

Employee Privacy

The German government has also reopened the debate on a proposed law to protect employee data, in response to recent breaches. Secretary of the Interior, Wolfgang Schãuble, who made the announcement Feb. 16, stated that

this law should address issues relating to the monitoring of employee communications and Inter-net usage in the workplace, as well as the use of video surveillance and GPS navigators tracking workers in company cars, and, in particular, the processing of personnel files and health data. “In certain cases, employers need to have the right to control employees,” Schãuble said, “but it is a question of the right proportionality.”

Peter Schaar, head of Germany’s Data Protection Commissioner’s Office in Bonn, alluded to recent breaches of employee data, stating that data “provided in the context of a work relationship should not be used for other matters,” and that the new law, if passed, would tighten restrictions on employee data in Germany.

The proposed law would come after a decade of fruit-less lobbying by privacy advocates about the need for an employee data protection act in Germany. Given this, it is still unclear whether the law will ultimately be enacted. Schãuble himself has warned that substantive discussions will only begin after the general elections. Until then, Schãuble has merely invited the German Labor Minister, the Minister for Economics, the Federal Data Protection Commissioner, and representatives of trade and industry to evaluate “whether there is a need for an employee data protection law.”

Conclusion

Given the current economic circumstances and the volatility of the German data protection landscape, organizations need to remain vigilant regarding data protection issues. Compliance with data protection and security requirements, while more and more challenging, is clearly the focus of growing scrutiny, and penalties for non-compliance are increasing.

Footnotes

[1] Gesetz zur Äderung des Bundesdatenschutzgesetzes. Available (in German) at http://dip21.bundestag.de/dip21/brd/ 2009/0536-09.pdf.……

[2] Gesetz zur Bekämpfung unerlaubter Telefonwerbung und zur Verbesserung des Verbraucherschutzes bei besonderen Vertriebsformen. Available (in German) at http:// dip21.bundestag.de/dip21/brd/2008/0553-08.pdf.

[3] Erstes Gesetz zur Äderung des Telekommunikationsgesetzes und des Gesetzes über die elektromagnetische Verträglichkeit on Betriebsmitteln. Available (in German) at http:// dip21.bundestag.de/extrakt/ba/WP16/154/15412.html.

[4] Gesetz zur Regelung des Datenschutzaudits und zur Äderung datenschutzrechtlichr Vorschriften. Available (in German) at http://dip21.bundestag.de/dip21/btd/16/120/1612011.pdf.