

Changes to German data protection law

*Dr Jörg Hladjk,
Associate at Hunton
& Williams, examines the
major changes brought in
by recent amendments to
German data protection
legislation*

The amendments to the Federal Data Protection Act, the Telemedia Act and the Telecommunications Act largely came into force on 1st September 2009, and have a far reaching impact, not least because of the introduction of the first ever statutory data security breach requirement. The amendments cover a range of issues in addition to security breach notification, including encryption and service provider contracts. They also include new powers for data protection authorities and provide for increased fines for violations of data protection law provisions.

The amendments will apply to all private sector organisations acting as data controllers and to their various activities. This article focuses on the main changes brought in by the revised Federal Data Protection Act ('revised Act') from a corporate compliance perspective.

Change in marketing rules

The revised Act introduced various changes to rules on marketing which, depending on the business model, may have to be taken into account by organisations in addition to the existing rules for email marketing in the German Unfair Competition Act, and the existing provisions on the use of customer data and usage data in the German Telemedia Act.

Under the revised Act, use of contact details for marketing will be permitted only if the customer has expressly consented to such use. The exceptions to this basic rule are:

Existing data sets — The processing and use of existing data sets will continue to be governed by the old rules until 31st August 2012. During the transition period, the so-called 'list privilege' will continue to apply to previously collected data. The revised restrictions on processing and use of new data sets apply since 1st September 2009.

Data combined in lists — Consent will not be required for the processing and use of certain data combined in lists, provided that processing and

use are necessary for one of the following purposes:

- a) promoting the organisation's own offers if it collected the data directly from the customer or from a public directory; or
- b) advertising regarding the professional services of a customer using a professional address.

Data contained in lists may be transferred without the customer'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 the data controller that originally collected the data.

When planning marketing campaigns, organisations should take into account the new rules. Further, existing arrangements should be reviewed to evaluate whether there is a legal basis for the transfer and the use of data after the 31st August 2012 compliance deadline.

Encryption

The Annex to section 9 of the Federal Data Protection Act required that where personal data are processed or used automatically, the internal procedures of an organisation must be structured in a way that meet the specific requirements of data protection. In particular, appropriate measures must be taken depending on the type of personal data or data categories to be protected.

Although the legislation previously recognized encryption as an appropriate technical and organisational measure, an amendment to the Annex now explicitly refers to encryption tools and procedures as being appropriate for access control, admission control and safeguarding data transmission. Such encryption tools and procedures must reflect the 'Stand der Technik' (state-of-the-art technology).

This amendment implies in particular that all websites that collect personal data online via web forms or through other means should be reviewed in order to determine whether encryption has to be applied to protect data during the electronic transmission

process. In addition, an assessment should identify the other areas of the organisation's functions where encryption may be necessary in order to comply with the requirements for access and admission control.

Security breach notification requirement

Organisations will be subject to comprehensive breach notification requirements. The notification rules will apply to a number of categories of data:

- i) sensitive data (as defined in the Federal Data Protection Act);
- ii) personal data subject to professional or official confidentiality obligations (for example, data held by lawyers and doctors);
- iii) data concerning criminal acts or administrative offences;
- iv) bank or credit card account details;
- v) customer data or traffic data as defined in the Telecommunications Act (for example, data held by telecommunications operators, such as subscriber personal data and traffic data); and
- vi) customer data or usage data as defined in the Telemedia Act (for example, data held by electronic information and communication service providers, including registration or usage data that may identify an individual user).

Notification is required in the event of unlawful data transfers 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'.

“The requirements for the service provider contracts will affect contracts between German entities as well as contracts between foreign service providers and their German customers. Organisations should therefore review any existing contracts involving German organisations to ensure that they comply with the minimum requirements imposed by the amended Act.”

Where notification is required, the data controller must notify the appropriate data protection authority and the affected individuals. 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 specifies certain minimum content requirements for the notification. The notification to the data subject must describe the nature of the unlawful disclosure and recommendations for measures to minimise possible detrimental con-

sequences. In addition, the notification to the competent supervisory authority must also include a description of the possible detrimental consequences of the unlawful disclosure, and include the measures taken by the company as a result.

Where notification to individuals would be disproportionately burdensome, particularly where a large number of individuals are affected, then the organisation may replace individual notifications with public announcements of at least half a page and in at least two national

daily newspapers, or by other means that would be equally effective in terms of informing the persons affected.

A notification which has been made by the entity liable to notify may be used in criminal proceedings (or in proceedings pursuant to the Act on Administrative Offences) against it only with its consent.

Failure to notify, notifying incorrectly, not completely or not in time, constitutes an administrative offence and is punishable with a fine of up to €300,000.

Organisations need to develop incident response procedures and to appoint an incident response team in order to ensure that any data breach is dealt with effectively, efficiently and in accordance with the legal notification requirements.

Detailed requirements for service provider contracts

Under the new Act, contracts between organisations acting as data controllers and data processors such as entities providing call center services, electronic archiving services or data destruction services, will need to contain detailed data protection requirements.

The revised Act lists ten issues that must be covered, including:

- the scope and purposes of the data processing;
- security measures;
- data processor obligations;
- subcontracting rights;
- audit rights; and
- return of storage media and disposal.

Failure to conclude the contract correctly, completely or not as legally required, will constitute an administrative offence punishable with a fine of up to €50,000. The same sanction applies where the data controller does not assess compliance of the data processor regarding the technical and organisational measures

(Continued on page 12)

(Continued from page 11)

taken by the latter before the data processing begins.

The requirements for the service provider contracts will affect contracts between German entities as well as contracts between foreign service providers and their German customers. Organisations should therefore review any existing contracts involving German organisations to ensure that they comply with the minimum requirements imposed by the amended Act.

Additional protections regarding employee data

The new law 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 an 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 offences, employee data may be collected and processed only if a number of specific requirements are met:

- a) documented evidence must substantiate the suspicion that the individual has committed a criminal offence;
- 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 that organisations may engage in when investigating employees, they will have a significant impact on any internal investigations or employee screening efforts.

Greater protection for corporate data protection officers

Corporate internal data protection officers employed by an organisation will benefit from stronger employment rights under the new Act. 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 on important grounds.

Data protection officers will also be entitled to participate in continuing education and training programs at the organisation'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

Under the revised Act, the data protection authorities are now empowered to order organisations to remedy compliance failures, including deficiencies relating to the collection, processing or use of personal data, or to technical or organisational measures. In the event of 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, in certain circumstances.

Increased fines and sanctions

The amendments to the Act 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, still higher fines may be imposed for commercial profits resulting from a violation — a violating organisation may be forced

to hand over its 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 of organisations across the board.

From adjusting marketing practices, implementing encryption measures, to renegotiating service provider relationships and complying with new data breach notification requirements, now is the time for organisations to review their data protection practices and consider implementing a more holistic approach. The new rules are likely to lead to stronger interest in enforcement on the part of the data protection authorities.

Compliance efforts must be properly focused to avoid business risks including fines, audits and reputational damage.

Data protection compliance and risk management must be understood as core elements of good business governance with respect to customers.

Dr Jörg Hladjk
Hunton & Williams
jhladjk@hunton.com
