Germany's Federal Data Protection Act

The European General Data Protection Regulation (GDPR) provides exceptions within its articles which oblige Member States to pass GDPR implementation laws. The GDD has gathered important information regarding Germany's implementation law („Federal Data Protection Act" FDPA[1]). These guidelines will focus on special requirements for private bodies and will not touch topics such as the powers and structure of the Federal Data Protection Commissioner or the accreditation of certification bodies.

Lawfulness of processing

Video surveillance

When monitoring **publicly accessible** areas, Sect. 4.1 FDPA allows such monitoring only when it is necessary

- for public bodies to perform their tasks,
- to exercise the right to determine who shall be allowed or denied access or
- to safeguard legitimate interests for specifically defined purposes.

Besides the abovementioned conditions, there may be nothing to indicate **legitimate overriding interests** of the data subjects. Any monitoring of public places therefore requires a **blance of interests**.

Protecting the **lives, health and freedom** of persons shall be regarded as a very important interest when monitoring **large publicly accessible** facilities or vehicles of public transportation which still needs to be balanced with the interests of the data subjects.

When monitoring publicly accessible areas, special requirements regarding the **information of the data subject** apply. According to Sect. 4.2 FDPA appropriate measures shall be taken to make the **surveillance** and **the controller's name and contact details** identifiable as early as possible. Germany's FDPA stipultes **reduced information obligations** when data subject are merely monitored on publicly accessible areas.

Storage and usage of video monitoring data is permitted if necessary to achieve the intended purpose and if there is nothing to indicate legitimate overriding interests of the data subjects (Sect. 4.3 sentence 1 FDPA).

A **further processing** of video footage by changing the original purpose of processing shall only be allowed if necessary to **prevent threats to state and public security and to prosecute crimes** (Sect. 4.3 sentence 3 FDPA).

If data collected from video surveillance **are attributed to a particular person**, that person shall be informed of the processing in accordance with Art. 13 and 14 GDPR (Sect. 4.4 FDPA).

Personal data from video footage has to be **deleted** without delay, if they are **no longer needed** for the intended purpose or if the **data subject's legitimate interests** overrides any further storage (Sect. 4.5 FDPA).

Processing of special categories of personal data

Under Art. 9.1 GDPR, the processing of special categories of personal data is prohibited. However, Art. 9.2 GDPR provides excepions of this prohibition.

In the cases referred to in Art. 9(2)(b), (g), (h) and (i) GDPR the exceptions are to be shaped by national regulations.

Sect. 22.1 FDSPA specifies the conditions under which the processing of special categories of personal data may be carried out. Processing special categories of personal data shall be admissible for public

[1] https://www.gesetze-im-internet.de/englisch_bdsg/index.html.

or private bodies according to the FDPA, inter alia, if necessary

- in the context of **social security** and **social protection** and to meet the related obligations
- for the purposes of **preventive medicine**, for the **assessment of the working capacity** of the employee, **medical diagnosis**, the provision of **health** or **social care** or **treatment** or the **management of health** or **social care systems and services** or pursuant to the data subject's **contract with a health professional** and if these data are processed by health professionals or other persons subject to the obligation of professional secrecy or under their supervision
- for reasons of **public interest** in the area of **public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

With regard to public bodies Sect. 22.1 FDPA sets out additional conditions under which processing special categories of personal data shall be lawful, such as the processing being **urgently** necessary for reasons of **substantial public interest**.

Sect. 22.2 FDPA stipulates the requirement of Art. 9(2)(b), (g) and (i) GDPR **regarding appropriate safeguards** for the fundamental rights and interests of the data subject. The list of non-exhaustive **technical-organisational measures** (e.g. training of employees, appointing a DPO, pseudonymisation, encryption) is a suggestion of the legislator and has to be assessed on a case-by-case basis following a risk-based approach.

Processing for other purposes by private bodies

When personal data is processed by a private body for a purpose other than the one for which the data were collected, such ‚further processing' shall be admissible under the conditions laid down in Sect. 24.1 FDPA. A further processing according to Sect. 24.1 is considered compatible, if

- it is necessary to **prevent threats to state or public security or to prosecute criminal offences**; or
- it is necessary for the **establishment, exercise or defence of civil law claims**,

unless the data subject has an overriding interest in not having the data processed.

Sect. 24.2 FDPA clarifies that the further processing of **special categories** of personal data is only allowed if, besides one of the conditions of paragraph 1, an exception in accordance with Art. 9.2 GDPR or Sect. 22 FDPA is met.

Data processing for employment-related purposes

The opening clause of Art. 88 GDPR allows national rules on data processing in the **employment context**. The German legislator made use of this option in Sect. 26 FDPA.

Sect. 26.1 sentence 1 FDPA allows the processing of personal data when such processing is **necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract** or to exercise or satisfy rights and obligations of the **employees' representation** laid down by law or by collective agreements or other agreements between the employer and the works council. The works council is targeted by Sect. 26.1 FDPA regarding the processing of personal data of employees whereas the necessiy of processing heavily relies on the taks and duties stipulated in the Works Constitution Act.[2]

Sentence 2 of Sect. 26.1 FDPA specifies the conditions for the processing of personal data of employees for the **purpose of disclosure of crimes committed in employment**. It does **not** cover measures to **prevent** crimes or breaches of obligations within the employment relationship. Processing personal data for the latter purposes would have to assessed according to Sect. 26.1 sentence 1 FDPA or according to Art. 6.1 lit. f GDPR.

Sect. 26.2 regulates the conditions under which personal data of employees may be processed with the **employee's consent**. Sentence 2 stipulates that freely given consent may, in particular, exist if the employees obtain **a legal or economic advantage** as a result of the data processing, or if the employer and employees **pursue the same interests**.

[2] https://www.gesetze-im-internet.de/englisch_betrvg/index.html.

Sentence 3 requires consent to be given in **written form**, unless a different form is appropriate because of special circumstances. Germany's FDPA is less versatile then the GDPR when a consent is obtained from an employee.

When **special categories of personal data** are processed in an employment context, Sect. 26.3 FDPA allows such processing for employment-related purposes if such processing is necessary **to exercise rights or comply with legal obligations** derived from **labour law**, **social security** and **social protection law**, and there is no reason to believe that the data subject has an overriding legitimate interest that his/her data shall not be processed.

Sect. 26.4 FDPA stipulates that the processing of personal data relating to employees on the basis of **collective agreements** is allowed, however, Art. 88.2 GDPR has to be taken into account. Germany's FDPA provides the possibiltiy to establish an **autonomous legal basis** outside of the GDPR by concluding a collective agreement with the works council for example. The conclusion of a collective agreements may be mandatory when a processing is subject to the rules of co-determination according to the Works Constitution Act.[3]

According to Sect. 26.5 the controller must take appropriate measures to ensure compliance in particular with the **principles** for processing personal data described in Art. 5 GDPR.

The works or staff council as primarily referred to as the representation of employees' interests has very far-reaching participation rights in the field of employee data protection. Sect. 26.6 FDPA clarifies that the rights of participation of works or staff councils shall remain unaffected by the FDPA.

The FDPA's provisions concerning the processing of personal data of employees shall also apply to such data, including special categories of data, which are being processed **without forming or being intended to form part of a filing system** (Sect. 26.7 FDPA). Handwritten remarks about an employee are therefore also bound to the requirements of Sect. 26 FDPA.

Sect. 26.8 FDPA holds definitions for employees covered by the special regulations of Sect. 26 which shall include, inter alia, applicants or retired personnel.

Protection of commercial transactions in the case of scoring and credit reports

Sect. 31.1 FDPA restricts the processing of personal data in the context of a decision on the creation, execution or termination of a contractual relationship with the data subject using a **probability value for certain future actions by this person** (score). Inter alia, the data used to calculate the probability value must be **demonstrably essential** (for the prediction) and the **algorithm** must be created on the basis of a **scientifically recognized mathematical-statistical procedure**.

The **use** of a probability value calculated by credit reporting agencies to determine a natural person's ability and willingness to pay shall be permitted as far as the conditions of Sect. 31.1 are met and only claims according to Sect. 31.2 no. 1-5 for services owed which have not been rendered on time are considered.

Rights of the data subject

Restrictions

a) Information of the data subject (Art. 13 GDPR)

When transferring personal data to a **lawyer bound to professional secrecy obligations**, the transferring body shall **not** be obligated to inform the data subject according to Art. 13.3 GDPR, unless the data subject has an overriding interest in being informed (Sect. 29.2 FDPA).

In addition to Art. 13.4 GDPR, Sect. 32.1 FDPA provides exceptions to the information obligation according to Art. 13.3 GDPR, inter alia, if

- the further processing concerns data stored in **analogue form** in which the controller **directly contacts** the data subject in a non-digital way, the purpose is **compatible** with the original purpose and the interest of the data subject in receiving the information can be regarded as **minimal** or
- the information would **endanger public security** or would interfere with the establishment, exercise or defence of **legal claims** and the controller's interests in not providing the information outweigh the interests of the data subject.

Sect. 32.2 FDPA obliges controllers to **implement appropriate measures** to protect the legitimate inte-

[3] E.g. the cases referred to in Art. 87 WCA.

rests of the data subject when he/she is not informed according to Art. 13.3 GDPR. Appropriate measures include the **provision of this information to the public** using the controller's web site for example.

b) Information of the data subject (Art. 14 GDPR)

Art. 14.1 to 14.4 GDPR shall **not** apply as far as meeting this obligation would disclose information which **by its nature** must be **kept secret**, in particular because of overriding legitimate interests of a third party (Sect. 29.1 FDPA).

In addition to the exception in Art. 14.5 GDPR, the obligation to provide information to the data subject according to Art. 14.1, 14.2, 14.4 GDPR shall **not** apply, inter alia, if providing information would interfere with the **establishment, exercise or defence of legal claim**s, or processing includes data from contracts under private law and is intended to **prevent harm from criminal offences** or the responsible public body has determined with respect to the controller that disclosing the data would **endanger public security** (Sect. 33.1).

Sect. 33.2 FDPA requests for **public, precise, transparent** and **understandable information** when an excep-tion according to Sect. 33.1 FDPA applies.

Sect. 33.3 FDPA makes the information to the data subject dependent on the approval of authorities for the protection of the constitution, the Federal Intelligence Service and the Military Counterintelligence Service when personal data is transmitted from public bodies to the aforementioned bodies.

c) Right of access

Germany's FDPA also provides for exceptions concerning the data subject's right of access. According to Sect. 34.1 FDPA the right of access shall not apply,

- if the data subject shall not be informed pursuant to Sect. 27.2[4], 28.2[5], 33.1 no. 1[6], no. 2 (b)[7] or 33.3 FDPA[8], or
- regarding information which, **by its nature**, must be kept secret according to Sect. 29.1 FDPA, or
- regarding information which may not be erased due to **legal or statutory provisions on retention** or regarding information which only **serves purposes of monitoring data protection or safeguarding data** (i.e. personal data in log files).

The latter exception shall only apply, when providing such type of information would require a **disproportionate effort** for the controller. Additionally, appropriate **technical and organisational measures** have to be implemented so that the data may not be processed for **other purposes**.

According to Sect. 34.2 FDPA the reasons for the refusal to provide information shall be **documented**. Besides, **the grounds for refusa**l of information have to be **communicated to the data subject** unless such communication would undermine the purpose of refusal.

Data stored for the purpose of providing information to the data subject and preparing such provision may be processed only for this purpose and for purposes of data protection monitoring; processing for other purposes shall be restricted according to Art. 18 GDPR.

d) Right to erasure

If erasure of personal data in case **of non-automated data processing** would be impossible or would involve a disproportionate effort due to the specific mode of storage and if the data subject's interest in erasure can be regarded as minimal, the data subject shall **not** have the right to erasure and Art. 18 GDPR shall apply (Sect. 35.1 FDPA).

Furthermore, in cases of Art. 17.1(a) and (d) GDPR the controller is not obliged to delete personal data if it has reason to believe that erasure **would adversely affect legitimate interests of the data** subject (Sect. 35.2 FDPA).

[4] E.g. the right of access would render impossible or seriously impair the achievement of the research or statistical purposes, and such limits are necessary for the fulfilment of the research or statistical purposes.

[5] E.g. archival material is not identified with the person's name or no information is given which would enable the archival material to be found with reasonable administrative effort.

[6] E.g. the information would endanger a public body's tasks or public safety or order.

[7] E.g. a competent public authority has determined that the disclosure of the data is in breach of public policy or public security.

[8] E.g. the provision of information relates to the transfer by public bodies of personal data to the authorities for the protection of the Constitution, the Federal Intelligence Service, the Military Counterintelligence Service.

In addition to Art. 17.3 (b) GDPR the right to erasure shall not apply if erasure **would conflict with retention periods set by statute or contract** (Sect. 35.3 FDPA).

In the latter cases the controller is obliged **to restrict the proccessing**.

e) Data breach

In addition to the exception in Art. 34.3 GDPR, the obligation to inform the data subject of a personal data breach shall **not** apply, as far as meeting this obligation would **disclose information which by law or by its nature must be kept secret**, in particular because of overriding legitimate interests of a third party (Sect. 29.1 sentence 3 FDPA) .

Data protection officer

Designation of the DPO

In addition to Art. 37.1 (b) and (c) GDPR, private bodies shall designate a DPO according to Sect. 38 FDPA, if

- they **constantly employ**, as a rule, at least **ten persons** dealing with the automated processing of personal data, or
- they process personal data subject to *a data protection impact assessment* pursuant to Art. 35 GDPR, or
- if **they commercially process** personal data for the purpose of **transfer, of anonymized transfer or for purposes of market or opinion research**.

DPOs from private and public bodies have special protection against dismissal (Sect. 38.2 FDPA). Furthermore, they have the **duty of confidentiality** (Sect. 38.2 and Sect. 6.5 FDPA).

Communication to the supervisory authority

There is no consistency mechanism in Germany for communicating the appointed DPO to a supervisory authority. Controllers or processors with establishments in several "Länder" of Germany have to communicate a designated DPO **to each competent authority separately**.

Forms provided by the supervisory authorities vary regarding mandatory information to be provided upon communication.

Group DPO

A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment (Art. 37.2 GDPR).

According to a position paper of the German supervisory authorities ("Datenschutzkonferenz") this also includes the case that under German law there is an obligation to designate a DPO and that this DPO is **designated outside Germany for German branches**. In this context, however, it is recommended to locate the DPO in the **European Union** in order to facilitate compliance with the GDPR.[9]

Competences of the supervisory authorities with regard to the DPO

The supervisory authorities shall advise and support the data protection officers to meet their typical needs. They may **demand the dismissal** of a data protection officer if he or she does not have the **expert knowledge** needed to perform his or her tasks or **if there is a serious conflict of interests** as referred to in Art. 38.6 GDPR (Sect. 40.6 FDPA). There have been cases in the past where a DPA has demanded the dismissal of DPO mostly in instances where there was a **conflict of interest** (especially where a DPO had decision making powers in his/her other role being head of IT or head of HR for example).

Sanctions

Criminal offences

Transferring personal data or making data accessible data of a large number of people which are not publicly accessible shall be punishable with imprisonment of up to three years or a fine (Sect. 42.1 FDPA).

Processing without authorization or fraudulently acquiring personal data which are not publicly accessible in return for payment or with the intention of enriching oneself or some else or harming someone shall be punishable with imprisonment of up to two years or a fine (Sect. 42.2 FDPA).

[9] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Kurzpapier_Datenschutzbeauftragte.pdf, p. 2.

The above-mentioned offences shall be prosecuted only if a complaint is filed (Sect. 42.3 FDPA).

A notification pursuant to Art. 33 GDPR or a communication pursuant to Art. 34 GDPR may be used in criminal proceedings against the person required to provide a notification or a communication or relatives as referred to in Section 52 (1) of the Code of Criminal Procedure only with **the consent of the person required to provide a notification or a communication** (Sect. 42.4).

Supervisory Authority

Structure

Due to the structure as a Federal State each "Land" in Germany has established a Supervisory Authority according to Art. 51 GDPR. Besides each authority of a "Land", the Federal Data Protection Commissioner ("BfDI") shall be competent to supervise **public bodies of the Federation**, also when taking part in competition as enterprises governed by public law and **processors** if they are private bodies **under control of the Federation** (see further requirements in Sect. 9 FDPA)

Consistency Mechanism

The Federal Commissioner shall serve as the **joint representative** on the **European Data Protection Board** and single contact point (joint representative) ensuring a smooth and swift cooperation with other concerned supervisory authorities (Sect. 17 FDPA).

The supervisory authority of a "Land "serves as the **joint representative's deputy** and shall be elected by the "Bundesrat". Sect 18 holds procedures for cooperation among the Federal Data Protection Commissioner and the "Länder" supervisory authorities such as the opportunity to comment on matters at an early stage and providing each other all relevant information for commenting.

Powers

If a supervisory authority determines that data protection legislation has been violated, it shall have the power to **inform the data subjects** concerned, **to report the violation to other bodies responsible for prosecution or punishment** and, in the case of serious violations, **to notify the trade supervisory authority** to take measures under trade and industry law (Art. 40.3 sentence 2 FDPA).

Persons assigned by the supervisory authority to monitor compliance with data protection legislation shall be authorized, as needed to perform their tasks, **to enter the property and premises** of the body and **to have access to all data processing equipment and means**. The body shall be obligated to tolerate such access (Art. 40.5 FDPA).

The German Association for Data Protection and Data Security (GDD) is a non-profit association advocating a meaningful, justifiable and technically feasible data protection. Its aim is to support controllers an processors - in particular data protection officers - in solving and implementing the various legal, technical and organisational requirements associated with data protection and data security.

Die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen - insbesondere auch die Datenschutzbeauftragten - bei der Lösung und Umsetzung der vielfältigen mit Datenschutz und Datensicherheit verbundenen rechtlichen, technischen und organisatorischen Anforderungen zu unterstützen.

Gesellschaft für Datenschutz und Datensicherheit e.V.
Heinrich-Böll-Ring 10, D-53119 Bonn
info@gdd.de | www.gdd.de