

## IT Ticker

### Overview of topics:

- **Foreword**
- **Data protection officer**
- **Protection of employee data**
- **Data security**
- **Commissioned data processing**
- **Scoring and credit agencies**
- **Stricter requirements regarding prior consent**
- **Advertising using proprietary data**
- **Advertising using third-party data**
- **Duties to provide information and publish in the event of violations of data protection**
- **Aggravated regulations regarding administrative fines and penal provisions**
- **Entry into force and transitional provisions**
- **Need for action**

### Foreword

In this special Issue of our IT Ticker, we would like to inform you of some of the main points of the two reforms of the German Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) in the year 2009.

The first reform relates to "scoring" and the activities by credit agencies; it was adopted by the German Federal Parliament on 12.05.2009. The second reform was preceded by data scandals and intensive discussions regarding their consequences, such as the abolition of the "list privilege". That reform was adopted by the German Federal Parliament on 03.07.2009 and approved by the German Federal Council on 10.07.2009. The planned "Data Protection Audit Act" was not adopted. Large parts of the amendments will apply as early as from **01.09.2009**.

In this special Issue of our IT Ticker, we set out some of the central issues of both reforms, which will result in various changes to the BDSG.

### Data protection officer

The position of the data protection officer is strengthened. Business enterprises engaged in the anonymized transmission of data, or in market or opinion research, now

must always commission a data protection officer, regardless of their number of employees (sec. 4f para 1 BDSG). Data protection officers may only be dismissed for good cause and will now also be granted special protection against termination of their employment contract (sec. 4f para 3 BDSG). During their term of office and for one year thereafter, their employment contract may only be terminated for good cause. Their position is, therefore, comparable to that of a member of a works council. The body responsible for data processing is now expressly obliged to provide data protection officers with opportunities for education and training and has to bear the related costs. The previous requirements (such as the data protection officer's qualification) will continue to exist unchanged.

Martin Schweinoch, Munich

### Protection of employee data

A special provision (sec. 32 BDSG) has been introduced in relation to all measures relevant to data protection in connection with employment relationships.

For the purpose of an employment relationship, personal data may now only be collected, processed or used to the extent that is necessary for its initiation, performance or termination. The collection, use or processing of any such data to detect a criminal offence is (only) admissible if there is documented evidence that the person concerned committed a criminal offence (*Straftat*) within the framework of his or her employment relationship.

The revision is problematic in various respects. For example, the requirement of documented evidence of a criminal offence committed by the data subject will result in the employer acting lawfully only if the employer is able to use as a basis a documented initial suspicion. This will also affect certain elements of Compliance programmes, which were introduced in many business enterprises at great expense with the objective of preventing not only criminal offences but also administrative offences (*Ordnungswidrigkeiten*), and which cannot work without preventive control and the related use of personal data.

The duty to document the actual evidence of a specific suspicion also appears to be problematic. As a result of that duty, employers are required, in order to prove their compliance with that duty, to also keep the documentation even if the suspicion has dissipated, i.e., the employer is

required to store even more data than before. What is also quite unclear is the relation between the duty to document and the unchanged duties regarding the erasure and blocking of data (sec. 35 BDSG).

Those amendments in respect of employment relationships also apply to non-electronic data. In future, any collection, processing or use of data will be covered, regardless of the form of the storage or transmission, including purely physical notes. Notwithstanding the omnipresent IT, the scope of applicability of the BDSG is thereby massively extended. For example, data collections over the phone (e.g., a call to a former employer of an applicant), in relation to performance and conduct control (e.g., the monitoring by a camera), and handwritten notes regarding a job interview will also be covered.

The amendment aims to be a first step towards an act concerning the protection of employee data. Unfortunately, the revision results in uncertainties regarding interpretation and leaves important practical questions unanswered. One thing is certain, though: There exists no area in connection with employment relationships that is not covered by the scope of data protection, and business enterprises will have to prepare for that fact in a very short term.

Udo Steger, Munich

### Data security

The statutory objective of data reduction and data economy was reworded (se. 3a BDSG) and now generally covers the collection, processing and use of personal data. Still, the principle applies that as little personal data as possible is to be collected, processed or used. Personal data must now, however, be anonymized or pseudonymized, to the extent as is technically possible in line with the intended use and provided that the effort involved is reasonable. Enterprises ought to review accurately whether they are required to adjust their procedures accordingly, e.g. because too much data is stored or stored data is not rendered anonymous or pseudonymized in good time.

The new sec. 30a BDSG also contains provisions regarding anonymization and pseudonymization, according to which data collected or stored for market or opinion research purposes may only be processed or used for that purpose. Data from not generally accessible sources may only be processed or used for the specific research

project, for which the data was collected. A use for any other purpose is only admissible in anonymized form, i.e., if no reference to a person can be established (first alternative of sec. 3 para 6 BDSG).

Now, there exist graded duties: Personal data must be anonymized (sec. 3 para 6 BDSG), once this is rendered possible by the purpose of the market or opinion research. Until such time, the data must be pseudonymized (sec. 3, para 6a BDSG) and that pseudonymization may not be removed, save for a few exceptions. Violations of sec. 30a BDSG are subject to a fine. The affected enterprises ought to adjust their procedures shortly, and document the adjustments. In combination with the duty to store the data origin that provision has a particularly high significance, as violations can thus be proven especially easily.

A revision of a rather technical nature was introduced in the annex to sec. 9 BDSG, according to which the encryption of data is now "in particular" included in the measures required to be taken to warrant access and transmission control. According to the wording "in line with the state of the technology", advanced procedures must be used, which have stood the test of practice and warrant a high standard of security. In practice, most of the procedures considered to be safe and effective ought to be applicable, some of which have also, in part, already been included in operating systems and applications. Ultimately, enterprises are now subject to a higher requirement of encrypting each single data storage device and to instruct data processors accordingly. As is well known, the reality often differs, so that there is need for action in that respect.

Udo Steger, Munich

### Commissioned data processing

The regulations regarding commissioned data processing (sec. 11 BDSG) will also become stricter: The written commission now has mandatory contents, which must reflect certain essential measures regarding the handling of personal data in detail. These contents also include the scope, type and purpose of the handling of the data, the technical and organisational actions to be taken, the data processor's control duties, the data controller's rights of control and authority to give instructions etc. The data controller is now also obliged to inspect the data processor's technical and organisational measures prior to the commencement of the data processing and on a

regular basis thereafter, and to document the results of those examinations.

The objective pursued by the legislator thereby is to require detailed determinations and serious examinations, as there had been, in the legislator's view, material deficits in that area in the past. That approach is underlined by the fact that an improper commissioning and a failure to check the data processor in advance will in future constitute administrative offences, punishable by a fine of up to EUR 50,000.00 (sec. 43 para 1, subpar. 2b BDSG).

Those provisions also apply to (remote) maintenance work by third parties in relation to IT systems, if in connection with such work - as it is true in most cases - access to personal data cannot be excluded (sec. 11 para 5 BDSG).

Pending the entry into force of the amendments on 01.09.2009, the contracting parties of commissioned data processing are required to document the existence of proper conditions in line with the new requirements.

Martin Schweinoch, Munich

### Scoring and credit agencies

The first reform of the BDSG in 2009 deals with data protection issues in relation to scoring and the transmission of data to, and by, credit agencies.

Firstly, the term "automated individual decision" is defined (sec. 6a BDSG) and the applicable conditions were aggravated: Upon request, the material reasons for a decision to the detriment of the data subject must be notified and explained.

The requirements in relation to the admissibility of scoring procedures (sec. 28b BDSG) are now dealt with separately. For decisions regarding the establishment, performance or termination of a contractual relationship with the data subject, probability values relating to the data subject's future conduct may only be collected or used if it can be demonstrated by using a mathematical-statistical procedure that the type of data used for their calculation is essential for the probability of that conduct. It can be concluded from the wording that scoring procedures for advertising purposes are not covered. The question remains, however, whether those procedures can be structured completely "unscientifically". As regards the highly disputed address data, a compromise applies to the effect that scoring procedures may not be based exclusively on address data. When using address data, the data subject must be informed thereof (such as in General Terms and

Conditions). At the same time, the data subject's rights to information were extended considerably. If requested by the data subject, the body responsible for the decision (e.g., an online-shop) must provide the data subject with information regarding the probability values that were collected or stored for the first time, within a period of six months before the data subject's request (sec. 34 para 2 BDSG). In addition, the type of data used to calculate the probability values, as well as the creation and meaning of the probability values, must be notified in relation to the individual case in a generally understandable manner. This will have considerable consequences in relation to the storage procedures and the correspondence with data subjects.

The requirements regarding admissible notifications to credit agencies were redefined (sec. 28a BDSG). In respect of so-called "negative data", the requirements basically follow the precedents already established by court rulings. The requirements regarding the transmission of "positive data" are also provided for. It remains unclear, however, for what positive data a prior consent will still be required. Regardless of that, the notifying enterprise must correct its notifications, while details (materiality of modifications) still remain unclear also in that respect.

The reformed BDSG does not contain a definition of "credit agency", either. However, a description is contained in sec. 29 para 6 BDSG as a result of the Act Regarding the Implementation of the Consumer Credit Directive (*Gesetz zur Umsetzung der Verbraucher-kreditrichtlinie*). It must be noted that group-internal payment history databases may also be covered by the term "credit agency", and thus by the amended BDSG.

Dr. Wulf Kamlah, Frankfurt/M.

### Stricter requirements regarding prior consent

Of particular importance to the practice are stricter formal requirements regarding the prior consent by the data subject. This is true both in relation to prior consents in General Terms and Conditions and the oral collection of data.

An effective prior consent may not be "hidden" in General Terms and Conditions. Rather, an express and typographically prominent arrangement of the declaration of consent is required. The provisions regarding the prior consent must clearly stand out against the other provisions and must be highlighted. Thereby, the legislator

has implemented into the BDSG the provisions of the rulings by the German Federal Supreme Court (*Bundesgerichtshof*) of 2008 (such as the "Payback decision"). Even stricter regulations, which had been demanded initially, were not made. A cumbersome procedure is provided in relation to the oral collection of data. Following the granting of an oral consent, such as in a conversation with a call centre, the enterprise must provide the data subject with a written confirmation thereafter. That change in media poses a special challenge for enterprises.

The practical consequence of the revision is that enterprises must adjust their General Terms and Conditions in order to be able to use customer data comprehensively in future and to avoid infringements of the law.

Stefan C. Schicker, LL.M., Munich

#### Advertising using proprietary data

Also under the amended BDSG, the advertising directed at an enterprise's own customers for goods and services provided by the enterprise itself does not require the prior consent by the addressee, if the data was collected by the enterprise itself.

Interestingly, according to the new regulations, this also applies to third-party advertising distributed together with an enterprise's own advertising ("enclosed advertising", "*Beipackwerbung*"). What is merely required is that the data subject knows the responsible body which sent the principal advertising to him. Furthermore, the sending of advertising in relation to the recipient's occupational activities to the recipient's business address continues to be admissible.

Stefan C. Schicker, LL.M., Munich

#### Advertising using third-party data

One of the most disputed topics was the so-called "list privilege". Previously, it was admissible to use and transmit certain data compiled in the form of a list (name, title, academic degrees, address, year of birth, occupational title, the belonging to a specific group of persons) for advertising purposes without the data subject's prior consent. This was considered as a trigger of many data protection scandals. Initially, the declared objective of the legislative procedure was to abolish the list privilege completely. While in the end the list privilege has been kept, substantial restrictions were imposed.

In future, summarised personal data may only be transmitted for advertising purposes and used by the data recipient if the addressee of the advertising is able to clearly identify the body responsible for the use of the data. It must be evident to the data subject where the data came from or, as the case may be, who collected that data.

In addition, the body transmitting the data is obliged to store information on the origin of the data and the identity of the data recipient for a period of two years following the transmission and to provide the data subject with information regarding the origin of the data and the recipient. These duties to store and provide information also apply to the data recipient.

The primary intent and purpose of the duties to store and provide information is to facilitate the exercise of the data subject's right of objection in relation to the use of the data. The data subject must also be informed of the right of objection. As a consequence, it is now easier for the data subject to declare his objection both to the body collecting his data and the recipient of the data, thereby blocking his data for the use and transmission for advertising purposes.

These restrictions in relation to the list privilege will have serious consequences for enterprises dealing with addressees, but also for their customers, enterprises from the Internet and mail order industry, and the publishing industry. When collection data of new customers, from 01.09.2009 on, entities that collect and/or use data as described above must accurately comply with the new regulations in order to avoid administrative fines, or even criminal liability.

Dr. Daniel Kaboth, Munich

#### Duties to provide information and publish in the event of violations of data protection

The reformed BDSG contains completely new duties to provide information to the regulatory authority and the data subject in the event of data abuse. Failure to comply with those duties is punishable by a fine. The duties apply if data particularly worthy of protection becomes known outside the enterprise in an unlawful manner, thus potentially seriously impairing the data subject's rights or interests worthy of protection (sec. 42a BDSG).

The following data is particularly worthy of protection: (a) data regarding racial or ethnic origin, political opinions, religious or philosophical convictions, union membership,

health and sex life, (b) data subject to professional secrecy, (c) data regarding (potential) criminal or administrative offences by the data subject, as well as (d) bank and credit card information. For example, if an enterprise becomes aware of the fact that its customers' bank or account data was unlawfully transmitted to third parties (such as through address trading), the enterprise must notify the regulatory bodies and the data subjects.

The notification must be made without undue delay after the enterprise becomes aware of the data abuse. The information of the data subject may be delayed, however, until suitable measures regarding data backup have been taken and prosecution is no longer jeopardised. The objective is to avoid informing wider circles of security gaps and to not warn offenders unnecessarily. If the direct notification of the data subjects requires unreasonable efforts (e.g., owing to their number), the enterprise must provide information on half a page in two daily newspapers circulated nationally, or by equivalent measures.

The data subject must be informed of the type of the data abuse and recommendations to avert damage. The notification to the competent regulatory authority must contain potential adverse consequences and protective measures taken by the enterprise.

While those notifications may only be used to a limited extent in criminal or administrative procedures against the enterprise required to protect the data (sec. 42a BDSG), a more significant effect will be the negative publicity as a result of mandatory information regarding data abuse, as was shown by the latest data scandals.

Sabine Kröger, Munich

#### **Aggravated regulations regarding administrative fines and penal provisions**

The administrative fines for violations of data protection were increased considerably. In addition, the BDSG now also sanctions other breaches of duty. The maximum range of a fine for less severe administrative offences was doubled from EUR 25,000 to EUR 50,000.

Severe administrative offences are now punishable by a fine of up to EUR 300,000. That range can even be exceeded if the financial benefit gained by the offender as a result of the administrative offence was higher. In this case a higher fine may be imposed.

Also, new regulations regarding administrative fines were

introduced. These relate to automated retrieval procedures (sec. 10 BDSG), in relation to which the storing body must ensure that the data transmission can be monitored, at least by suitable sampling procedures.

New sanctions also apply to commissioned data processing. An administrative offence will exist if the individual requirements regarding the commissioning (second sentence of sec. 11 para 2 BDSG) are not met, or if the data controller fails to verify in advance the technical and organisational measures of the data processor. Therefore, the commissioning agreement ought to be worded very carefully and its preparation should be well documented. An administrative offence will also exist if the process required by the data subject to object the use of its data for advertising, or market and opinion research, is made subject to stricter formal requirements than the process under which the data was obtained.

Responsible bodies transmitting data to credit agencies must transmit to the credit agency subsequent changes within one month. A violation of that provision will also constitute an administrative offence. This is likely to affect anybody who transmits to credit agencies notifications regarding their debtors.

The data subject's rights to information are strengthened, as an administrative offence will now also exist if specific information is not provided properly, or if other related duties are violated. Now is the time to define clear processes within the enterprise in relation to requests for information by data subjects.

New sanctions are also imposed in relation to those new "less severe" administrative offences, subject to fines of up to EUR 300,000. Those sanctions will apply if the conclusion of the contract with the data subject is made subject to the data subject consenting to the use of his data for address trading or advertising purposes, while the data subject has no other reasonable access to equivalent services without that consent. The same sanctions are threatening if personal data is used for advertising, market or opinion research despite an objection by the data subject.

Duties regarding the anonymization of personal data are also of particular importance: If the anonymization is reversed in specific cases by consolidating a specific feature with individual details, this will also constitute a severe administrative offence.

Dr. Oliver Bühr, Frankfurt/M.

### Entry into force and transitional provisions

A substantial number of the amendments to the BDSG will enter into force as early as on 01.09.2009, i.e., in less than two months.

Three exceptions apply: The regulations regarding scoring and credit agencies (see above) will apply from 01.04.2010. Likewise, the amendments regarding the provision of information to data subjects, including the new storage duties, will enter into force on 01.04.2010. The applicability of the amended sec. 28 BDSG ("list privilege") is graded: From 01.09.2009, the revised regulations will apply to data collected or stored for the first time. Only in relation to "legacy data" will the previous regulations apply until 31.08.2010 in relation to market and opinion research, and until 31.08.2012 in relation to advertising.

It appears to be mandatory to implement the necessary mechanisms by the aforementioned dates. This applies, in particular, to the stricter requirements regarding prior consents and its necessity, but also to documentation duties regarding the origin of data, in order to comply with the statutory requirements when the revised regulations enter into force.

Anticipatory data management is essential. The implementation of the requirements should by no means be put off.

Florian Hensel, Munich

### Need for action

This newsletter can only provide a first overview of the main points of the revised regulations.

The controversial discussions in legislation have, in part, resulted in quite complex provisions, and their consequences must be examined on the basis of the specific arrangements in an individual case. The legislator did not provide for a long transitional period for many of the new regulations; large parts of the revisions will enter into force as early as on 01.09.2009.

Until then, business enterprises must not only review existing procedures and contracts for their further usability, but must also transform the necessary modifications into practice.

Should you have any questions, please do not hesitate to contact us.

Martin Schweinoch

### Practice Group IT, Internet and E-Business

Nikolaus Bertermann

Dr. Oliver Bühr

Thomas Eigen, LL.M.

Markus von Fuchs LL.M.

Florian Hensel

Johann Heyde

Dr. Oliver Hornung

Dr. Daniel Kaboth

Dr. Wulf Kamlah

Sabine Kröger

Dr. Eberhard Kromer MBA

Dr. Karolin Nelles

Dr. Matthias Nordmann, M.A.

Dr. Andreas Peschel-Mehner

Dr. Ulrich Reber

Stefan C. Schicker, LL.M.

Prof. Dr. Mathias Schwarz

Martin Schweinoch

Udo Steger

Martin Stück

Dr. Johannes Thoma

Julian Westpfahl

Dr. Anne Zoll

### Legal notice

#### SKW Schwarz

#### Rechtsanwälte Steuerberater Wirtschaftsprüfer Partnerschaft

The seat of the partnership is in Munich, registered with the Local Court of Munich under PR 884.

Authorised representative: Prof. Dr. Mathias Schwarz,  
Chief editor: Martin Schweinoch.

E-mail: [IT@skwschwarz.de](mailto:IT@skwschwarz.de)

#### Locations:

##### 10719 Berlin

Kurfürstendamm 38/39

Phone: +49 (0) 30.889 26 50-0

Fax: +49 (0) 30.889 26 50-10

##### 40212 Düsseldorf

Steinstraße 1/Kö

Phone: +49 (0) 221.82 89 59-0

Fax: +49 (0) 221.82 89 59-60

##### 20095 Hamburg

Spitalerstraße 4

T +49 (0) 40-33 40 10

F +49 (0) 40-33 40 15 21

##### 60598 Frankfurt/Main

Mörfelder Landstraße 117

Phone: +49 (0) 69.63 00 01-0

Fax: +49 (0) 69.63 55 22

##### 80333 Munich

Wittelsbacherplatz 1

Phone: +49 (0) 89.286 40-0

Fax: +49 (0) 89.280 94-32

If you no longer wish to receive the IT Ticker, please send us an e-mail or inform your contact at our firm. We will be happy to inform you of our other tickers and newsletters.

Occupational title: Rechtsanwalt/-anwältin der BRD.

Competent chamber of lawyers: Chambers of lawyers of Berlin, Düsseldorf, Frankfurt a.M., Hamburg and Munich.

The professional regulations may be retrieved at <http://www.brak.de> under the heading "Professional Regulations" - duties to inform pursuant to § 5 Telemedia Act.

© SKW Schwarz 2009