

The topic of sensitive data loss has stayed hot for a while now. Publicly announced incidents usually draw much attention, which can be easily explained by the fact that basically everyone can be affected by deliberate or accidental data loss.

Despite serious technological and organizational measures data leakages continue to occur. Below several much touted in 2009 in Germany data leakages are represented.

Number of lost records	Incident description
7.5 Mln.	A serious vulnerability in the social network StayFriends GmbH ( <a href="http://www.stayfriends.de">www.stayfriends.de</a> ) provided access to the personal data of all registered users.
563.640	One of the biggest German online bookstores Libri.de suffered customers' personal data leakage. According to Spiegel, about 563.640 invoices with customers names, addresses, orders history and accounts numbers became public.
2.400	The D.C. agency that handles college financial aid requests had accidentally e-mailed personal information from 2.400 student applicants to more than 1.000 of those applicants. The information included student names, e-mail and home addresses, phone and Social Security numbers and dates of birth.

For businesses protection of their classified information is a priority, as business sustainability and efficiency to a great extent depend on how well sensitive information is protected.

The loss of confidential data, such as customer database, intellectual property, financial or legal documentation, market research or personal data can badly affect businesses of any size. Sensitive data leakage can result in direct financial loss, for example when competitors get hold of commercial or technological data or in indirect reputational loss.

What are the legal consequences of data leakages and what rules govern data processing in businesses? What compliance requirements businesses should meet to operate in Germany?

## Governmental Data Protection Requirements

On July 3, 2009, the German Federal Parliament passed comprehensive amendments to the **Federal Data Protection Act** (the "Federal Act"). The revised law entered into force on September 1, 2009. It covers a range of data protection-related issues, including marketing, security breach notification, service provider contracts and protection of employee data. New powers for data protection authorities are named and fines for violations of data protection law provisions are increased.

Let's review the revised data protection requirements.

### Change in Marketing Rules

The processing and use of personal data for the purposes of selling addresses and using contact details for marketing is permitted only if the individual has explicitly consented to such use. The exceptions of this basic rule are:

1. Processing and use of existing data sets is governed by the old law until August 31<sup>st</sup> 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 apply beginning September 1<sup>st</sup>, 2009.
2. 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

- c. advertising for charitable donations.
3. 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
  - b. the advertisement identifies which data controller originally collected the data.
4. 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.

Planning their marketing campaigns, data-list sharing or third-party promotions companies should adhere to the new regulations. Moreover 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.

## Encryption

The annex to Section 9 of the Federal Act now explicitly refers to encryption tools and procedures as appropriate tools for access control and safeguarding data transmission. Such encryption tools and procedures must reflect the "Stand der Technik" — state-of-the-art technology.

## Security Breach Notification Requirement

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

1. sensitive data (as defined in the Federal Data Protection Act);
2. personal data subject to professional or official confidentiality obligations (e.g., data held by lawyers and doctors);
3. data concerning criminal acts or administrative offenses;
4. bank or credit card account details;
5. 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);
6. 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. 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.

## Requirements for Service Provider Contracts

Under the new law, contracts between data controllers and data processors 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 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 of 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:

1. documented evidence must substantiate the suspicion that the individual has committed a criminal offense;
2. the collection, processing and use of the data must be necessary for the detection;
3. 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 of the contract with 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 amended Federal Data Protection Act seriously impacts business activities. 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.

## Internal Information Security Solutions for Legal Compliance

**InfoWatch** develops high-tech packaged solutions in the field of internal information security, including data leakage prevention (DLP). InfoWatch solutions protect sensitive and classified information against various risks, including deliberate theft and negligence to provide compliance with data protection requirements.

With its more than 7 year experience in data protection technologies **InfoWatch** has elaborated strategic approach to the development and implementation of data loss prevention and encryption solutions. Our comprehensive solutions enable businesses to control all major risks and prioritize their data security efforts despite the ever increasing number of data loss accidents.

**InfoWatch** products target enterprises and small and mid-sized businesses. The data protection product line includes:

### Data Leakage Prevention Solutions

For enterprise customers

- **InfoWatch Traffic Monitor Enterprise** – a comprehensive solution, that gives enterprises full control over sensitive data flow via all common data transmission channels (e-mail, web, instant messengers)
- **InfoWatch Device Monitor Enterprise** - a packaged solution, that provides control over the most commonly used portable devices, removable media (CD/DVD, USB, COM) and local and network printers

For SMB customers

- **InfoWatch Data Control** – an easy-to-use DLP solution, especially optimized for the needs of SMB customers

### Encryption Solutions

For enterprise and SMB customers

- **InfoWatch CryptoStorage Enterprise** – an encryption solution that protects enterprises and SMBs against unauthorized access to confidential data

**InfoWatch** solutions have been successfully implemented and are being used by leading international and Russian companies and governmental institutions.

---

### Contacts:

[www.infowatch.com](http://www.infowatch.com)

Proezd #607, build. 30, off. 507,123458, Moscow, Russia

Tel.: +7 (495) 22 900 22

[sales@infowatch.com](mailto:sales@infowatch.com)

[sales-oem@infowatch.com](mailto:sales-oem@infowatch.com)

### Regional Representatives:

Austria and Switzerland: [sales-ach@infowatch.com](mailto:sales-ach@infowatch.com), +49 (8152) 969340

Germany: [sales-de@infowatch.com](mailto:sales-de@infowatch.com), +49 (4207) 689933

Benelux, France and Mediterranean: [sales-be@infowatch.com](mailto:sales-be@infowatch.com), +32 477920909

India: [sales-in@infowatch.com](mailto:sales-in@infowatch.com), +91 9833799299