SKW
Schwarz
Rechtsanwälte

Practice Group IT & Digital Business
IT Ticker – Special Issue

The New German Federal Data Protection Act

An initial introduction to the new provisions introduced by the Data Protection Adaptation and Implementation Act EU

Table of Contents

Status June 7, 2017 – © SKW Schwarz

www.skwschwarz.de

Editor: Nikolaus Bertermann
Authors: Nikolaus Bertermann, Dr. Oliver Bühr, Dr. Oliver Hornung, Dr. Wulf Kamlah, Franziska Ladiges, Yvonne Schäfer, Martin Schweinoch, Benjamin Spies, Dr. Volker Wodianka, LL.M., Dr. Hans Markus Wulf
Head of the IT & Digital Business Department: Martin Schweinoch

1. Introduction and Scope of Application

This Special Ticker offers an overview of the **new German Federal Data Protection Act** for the implementation of European regulations with a clear focus on the non-public sector – in particular companies.

Effective May 25, 2018, the **EU General Data Protection Regulation (GDPR)** will govern data protection in the entire European Union in the non-public and public sector as directly applicable law. Some regulations of the GDPR can or must be further specified or shaped in more detail by means of statutes by the individual Member States. At the same time with the GDPR, the EU issued a **Directive** on **data protection** for the purposes of the **prevention** and **prosecution of criminal offenses** on April 27, 2016, whose content is also to be implemented by May 25, 2018 by the Member States.

The **Data Protection Adaptation and Implementation Act EU** is intended to fill the regulatory space left by the GDPR on the one hand and to transpose the EU Data Protection Directive into German law in cases of law enforcement and crime prevention on the other hand. The Data Protection Adaptation and Implementation Act EU contains an entirely new **Federal Data Protection Act ("Bundesdatenschutzgesetz", "BDSG-new")** and amendments to other laws (Federal Constitution Protection Act, Military Counterintelligence Service Act, Security Screening Act). The Data Protection Adaptation and Implementation Act EU was adopted by the Bundestag on April 27, 2017 and by the Federal Council on May 12, 2017. In addition, sector-specific data protection regulations in many German statutes are to be adapted to the GDPR, which will only take place in a further statute in the future ("Omnibus Act").

The **new Federal Data Protection Act** applies simultaneously with the GDPR from May 25, 2018 and governs data protection – just like the current Federal Data Protection Act ("Federal Data Protection Act-2003") – in the public sector and non-public sector (companies, etc.) in 85 Sections. The new Federal Data Protection Act consists of four parts: joint provisions, implementing provisions for the GDPR, transposition of the Directive for data protection for the purposes of prevention and prosecution of criminal offenses, and special provisions for processing, which is not subject to the European regulations. This **SKW Schwarz Special Ticker** is limited to the joint provisions and the implementing provisions of the GDPR of the BDSG-new.

The BDSG-new applies in the public sector, except if the processing of personal data is to be regulated by the federal states. Irrespective of the legal form, all federal and state bodies are considered part of the public sector, as well as private associations that perform public duties, excluding public sector companies competing with private sector companies.

All other bodies are in the non-public sector. The BDSG-new will apply there if the controller or external processor has its residence or a branch in Germany or if data processing outside of the EU (including the EEA and Switzerland) falls under the GDPR.

2. Video Surveillance of Publicly Accessible Areas

The regulations on video surveillance in publicly accessible areas have not changed considerably in comparison with the Federal Data Protection Act-2003. Some parts have simply been made more precise or necessary adjustments have been made to the GDPR.

For private persons and companies, the two alternatives for permissibility remain the "**protection of domiciliary rights**" and the "**realization of legitimate interests for specified purposes**." What is new is that it is expressly clarified that in case of large premises, the protection of life, health, and the freedom of persons who spend time there, are considered to be particularly important. Premises of this kind include sports, meeting, and entertainment venues, shopping malls, and parking lots. The same applies to vehicles and large public facilities of rail, ferry, and bus transportation.

With regard to the notification of video surveillance that was already necessary previously, and included the name and contact information of the controller, it has now been clarified in addition that this notification must be visible at the earliest possible opportunity, i.e**., it is best for the notification to be located before the entrance to the area covered by video surveillance.**

Video surveillance is to be included in the record of processing activities in accordance with Art. 30 GDPR. This record replaces the previous list of procedures. The new data protection impact assessment introduced by Art. 35 GDPR is necessary for the systematic comprehensive surveillance of publicly accessible areas. The consequences of the intended processing procedures with regard to the protection of personal data are thus to be assessed in advance.

Due to the slight adjustment in the provisions on video surveillance, it is possible to continue using significant portions of the **guide "Video Surveillance by Non-Public Bodies"** issued by the Düsseldorfer Kreis committee until a new edition is published. Companies should check the available data protection law documentation for their video surveillance equipment and adapt it to the new requirements of the GDPR and the BDSG-new.

3. Supervisory Authorities

Provisions on regulated **cooperation between supervisory authorities** are not only restricted to the very important question of determining the competent authority ("Lead Supervisory Authority") (Art. 60 GDPR) and the exchanging of useful information, but also deal with concrete mutual assistance (Art. 61 GDPR). Section 83 BDSG-new fulfills the mandate to act under Art. 61(1) GDPR with the provisions for mutual assistance, according to which "measures for effective cooperation with one another shall be put in place."

At the core of the Adaptation and Implementation Regulation is the **securing of the uniform implementation and application** of Directive (EU) 2016/680. Cooperation between the national supervisory authorities has already been governed by Art. 28(6) of Directive (EU) 1995/46, however, the drafting of content was left out ("Each authority may be re-

quested to exercise its powers by an authority of another Member State."). Now mutual assistance will be regulated in detail based primarily on five factors:

(1) Subject matters of mutual assistance are, in the view of the legislator, in particular requests for information and measures relating to supervision, such as requests for consultation or for the performance of follow-up inspections and investigations (Section 82(1) BDSG-new).

(2) Requests for mutual assistance are to be complied with immediately (without culpable delay) and at the latest within one month from their receipt (Section 82(2) BDSG-new). This period will begin upon receipt of all necessary information including the purpose of the justification (Section 82(7) BDSG-new). If earlier processing is possible without taking up the entire period of one month, this processing must be performed earlier. Nevertheless, the processing does not have to be completed by that time in that case.

(3) Grounds for refusing mutual assistance are listed in Section 82(3) BDSG-new and are only relevant in case of lack of competence or legal infringements. They must be explained to the requesting authority.

(4) Data transfer is to take place electronically and in a standardized format (Section 82(5) BDSG-new). In Art. 61(9) GDPR, the Commission was given competence for the arranging of the exchange of information electronically.

(5) Where authorities have not agreed on the charging of **cost** incurred, administrative assistance requests are to be performed free of charge (Section 82(6) BDSG-new).

In practice, it is predominantly EU lead supervisory authorities who will use the means of "mutual assistance." Supervisory authorities outside of Europe may ask for cooperation according to Art. 50 GDPR.

4. Remedies, liability and penalties

In Art. 77 to 81, the GDPR provides regulations on remedies, liability and penalties for data subjects (complaints to the supervisory authorities, complaints against the supervisory authority, as well as complaints against the controller or the external processor). Not only the data subjects but also not-for-profit organizations or associations, which are active in the field of the protection of data subjects' rights, such as consumer protection associations may lodge a complaint (Art. 80 GDPR).

Section 20 BDSG-new regulates the **complaints procedure against decisions by the supervisory authorities** without a prior appeal procedure before the administrative courts. If the complaint focuses only on a decision on a fine made by the supervisory authority, the local court is competent (Section 68 Administrative Offenses Act ("Ordnungswidrigkeitengesetz", "OWiG")), in case of fines in excess of EUR 100,000.00, the district court (Section 41(1) sentence 3 BDSG-new).

In Section 21 BDSG-new, German supervisory authorities are for the first time granted **the right of complaint against decisions by the EU Commission with relevance to**

data protection law. In accordance with this standard, German supervisory authorities may have decisions on appropriateness, as well as decisions on standard protective clauses or approved codes of conduct, examined in court. The German authorities have been requesting a right of this kind for a long time. The CJEU derived the basis for it from its decision on the validity of the decision on appropriateness with regard to the Safe Harbor Agreement (October 06, 2015, C-362/14) from Art. 28(3) Data Protection Directive and from the European Charter of Fundamental Rights. The Federal Administrative Court is responsible for complaints by the supervisory authorities. If the Federal Administrative Court considers the EU Commission decision also to be illegal, the case must be remanded to the CJEU for its own decision.

5. Processing of Special Categories of Personal Data

The processing of special categories of personal data is governed by Sections 22, 24(2) BDSG-new. These norms are associated with the term of special categories of personal data under union law.

In Section 22(1) BDSG-new, beyond the GDPR, further admissibility elements for processing of special categories of personal data are listed. For example, such data processing is explicitly permitted insofar as it is necessary to exercise the rights arising out of the **right to social security** and **social protection** and to comply with obligations in this respect. In general, in accordance with Section 22(2) BDSG-new, appropriate and specific measures have to be provided for (in particular taking into account the state of the art) to protect the interests of the data subjects.

The processing of special categories of personal data for other purposes than that for which it was originally collected is permissible in accordance with Section 24(2) BDSG-new, if data processing is necessary to avoid risks to State or public security or for the prosecution of criminal offenses or for the asserting, exercising, or defense of claims under civil rights law, insofar as the interests of the data subjects in the exclusion of the processing do not outweigh this. In addition, exceptional circumstances under Art. 9(2) GDPR or Section 22 BDSG-new must be given.

6. Processing in the context of employment

Art. 88(1) GDPR allocates the Member States of the EU responsibility for issuing regulations on data protection in the context of employment and provides in Art. 88(2) GDPR that the national provisions must include, among other things, suitable and specific measures to safeguard employees' human dignity, legitimate interests, and fundamental rights. The German federal government regulated employee data protection in Section 26 BDSG-new. In this process, it **noticeably focused on the previous regulations of Section 32 Federal Data Protection Act-2003** and in addition, adopted regulations that, based on the understanding of the federal government, were intended to reflect the predominant opinion in literature and case law. There was no comprehensive new regulation of employee data protection, as discussed in the past – probably also to take into account with the lack of time and the upcoming Bundestag elections.

The scope of application of Section 26 BDSG-new is widely formulated and in addition to traditional **employees** expressly also includes **temporary employees**, **home workers**, **trainees**, as well as civil servants, judges, and soldiers. The scope of application expressly includes applicants. As previously, the requirements also apply to non-automated forms of processing, such as **human resources files kept in paper form**. Participation rights of work councils are not limited by Section 26 BDSG-new.

As was already the case in accordance with Section 32 Federal Data Protection Act-2003, processing of personal data is permitted in an employee context as long as the processing is "necessary" for the formation, **performance, or termination of the employment relationship**. The official justification of the law states that "necessity" is not to be understood to mean an imperative need, but rather results from a balancing of interests between the employer and the fundamental rights of the employees. This corresponds to the current understanding of Section 32 Federal Data Protection Act-2003. The current regulation for the processing of personal data to uncover offenses was retained. In addition, further documented concrete indications of an offense are needed and the measures for the uncovering of the offense may not be disproportionate. In addition, it is expressly regulated that the permissibility of the processing may also be based on collective agreements and tariff agreements.

The explicit provision on **consent in the employment relationship** is new. In particular, the supervisory authorities have viewed consents in the employment relationship critically. The employer must ensure that the consent is submitted **voluntarily** despite the dependent relationship. In accordance with Section 26(2) BDSG-new, this can be the case in particular if the employee gains an advantage from the consent or the interests of the parties are similar. The official justification of the law states as examples of advantages the private use of IT systems and operational health management for the promotion of health. As an example of similar interests, birthday lists and photos on the intranet are listed. Consent must generally be obtained in writing, although as a result of the circumstances, other forms are also possible. In any case, the purposes of the processing must be clearly stated and the employees must be informed clearly of the processing and must be informed of their right of withdrawal.

Processing of special categories of personal data, such as health information, information on race or ethnic origin, or union membership may be performed if this is necessary for the exercising of rights or the fulfillment of legal obligations under employment law or social security and social protection law and there is no reason to presume that interests of the data subject in the exclusion of the possibility of the processing, which are worthy of protection, take priority.

Prior to May 25/2018, the employer should check in particular **declarations of consent** by employees and existing **agreements with work councils** for conformity with Section 26 BDSG-new and Art. 88(2) GDPR.

7. Science, Research, Archiving

Science and research play an increasingly important role. In this connection, (archived) information assets and statistics are of major significance, which may be of significant benefit to science, e.g., in medicine. Information assets and statistics, however, are based on multiple personal data, for which data protection applies. In order not to impede science and research to too great an extent through data protection requirements, GDPR has provided rules on exceptions in Art. 89 and recitals 156 to 163. German legislators regulate corresponding exceptions in Sections 27, 28 BDSG-new for data processing for:

- scientific or historical research purposes (Section 27 BDSG-new)
- statistical purposes (Section 27 BDSG-new)
- archiving purposes in the public interest (Section 28 BDSG-new)

Sections 27, 28 BDSG-new provide that special categories of personal data as defined in Art. 9(1) GDPR (e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data, health data) can be processed as an exception, if

- this is necessary for the relevant purposes in accordance with Sections 27, 28 BDSG-new and
- if the data is intended for appropriate protective measures (Section 22(2) sentence 2 BDSG-new), such as technical and organizational measures, pseudonymization, encryption.

For research and statistical purposes, before processing of special categories of personal data, the **interests in it not being processed must be considered**. The interests of the researchers must outweigh those of the data subject (Section 27(1) BDSG-new). Otherwise, the processing is not permitted.

If it is permitted for research or statistical purposes, special categories of personal data must **strictly be made anonymous** (Section 27(3) BDSG-new). Until then, pseudonymization is necessary in order to protect the data subject. The characteristics that make the person identifiable are to be stored separately. They may only be combined with individual information if necessary for research or statistical purposes.

Sections 27, 28 BDSG-new results in the **restriction of the rights of the data subject** to information (Art. 15 GDPR), rectification (Art. 16 GDPR), restriction of processing (Art. 18 GDPR), and the right to object (Art. 21 GDPR). Section 28 BDSG-new also limits the right to data portability (Art. 20 GDPR). The rights of the data subject may be limited if that is the only way of achieving the purposes in question, i.e., if:

- the exercising of the rights of the data subject would make impossible or seriously impair the realization of the purposes in question, and
- the limitation is necessary for the fulfillment of the purposes.

The right to information of the data subject has also been removed under Sections 27, 28 BDSG-new if the provision of information would require a disproportionate expense. In order to avoid a disproportionate expense in case of scientific research, the limitation of the right to information must be necessary for achieving the purpose.

Section 28(3) BDSG-new contains an exception to the right to rectification (Art.16 GDPR) in case of archiving: in order not to put the data subject in an unprotected position, the data subject has an opportunity to reply. In this area, data subjects may state that the data is incorrect from their point of view. The responsible archive will be obligated to add the reply to the documents.

In accordance with Section 27(4) BDSG-new, personal data may only be published for research and statistics purposes if the data subject has consented or this is essential for the presentation of research results on events in current history.

8. Restriction of the Rights of Data Subjects

Section 29 BDSG-new restricts obligations to provide information on the part of the controller in the case of **confidentiality obligations**, in particular if information were published as a result of meeting the obligation for which confidentiality is required. Bearers of professional secrecy, such as lawyers, auditors, and physicians are also not obligated to provide information to data subjects, unless the data subject's interest in the granting of information takes precedence.

Section 32 BDSG-new limits the obligation to provide information among other things in case of a change in purpose for further processing if the **data is stored in an analog manner**, the further processing is compatible with the original purpose and communication with the data subject does not take place digitally. Section 33 BDSG-new restricts the obligation of non-public bodies to provide information if the information were to have a negative effect on the **asserting, exercising, or defending of claims under civil rights law** or were to pose a risk to public safety and order. If the information is not provided, the controller must take measures to protect the legitimate interests of the data subject. In these cases, in accordance with Section 34 BDSG-new, the **right of the data subject to information is restricted.** However, the reasons for the refusal to provide information must be documented.

The provision under Section 35 BDSG-new, which applies equally to both public and non-public bodies, includes **exceptions to the right to deletion**, in cases where this is – in case of a non-automated data processing – not possible or is only possible at a disproportionate expense. In these cases, data processing is to be restricted (previously "blocking"). This does not apply if data have been processed unlawfully. The **right to object** is restricted in Section 36 BDSG-new if and insofar as there is an overriding, mandatory public interest in the processing, which outweighs the rights of the data subject or in case of an obligation to perform the processing under a statutory provision. Section 37 BDSG-new takes into account the **specific concerns of the insurance industry.** The right not to be subject to decision based exclusively on automated processing (including profiling), which has a legal effect on the data subject does not exist if the decision is issued as part of the performance of services under an insurance contract. A prerequisite, however, is that the data subject's demand was fulfilled or the decision is based on applicability of binding fee regulations for treatments by healing professionals. In case of a non-fulfillment of the demand the data subject, further measures must be taken in order to protect the legitimate interests of the data subject.

9. Consumer Loans and Scoring

In accordance with the official justification of the BDSG-new, investigations into creditworthiness and issuing of **credit reports** is a foundation of the German credit industry and therefore also of the functioning of the economy. The new provisions of Section 31 BDSG-new on credit agencies and scoring are intended to protect commercial trade and are of paramount importance to data subjects and to the economy. Protecting the data subjects from overindebtedness is both in the interest of the data subjects themselves and in the interest of the economy.

The provision under Section 31 BDSG-new continues and puts into concrete terms the regulations that applied previously with regard to what requirements a score determined by a credit agency must fulfill with regard to "**negative features**" in order to be able to be used in commercial trade. The criteria under Section 31(2) sentence 1 BDSG-new restrict the permissibility of determining scores in certain cases and in this way create an appropriate balance between the conflicting interests for example because **open receivables** can only be reported to credit agencies and be processed there if they are **undisputed or titled**. Section 31(2) sentence 2 BDSG-new leaves the provisions of the general data protection law on permissibility of processing of personal data unchanged. This relates among other things to transmission and use for determination of probability values of personal data on the justification, proper performance, and ending of a contractual relationship of a transaction with financial default risk (positive data). In this respect, security is provided for all participants in such a way that scoring procedures and credit information systems with the registration of positive and negative data, for example from credit institutions, financial services companies, payment institutions, telecommunications, trade, energy supply, and insurance or leasing companies, continue to remain permissible in principle. They will still be considered important prerequisites for economic life. In this respect, Section 31 BDSG-new puts the balancing of interests in accordance with Art. 6(1)(f) GDPR, according to which the transmission of such data and its use by credit agencies for the formation of scores is permissible.

10. Data Protection Officers and Accreditation of Certification Bodies

The GDPR imposes an obligation on non-public bodies to **appoint a data protection officer**, if extensive regular and systematic monitoring of the data subjects by the controllers or external processors is a core activity or if extensive processing of certain categories of data in accordance with Article 9 or of personal data on criminal convictions and offenses in accordance with Article 10. In Section 38 BDSG-new, German legislators use the opening clause of Art. 37(4) GDPR. Accordingly, it is mandatory of a data protection officer to be appointed, as was already the case in Federal Data Protection Act-2003 – if the company in general permanently employs **at least ten people** in the automated processing of personal data. The same obligation applies to controllers and external processors in the case of processing that is subject to a data protection impact assessment in accordance with Art. 35 GDPR or personal data that is being processed in a business for the purposes for the purposes of transmission, anonymized transmission, or for the pur-

poses of market research or opinion polling. The determining factor is not a certain number of persons.

With regard to the **position of the data protection officer** in non-public bodies, Section 38(2) BDSG-new refers in some cases to the provisions on data protection officers in public bodies, in particular to the special requirements for dismissal and termination, particular secrecy and the data protection officers' right to refuse to give evidence. The essentials of these characteristics of the role of the data protection officer are already known from Sections 4g, f Federal Data Protection Act-2003.

Certification bodies in accordance with Art. 43 GDPR promote data protection and offer controllers and external processors tangible added value for the fulfillment of the accountability for compliance with the GDPR. They are authorized in Germany in accordance with Section 39 BDSG-new by the federal or state supervisory body responsible for data protection via the certification body on the basis of an accreditation by the German accreditation bodyhttp://www.dakks.de/.

11. Sanctions

The GDPR contains provisions in Art. 83 and 84 on penalties in case of data protection infringements. Firstly, **there are sanctions for practically all infringements of data protection guidelines** and secondly **the level of possible monetary fines has been drastically increased**. In parallel to the directly applicable European data protection standards, the national rules of the individual Member States also apply, unless the GDPR applies from a factual perspective, contains flexibility clauses, or orders this expressly. According to Art. 84 GDPR, the Member States specify the provisions on other sanctions for breaches against the Directive and take all measures necessary for their application (cf. also Recital 152 GDPR).

Provisions of this kind are now included in Sections 41-43 BDSG-new. These standards are linked to the fines in the GDPR and impose further sanctions depending on the severity of infringement. Section 41 BDSG-new regulates the application of the **provisions on fines and criminal proceedings** in case of infringements of the GDPR; Section 42 and Section 43 BDSG-new include provisions for fines.

In accordance with Section 41 BDSG-new, the provisions of the Administrative Offenses Act – with the exception of Sections 17, 35, and 36 – for infringements or for procedures in case of infringements in accordance with Art. 83(4) to (8) GDPR are applicable in a corresponding manner. Since Section 17 Administrative Offenses Act does not apply, the fines serve the sole purpose of punishment. The confiscating of illegally obtained profits should not take place. While the level of the fines is based on the provisions of the GDPR, the procedure for the imposing of these fines will be based on the Administrative Offenses Act.

According to Recital 152 GDPR, the Member States are obligated to implement effective, proportionate, and dissuasive penalties under criminal or administrative law in case of breaches of data protection infringements. **Sanctions under criminal law** are contained

in Section 42 BDSG-new. The two criminal offenses are – unlike the provisions on fines in the GDPR – designed as provisions that apply to anyone. Infringements during processing of data that is not generally accessible may therefore result in a custodial sentence of up to three years. Notification in accordance with Art 33 GDPR and communication in accordance with Art. 34 GDPR may, however, be used in criminal proceedings against reporting persons or their family members only with their consent.

The provisions on fines under Section 43(1) and (2) BDSG-new only apply in case of breaches of the obligations under Section 30 BDSG-new in connection with consumer loans. In case of breaches of this kind, the monetary fine is limited to a maximum of EUR 50,000. Section 43(3) BDSG-new makes clear that no monetary fines are imposed against authorities and other public bodies.

In the future, German legislators want to see fines in data protection law as are currently known in antitrust law. This increase in the framework of fines means that **significantly higher individual fines** than previously are to be expected. Individual German data protection authorities have already announced this.

SKW Schwarz Rechtsanwälte Wirtschaftsprüfer Steuerberater mbB
Registered at Munich Local Court PR 884, Partnership headquarters is Munich.
General managers authorized to represent the partnership: Markus von Fuchs LL.M., Stefan Schicker, LL.M.

10719 Berlin	**40212 Düsseldorf**	**60598 Frankfurt/Main**	**20095 Hamburg**	**80333 Munich**
Kurfürstendamm 21	Steinstr. 1	Mörfelder Landstr. 117	Ferdinandstr. 3	Wittelsbacherplatz 1
T +49 30 889 26 50 0	T +49 211 82 89 59 0	T +49 69 63 00 01 0	T +49 40 334 01 0	T +49 89 286 40 0
F +49 30 889 26 50 10	F +49 211 82 89 59 60	F +49 69 63 55 22	F +49 40 334 01 530	F +49 89 280 94 32