

This article was first published on www.complinet.com. Reproduced with permission.



August 27, 2009

Germany adopts stricter data protection law—impact on financial services companies



by Dr. Jörg Hladjk, a German-qualified associate in the European Data Protection and Privacy Practice at Hunton & Williams, Brussels. He may be contacted at jhladjk@hunton.com.

On July 3, 2009, the German federal parliament passed comprehensive amendments to the Federal Data Protection 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 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 financial services companies and their various activities acting as data controllers with respect to customer data. The new rules will affect departments such as marketing, IT and legal.

Change in marketing rules

Under the revised law, using contact details for marketing will be permitted only if the customer has expressly consented to such use. There are, however, certain exceptions to this basic rule. From a financial services company perspective, the following are most relevant:

- The old law will continue to govern processing and the use of existing data sets until August 31, 2012. During the transition period, the so-called “list privilege” will continue to apply to previously collected data. The revised restrictions on processing and the use of new data sets will apply from the beginning of September 1, 2009.
- 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:
 - Promoting the financial services company’s own offers if the financial services company collected the data directly from the customer or from a public directory.
 - 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:
 - Information regarding the origin and the recipient of the data is retained for two years.
 - The advertisement identifies which data controller originally collected the data.

In addition to taking into account the new rules when planning marketing campaigns, financial services companies should review existing arrangements to evaluate whether there will be a legal basis for the transfer and use of data after the August 31, 2012 compliance deadline.

Introduction of security breach notification requirement

Financial services companies will be subject to comprehensive breach notification requirements. The notification rules will apply to a number of categories of data. From a financial services company perspective the category of “bank or credit card account details” is most relevant. Notification is required in the event of an unlawful data transfer or unauthorised access by third parties if the data loss is likely to have a serious impact on the rights or protected interests of the customers concerned.

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

Where notification to customers would be disproportionately burdensome, particularly where a large number of individuals are affected, notice must be provided to the 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.

Failure to notify, not notifying correctly, or not completely, or not in time, constitutes an administrative offence and can be sanctioned with up to €300,000. Financial services companies will, therefore, need to prepare incident response procedures and appoint an incident response team 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 financial services companies and data processors, such as entities that provide call centre services, electronic archiving services or data destruction services, will need to contain specific requirements. The law lists 10 issues that must be covered, including:

- 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 German financial services companies. Financial services companies should, therefore, review any existing contracts that involve German companies, to ensure that they comply with the minimum requirements that the amended law imposes.

Greater recognition for corporate data protection officers

Corporate internal data protection officers that financial services companies employ 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 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

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 financial services companies to remediate compliance failures, including deficiencies in relation to the collection, processing or use of personal data, or in relation to technical or organisational 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 realised as a result of the violation — a violating company may be forced to disgorge profits that exceed the amount that it would normally have to pay in fines.

The new amendments to the Federal Data Protection Act will impact business activities of financial services companies 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.