Baker McKenzie.

Hot Topics

IT & Communications
Germany

June 2017

Insight into the New German Federal Data Protection Act Supplementing the GDPR

The German Parliament approved the new Federal Data Protection Act ("FDPA-new") on April 27, 2017 (Bundestag printing matter 18/11325 and 18/12084) in order to align the pre-existing German data protection law with the requirements of the European General Data Protection Regulation ("GDPR") and to make use of the GDPR's opener clauses. The German Federal Council approved the FDPA-new on May 12, 2017 (Bundesrat printing matter 332/17). The FPDA-new will come into effect on May 25, 2018, the same date as the GDPR.

Below we have summarized the main content of the FDPA-new relevant for private bodies.

1. Scope of Application

The future of privacy law in Germany will largely be the GDPR. Only to the extent the GDPR does not apply there is room for the FDPA-new to apply. According to the FDPA-new this is the case in the following circumstances: (1) where a controller or processor processes personal data in Germany; (2) where personal data is processed in the context of a German-based establishment of a controller or processor; or (3) where a controller or processor does not have an establishment in the EU/EEA, but is otherwise subject to the GDPR, in all cases to the extent the GDPR does not apply directly.

2. Special Categories of Personal Data

Art. 9 (2) (b), (g), (h), and (i) of the GDPR require national law makers to supplement the grounds that justify the processing of sensitive data. National law makers shall in particular provide for appropriate safeguards for the fundamental rights and the interests of the data subject. In light of this, Sec. 22 of the FDPA-new permits the processing of sensitive data in the following circumstances: (1) if the processing is necessary to exercise rights and comply with obligations in the area of social security or social protection laws; (2) for purposes of preventative health care, assessment of the working capacity of employees, medical diagnosis, provision of health or social care or treatment, management of health or social care systems and services as well as on the basis of a treatment contract; and (3) for reasons of public interests in the area of public health, such as protection against severe cross-border health risks. Processing of sensitive data based on such justification grounds requires appropriate and specific, state-of-the-art measures to protect the interests of the data subject. In particular, such measures may,

Our Expertise
IT & Communications

according to the FDPA-new, include: (1) technical and organizational security measures; (2) input controls; (3) training of individuals involved in the processing; (4) appointment of a DPO; (5) access restrictions within the controller or processor; (6) pseudonymization; (7) encryption; (8) ensuring the confidentiality, integrity, availability, and resilience of processing systems and services, including the ability to restore the availability and access in a timely manner in the event of a physical or technical incident; (9) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing; and/or (10) specific processes that ensure compliance with the FDPA-new and the GDPR in case of data transfer or processing for another purpose. Such security measures partly resemble the measures set forth in Art. 32 of the GDPR.

3. Purpose Limitation

Art. 6 (4) of the GDPR allows Member States to establish a legal ground for the processing of personal data for another purpose (purpose limitation). The FDPA-new determines in Sec. 24 that private bodies are permitted to process personal data for a purpose different than the purpose for which the personal data were originally collected if this is necessary to (1) defend against risks related to governmental or public safety or for criminal prosecution, or (2) exercise, establish, or defend against civil claims, unless the interests of the data subject prevail. Such justification grounds can also be applied to sensitive personal data provided that - as additional justification - a justification ground of Art. 9 (2) of the GDPR or Sec. 22 of the FDPA-new applies as well.

4. Employee Data

Pursuant to Art. 88 of the GDPR, Member States may provide for more specific rules for the processing of employee data in the employment context. Sec. 26 of the FDPA-new addresses the processing of employee data and basically retains the existing rules under Sec. 32 of the currently existing German Federal Data Protection Act. However, to the extent the processing is based on collective agreements, the FDPA-new states that the parties to the respective agreement must take into account Art. 88 (2) of the GDPR, according to which the rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

For example, employee data can be processed for the purposes of establishing, carrying out, or terminating an employment relationship, or for purposes of exercising rights and complying with obligations stemming from a law, union agreement, or works council agreement. Furthermore, for purposes of detecting a crime, employee data may only be processed if: (1) there is a documented reason to believe the data subject has committed a crime while employed; (2) the processing of such employee data is necessary to investigate the crime; and (3) the data subject does not have an overriding legitimate interest against the processing.

According to the FDPA-new, employee consent can be valid, provided that the employee gives consent voluntarily. The voluntary nature of the consent is determined by considering the dependency within the employment relationship and the circumstances of the consent, in particular whether the employee gained a legal or financial benefit through the consent or if the employee and employer pursue similar interests. Consent must be in writing, unless another form is justified due to the circumstances.

Furthermore, Sec. 26 of the FDPA-new permits the processing of sensitive employee data if the processing is necessary to exercise rights and/or comply with obligations under employment law, social security law, or social protection law, and there is no reason to believe that the interests of the employee prevail. The FDPA-new does not provide for a specific legal ground to transfer sensitive employee data as part of a matrix structure within a group of companies. It remains to be seen how strictly the narrow scope of Sec. 26 of the FDPA-new for the processing of sensitive employee data will be interpreted and applied.

5. Processing of Sensitive Data for Research Purposes

Art. 9 (2) (j) of the GDPR allows Member States to permit the processing of sensitive data for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes. Sec. 27 of the FDPA-new creates a legal basis for the processing of sensitive data for scientific or historical research purposes or for statistical purposes if the processing is necessary and if the interests of the controller prevail over the interests of the data subject.

Furthermore, in light of Art. 89 (1) of the GDPR, the controller must take appropriate and specific measures pursuant to Sec. 22 of the FDPA-new and must anonymize the sensitive data as soon as possible in light of the research or statistical purpose.

6. Additional Justification Grounds for Personal Data

The FDPA-new provides for special justification grounds for scoring and credit reporting, similar to, but more detailed than, the rules in the currently existing German Federal Data Protection Act. Furthermore, the FDPA-new provides for specific rules in order to implement CCTV systems in public areas.

7. Data Subject Rights

Based on the opener clause in Art. 23 of the GDPR, the FDPA-new restricts data subject rights in Secs. 32 to 35.

(a) Restriction of Art. 13 (3) of the GDPR

According to Art. 13 (3) of the GDPR, the controller must inform the data subject if the controller intends to further process personal data for a purpose other than that for which the personal data were collected. Sec. 32 of the FDPA-new allows for exceptions to this information obligation if the provision of such information: (1) concerns a new processing which is directed at the data subject, subject to further requirements, and if the interests of the data subject are rather low; (2) jeopardized the exercise,

establishment, or defense of legal claims provided that the interests of the data subject do not prevail; or (3) jeopardized a confidential transfer of data to a governmental body. Where the controller is not required to inform the data subject pursuant to Art. 13 (3) of the GDPR and Sec. 32 of the FDPA-new, the controller must provide information in this regard to the public and must generally document the reasons why it takes the view that the exception pursuant to Sec. 32 of the FDPA-new applies.

(b) Restriction of Art. 14 (1), (2) and (4) of the GDPR

According to Sec. 33 of the FDPA-new, the information obligations pursuant to Art. 14 (1), (2) and (4) of the GDPR do not apply if the provision of such information: (1) impaired the exercise, establishment or defense of legal rights, concerns the processing of data from commercial contracts, and serves the purpose of preventing damages from criminal offenses, unless the interests of the data subject prevail; or (2) may jeopardize public safety, in particular relating to public prosecution activities. Where the controller is not required to inform the data subject pursuant to Art. 14 (1), (2) and (4) of the GDPR and Sec. 33 of the FDPA-new, the controller must provide information in this regard to the public and must generally document the reasons why it takes the view that the exception pursuant to Sec. 33 of the FDPA-new applies.

(c) Data Access Right

According to Sec. 34 of the FDPA-new, the access right of Art. 15 of the GDPR is restricted if: (1) the controller is not required to inform the data subject pursuant to Sec. 33 of the FDPA-new; or (2) if the personal data (i) is only stored for compliance with statutory or contractual retention obligations or (ii) only serve the purposes of data security and data protection control, and in case of (i) or (ii) if the provision of access required an unreasonable effort, and the processing for any other purposes is prevented through appropriate technical and organizational measures. The data controller must document the reasons for not providing access and must inform the data subject about the reasons.

(d) Right to Erasure

According to Sec. 35 of the FDPA-new, the right to request erasure and the obligation to erase do not apply if erasure requires an unreasonably high effort due to the specific type of storage. In this case, the data shall be restricted from further processing. This exception, however, does not apply in case of an unlawful processing. The data controller has to inform the data subject about the restriction of the processing if possible and reasonable. Under certain circumstances, the obligation to erase personal data can be substituted by restricting the further processing of such data if the controller has reason to believe that the erasure would affect legitimate interests of the data subject.

8. Data Protection Officer

The FDPA-new takes advantage of the opener clause in Art. 37 (4) sentence 1 of the GDPR with regard to the circumstances that require the appointment of a data protection officer. As in the existing German Federal Data Protection Act, Sec. 38 of the FDPA-new requires the appointment of a data protection officer if a controller or processor employs on a regular basis at least 10 individuals which are permanently processing personal data. Regardless of the number of individuals that are permanently processing personal data, the controller or processor is also required to designate a data protection officer if the type of processing is likely to result in a high risk to the rights and freedoms of natural persons and therefore requires a data protection impact assessment pursuant to Art. 35 of the GDPR, or in other cases depending on the business operations of the controller, such as marketing or market opinion research or transferring data to third parties.

9. Federal Commissioner for Data Protection and Freedom of Information as Representative at the EDPC/Cooperation with the Supervisory Authorities

According to Art. 51 (3) and Art. 68 (4) of the GDPR, Germany is required to designate a representative for the European Data Protection Committee ("EDPC") as Germany has more than one supervisory authority. The FDPA-new determines that the Federal Commissioner for Data Protection and Freedom of Information in Germany ("Commissioner"), which is responsible within Germany for data protection supervision of federal public bodies, telecommunication providers and certain other private bodies, shall act as the representative of the 17 German supervisory authorities at the EDPC. The Commissioner also serves as the contact point for the European-wide consistency mechanism pursuant to Art. 63 of the GDPR et seq.

10. One-Stop Shop within Germany

The supervisory authority of the German state in which the private body is located is responsible for monitoring the company's compliance with applicable data protection law. If the private body is located in more than one state in Germany (for example, a bank with branches or a retail company with retail stores), the supervisory authority of the German state in which the main establishment (meaning the establishment in which the central administration of the private body takes place) is located shall act as the lead authority. For the performance of its tasks, the responsible supervisory authority is authorized to enter properties and offices of the private body and to obtain access to the private body's data processing systems.

11. Amnesty in Case of Security Breach Notifications

In case of a notification of a personal data breach to the supervisory authority pursuant to Art. 33 of the GDPR or a communication of a personal data breach to the data subject pursuant to Art. 34 of the GDPR, Secs. 42 (4) and 43 (4) of the DPA-new clarify in accordance with the opener clause in Art. 83 (7) of the GDPR that such notification or communication can only be used in criminal or administrative proceedings against the person that was subject to the notification requirement (i.e., the data controller), the reporter or his/her relatives if the person subject to the notification requirement or the reporter consented to it.

12. Sanctions

In addition to the fines provided in the GDPR, Sec. 42 of the FDPA-new provides for criminal penalties with up to three years imprisonment or criminal fines in case of certain intentional unlawful data processing activities. The FDPA-new also provides for administrative fines in addition to those in Art 83 of the GDPR, however, with up to EUR 50,000 the respective fines are rather low.

For further information, please contact:

Julia Kaufmann, LL.M.
julia.kaufmann@bakermckenzie.com

Dr. Holger Lutz, LL.M.
holger.lutz@bakermckenzie.com

Contributor:

Sara Ghoroghy
sara.ghoroghy@bakermckenzie.com