HUNTON& WILLIAMS

CLIENT ALERT

July 2009

Germany Adopts Stricter Data Protection Law — Serious Impact on Business Compliance

On July 3, 2009, the German Federal Parliament passed comprehensive amendments to the Federal Data Protection Act (the "Federal Act"). These amendments also passed the Federal Council on July 10, 2009, and the revised law will enter into force on September 1, 2009. The new amendments cover a range of data protection-related issues, including marketing, security breach notification, service provider contracts and protections for employee data. They also include new powers for data protection authorities and provide for increased fines for violations of data protection law provisions.

Change in Marketing Rules

Under the revised law, the processing and use of personal data for the purposes of selling addresses and using contact details for marketing will be permitted only if the individual has expressly consented to such use. There are, however, certain exceptions to this basic rule:

(i) Processing and use of existing data sets will continue to be governed by the old law until August 31, 2012. During the transition period, the so-called "list privilege" (permitting the transfer and use of certain data elements combined in lists) will continue to apply to previously collected data. The revised restrictions on processing and use of new data sets will apply beginning September 1, 2009.

(ii) Consent will not be required for the processing and use of certain data combined in lists, provided that the processing and use is necessary for one of the following purposes: (a) promoting the data controller's own offers if the data controller collected the data directly from the individual or from a public directory; (b) advertising regarding the professional services of an individual using a professional address; or (c) advertising for charitable donations.

(iii) Data contained in lists may be transferred without the individual's consent provided that: (a) information regarding the origin and the recipient of the data is retained for two years and (b) the advertisement identifies which data controller originally collected the data.

(iv) The data may be used for promoting third-party offers only if the advertisement states the identity of the data controller responsible for the data.

In addition to taking into account the new rules when planning marketing campaigns, data list sharing or third-party promotions, existing arrangements should be reviewed to evaluate whether there will be a legal basis for transfer and use after the August 31, 2012, compliance deadline.

Contacts

Lisa J. Sotto
200 Park Avenue
New York, NY 10166
(212) 309-1223
lsotto@hunton.com

Christopher Kuner
Park Atrium
Rue des Colonies 11
1000 Brussels, Belgium

Bridget C. Treacy
30 St Mary Axe
London EC3A 8EP

Dr. Jörg Hladjk
Park Atrium
Rue des Colonies 11
1000 Brussels, Belgium

Additional Lawyers
Cédric Burton
Purdey Castle
Natalie Hunt
Elizabeth H. Johnson
Ryan P. Logan
Manuel E. Maisog
Melinda L. McLellan
Olivier Proust
Boris Segalis
Aaron P. Simpson
Rachel M. St. John
Mason A. Weisz
John W. Woods, Jr.

Centre for Information Policy Leadership
Martin E. Abrams*
Paula J. Bruening
Fred H. Cate
Orson Swindle*

*Not a lawyer

Encryption as a Security Measure

Although the current law already recognizes encryption as an appropriate technical and organizational measure, a new amendment to the annex to Section 9 of the Federal Act will now explicitly refer to encryption tools and procedures as being appropriate for access control and safeguarding data transmission. Such encryption tools and procedures must reflect the "Stand der Technik" — state-of-the-art technology.

Introduction of Security Breach Notification Requirement

Data controllers will be subject to comprehensive breach notification requirements. The notification rules will apply to the following categories of data:

(i) sensitive data (as defined in the Federal Data Protection Act);

(ii) personal data subject to professional or official confidentiality obligations (e.g., data held by lawyers and doctors);

(iii) data concerning criminal acts or administrative offenses;

(iv) bank or credit card account details;

(v) customer data or traffic data as defined in the Telecommunications Act (e.g., data held by telecommunications operators, such as subscriber personal data and traffic data);

(vi) customer data or usage data as defined in the Telemedia Act (e.g., data held by electronic information and communication services providers, including registration or usage data that may identify an individual user).

Notification is required in the event of an unlawful data transfer or unauthorized access by third parties if the data loss is likely to have a serious impact on the rights or protected interests of the individuals concerned. The legislative commentary to the draft law indicates that both the types of data and the possible consequences of the breach should be taken into account when assessing whether the incident is likely to have a "serious impact."

Where notification is required, the data controller must notify the appropriate data protection authority and the affected individuals without delay. The notification must be made without delay (a) after appropriate measures have been taken to secure the data and (b) once criminal prosecution will no longer be affected. The law also specifies certain minimum content requirements for the notification.

Where notification to individuals would be disproportionately burdensome, particularly where a large number of individuals are affected, notice must be provided to the general public. Such notification must be made by placing at least a half-page advertisement in daily national newspapers, or by other means that would provide equivalent exposure for the notification.

Organizations will need to prepare incident response procedures and appoint an incident response team in order to ensure that any breach event is dealt with effectively, efficiently and in accordance with the legal notification requirements.

Detailed Requirements for Service Provider Contracts

Under the new law, contracts between data controllers and data processors will need to contain detailed data protection requirements. The law lists ten issues that must be covered, including, but not limited to, scope and purposes of the data processing, security measures, data processor obligations, subcontracting rights, audit rights, return of storage media and disposal. These requirements will affect contracts between German entities as well as contracts between foreign service providers and their German customers. Companies should review any existing contracts involving German companies to ensure that they comply with the minimum requirements imposed by the amended law.

Additional Protections Regarding Employee Data

The new law also provides greater protection for the collection, processing and use of employee data. It introduces a definition of employees and includes specific rules for the processing of employee data in the context of the employment relationship. As a basic rule, employee data may only be collected, processed or used if necessary for decision-making purposes when establishing, maintaining or terminating an employment relationship.

For the purposes of detecting criminal offenses, employee data may be collected and processed only if a number of specific conditions are met: (a) documented evidence must substantiate the suspicion that the individual has committed a criminal offense; (b) the collection, processing and use of the data must be necessary for the detection; and (c) the type and scope of the collection, processing and use of the data must be proportionate, considering the employee's protected rights and the circumstances of the investigation.

Because the new rules limit the activities companies may engage in when

investigating employees, they will have a significant impact on any internal investigations or employee screening efforts.

Greater Recognition for Corporate Data Protection Officers

Corporate internal data protection officers employed by the company will benefit from stronger employment rights under the new law. The employment relationship may not be terminated by management without good reason, and termination is not permitted for at least a 12-month period after the term as data protection officer has come to an end, unless management is entitled to terminate based on important grounds. Data protection officers will also be entitled to participate in continuing education and training courses at the organization's expense. Management should be aware of these changes to data protection officer employment status and may need to review current employment contracts or data protection officer appointment certificates accordingly.

New Powers for Data Protection Authorities

The amendments to the Federal Act also strengthen the powers of data protection authorities. For example, the data protection authorities will be empowered to order organizations to remediate compliance failures, including deficiencies relating to the collection, processing or use of personal data, or relating to technical or organizational failures. Where there are serious violations or deficiencies, the authorities will also be able to prohibit the collection, processing or use of data, or the implementation of individual data processing procedures, under certain circumstances.

Increase in Fines and Sanctions

The amendments to the law also increase the maximum fines for failure to comply with data protection formalities from the current €25,000 per violation to €50,000, and from €250,000 per violation to €300,000 for more serious violations of the law. In addition, even higher fines may be imposed for commercial gains realized as a result of the violation — a violating company may be forced to disgorge profits that exceed the amount it would normally have to pay in fines.

Conclusion

The new amendments to the Federal Data Protection Act will impact business activities across the board. From adapting marketing strategies, to renegotiating service provider relationships, to complying with new data breach notification requirements, now is the time for companies to review their data protection practices and consider implementing a more holistic approach. The new rules are likely to lead to increased interest in enforcement on the part of the data protection authorities. To avoid business risks including fines, audits and reputational damage, compliance efforts must be properly focused. Data protection compliance and risk management must be understood as core elements of good business governance with respect to customers as well as to employees.

We Can Help

Hunton & Williams' European Data Protection and Privacy practice assists clients in developing, implementing and evaluating data protection and data security programs to comply with German and European legal requirements. In addition, we have extensive experience counseling clients on all aspects of data breach response and in the development of security plans. If you would like assistance in reviewing your organization's data protection or data security practices, or developing new policies or procedures, please contact us.

Visit the Privacy and Information Security Law Blog at www.huntonprivacyblog.com for global privacy and information security law updates and analysis.