Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680

(DSAnpUG-EU)

of 30 June 2017

The Bundestag has adopted the following Act with the approval of the Bundesrat:

Article 1

Federal Data Protection Act

(BDSG)

Table of Contents

Sub-chapter 2
Special processing situations

Chapter 2
Rights of the data subject

Chapter 3
Obligations of controllers and processors

Chapter 4
Supervisory authorities for data processing by private bodies

Chapter 4
Obligations of controllers and processors

Chapter 5
Transfers of data to third countries and to international organizations

Chapter 6
Cooperation among supervisory authorities

Chapter 7
Liability and penalties

Part 4
Special provisions for processing in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680

Part I

Common provisions

Chapter 1

Scope and definitions

Section 1

Scope of the Act

(1) This Act shall apply to the processing of personal data by

1. public bodies of the Federation,

2. public bodies of the *Länder*, where data protection is not governed by *Land* law and where they

   a) carry out federal law or

   b) act in the capacity of judicial bodies in matters other than administrative matters.

For private bodies, this Act shall apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system unless such processing is conducted by natural persons in the course of a purely personal or domestic activity.

(2) Other federal data protection legislation shall take precedence over the provisions of this Act. If such legislation does not govern a matter conclusively or at all which is covered by this Act, then this Act shall apply. The duty to observe the legal obligation of maintaining secrecy or professional or special official confidentiality not based on legal provisions shall remain unaffected.

(3) The provisions of this Act shall take precedence over those of the Administrative Procedure Act where personal data are processed to establish the facts.

(4) This Act shall apply to public bodies. It shall apply to private bodies if

1. the controller or processor processes personal data in Germany,

2. personal data are processed in the context of the activities of an establishment of the controller or processor in Germany, or if,

3. although the controller or processor has no establishment in a Member State of the European Union or another contracting state of the European Economic Area, it does fall within the scope of Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119 of 4 May 2016, p. 1; L 314 of 22 November 2016, p. 72).

If this Act does not apply in accordance with the second sentence, only Sections 8 to 21 and 39 to 44 shall apply to the controller or processor.

(5) The provisions of this Act shall not apply where the law of the European Union, in particular Regulation (EU) 2016/679 in the applicable version, directly applies.

(6) The contracting states of the European Economic Area and Switzerland shall have equal status with the Member States of the European Union with regard to processing for purposes in accordance with Article 2 of Regulation (EU) 2016/679. Other states shall be regarded as third countries.

(7) With regard to processing for purposes in accordance with Article 1 (1) of Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119 of 4 May 2016, p. 89), the states associated with the implementation, application and development of the Schengen Acquis shall have equal status with the Member States of the European Union. Other states shall be regarded as third countries.

(8) Regulation (EU) 2016/679 and Parts 1 and 2 of this Act shall apply accordingly to processing of personal data by public bodies in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 unless otherwise provided for in this or another Act.

Section 2

Definitions

(1) Public bodies of the Federation are the authorities, judicial bodies and other public law institutions of the Federation, of direct federal corporations, statutory bodies and foundations established under public law and of their associations irrespective of their legal form.

(2) Public bodies of the *Länder* are the authorities, judicial bodies and other public law institutions of a *Land*, a municipality, an association of municipalities or of other legal

persons under public law subject to *Land* supervision and of their associations irrespective of their legal form.

(3) Associations of public bodies of the Federation and the *Länder* which are established under private law and perform tasks of public administration shall be regarded as public bodies of the Federation irrespective of the participation of private bodies if

1. they operate beyond the borders of a *Land*, or

2. the Federation holds the absolute majority of shares or controls the absolute majority of votes.

Otherwise they shall be regarded as public bodies of the *Länder*.

(4) Private bodies are natural and legal persons, societies and other associations established under private law unless they are covered by subsections 1 to 3. If a private body performs sovereign tasks of the public administration, it shall be a public body as defined in this Act.

(5) Public bodies of the Federation shall be regarded as private bodies as defined in this Act if they take part in competition as enterprises governed by public law. Public bodies of the *Länder* shall also be regarded as private bodies as defined in this Act if they take part in competition as enterprises governed by public law and carry out federal law, and if data protection is not governed by *Land* law.

Chapter 2

Legal basis for processing personal data

Section 3

Processing of personal data by public bodies

Public bodies shall be permitted to process personal data if such processing is necessary to perform the task for which the controller is responsible or to exercise official authority which has been vested in the controller.

Section 4

Video surveillance of publicly accessible spaces

(1) Monitoring publicly accessible areas with optical-electronic devices (video surveillance) shall be permitted only as far as it is necessary

1. for public bodies to perform their tasks,

2. to exercise the right to determine who shall be allowed or denied access or

3. to safeguard legitimate interests for specifically defined purposes

and if there is nothing to indicate legitimate overriding interests of the data subjects. For video surveillance of

1. large publicly accessible facilities, such as sport facilities, places of gathering and entertainment, shopping centres and car parks, or

2. vehicles and large publicly accessible facilities of public rail, ship or bus transport,

protecting the lives, health and freedom of persons present shall be regarded as a very important interest.

(2) Appropriate measures shall be taken to make the surveillance and the controller's name and contact details identifiable as early as possible.

(3) Storing or using data collected pursuant to subsection 1 shall be permitted if necessary to achieve the intended purpose and if there is nothing to indicate legitimate overriding interests of the data subjects. Subsection 1, second sentence, shall apply accordingly. The data may be further processed for another purpose only if necessary to prevent threats to state and public security and to prosecute crimes.

(4) If data collected from video surveillance are attributed to a particular person, that person shall be informed of the processing in accordance with Articles 13 and 14 of Regulation (EU) 2016/679. Section 32 shall apply accordingly.

(5) The data shall be deleted without delay, if they are no longer needed for the intended purpose or if the data subject's legitimate interests stand in the way of any further storage.

Chapter 3

Data protection officers of public bodies

Section 5

Designation

(1) Public bodies shall designate a data protection officer. This shall also apply to public bodies as defined in Section 2 (5) which take part in competition.

(2) A single data protection officer may be designated for several public bodies, taking account of their organizational structure and size.

(3) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Section 7.

(4) The data protection officer may be a staff member of the public body, or fulfil the tasks on the basis of a service contract.

(5) The public body shall publish the contact details of the data protection officer and communicate them to the Federal Commissioner for Data Protection and Freedom of Information.

Section 6

Position

(1) The public body shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The public body shall support the data protection officer in performing the tasks referred to in Section 7 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

(3) The public body shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. The data protection officer shall directly report to the highest management level of the public body. The data protection officer shall not be dismissed or penalized by the public body for performing his or her tasks.

(4) The dismissal of the data protection officer shall be permitted only by applying Section 626 of the Civil Code accordingly. The data protection officer's employment shall not be terminated unless there are facts which give the public body just cause to terminate without notice. After the activity as data protection officer has ended, the data protection officer may not be terminated for a year following the end of appointment, unless the public body has just cause to terminate without notice.

(5) Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under Regulation (EU) 2016/679, this Act and other data protection legislation. The data protection officer shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless they are released from this obligation by the data subject.

(6) Where in the course of their activities data protection officers become aware of data for which the head of a public body or a person employed by such a body has the right to refuse to give evidence for employment-related reasons, this right shall also apply to the data protection officer and his or her assistants. The person to whom the right to refuse to give evidence applies for employment-related reasons shall decide whether to exercise this right unless it is impossible to effect such a decision in the foreseeable future. Where the right of the data protection officer to refuse to give evidence applies, his or her files and other documents shall not be subject to seizure.

Section 7

Tasks

(1) In addition to the tasks listed in Regulation (EU) 2016/679, the data protection officer shall have at least the following tasks:

1. to inform and advise the public body and the employees who carry out processing of their obligations pursuant to this Act and other data protection legislation, including legislation enacted to implement Directive (EU) 2016/680;

2. to monitor compliance with this Act and other data protection legislation, including legislation enacted to implement Directive (EU) 2016/680, and with the policies of the public body in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

3. to provide advice as regards the data protection impact assessment and monitor its implementation pursuant to Section 67 of this Act;

4. to cooperate with the supervisory authority;

5. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Section 69 of this Act, and to consult, where appropriate, with regard to any other matter.

In the case of a data protection officer ordered by a court, these tasks shall not refer to the action of the court acting in its judicial capacity.

(2) The data protection officer may perform other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

(3) The data protection officer shall in the performance of his or her tasks give due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Chapter 4

Federal Commissioner for Data Protection and Freedom of Information

Section 8

Establishment

(1) The Federal Commissioner for Data Protection and Freedom of Information (Federal Commissioner) shall be a supreme federal authority. It is located in Bonn.

(2) Civil servants of the Federal Commissioner shall be federal civil servants.

(3) The Federal Commissioner may delegate human resources administration and management tasks to other federal bodies as long as doing so does not affect the Federal Commissioner’s independence. Personal data of staff members may be transmitted to these bodies as needed for them to perform their delegated tasks.

Section 9

Competence

(1) The Federal Commissioner shall be competent to supervise the public bodies of the Federation, also if they take part in competition as enterprises governed by public law. The provisions of this chapter shall also apply to processors if they are private bodies in which the Federation holds the absolute majority of shares or controls the absolute majority of votes and they process data on behalf of a public body of the Federation

(2) The Federal Commissioner shall not be competent to supervise processing operations of federal courts acting in their judicial capacity.

Section 10

Independence

(1) The Federal Commissioner shall act with complete independence in performing his or her tasks and exercising his or her powers. The Federal Commissioner shall remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

(2) The Federal Commissioner shall be subject to audit by the Bundesrechnungshof as long as this does not affect his or her independence.

Section 11

Appointment and term of office

(1) At the proposal of the Federal Government, the German Bundestag shall elect without debate the Federal Commissioner with more than half of the statutory number of its members. The person elected shall be appointed by the Federal President. The Federal Commissioner must be at least 35 years old at the time of election. He or she shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform his or her duties and exercise his or her powers. In particular, the Federal Commissioner must have knowledge of data protection law acquired from the relevant professional experience and be qualified for judicial office or higher administrative service.

(2) The Federal Commissioner shall swear the following oath before the Federal President: “I swear to do everything in my power to further the good and the benefit of the German people, to protect them from harm and to defend the Basic Law and the laws of the Federation, to perform my duties conscientiously and to exercise justice in all my dealings, so help me God.” The reference to God may be omitted from the oath.

(3) The Federal Commissioner’s term of office shall be five years. It may be renewed once.

Section 12

Official relationship

(1) The Federal Commissioner shall, in accordance with this Act, have official federal status under public law.

(2) The official relationship shall begin upon delivery of the certificate of appointment. It shall end upon expiry of the term of office or upon resignation. The Federal President shall remove the Federal Commissioner from office at the request of the President of the Bundestag if the Federal Commissioner has committed serious misconduct or no longer meets the requirements for performing his or her tasks. If the official relationship is ended or the Federal Commissioner is removed from office, the Federal Commissioner shall be given a document signed by the Federal President. Removal from office shall be effective upon delivery of this document. If the official relationship ends upon expiry of the term of office, at the request of the President of the Bundestag the Federal Commissioner shall be obligated to continue his or her work for no more than six months until a successor has been appointed.

(3) The senior civil servant shall exercise the rights of the Federal Commissioner if the latter is unable to perform his or her duties or if his or her term of office has expired and he or she is no longer obligated to continue his or her work. Section 10 (1) shall apply accordingly.

(4) From the start of the calendar month in which the official relationship commences until the end of the calendar month in which it ends, or, in the case of subsection 2, sixth sentence, until the end of the month in which he or she ceases his or her work, the Federal Commissioner shall be paid at the level of a federal civil servant in pay grade B 11 plus the family allowance according to Annex V of the Federal Civil Servants' Remuneration Act. The Federal Travel Expenses Act and the Federal Relocation Expenses Act shall apply accordingly. In all other respects, Section 12 (6), Sections 13 through 20 and 21a (5) of the Act on Federal Ministers shall apply, except that the four-year term of office stipulated in Section 15 (1) of the Act on Federal Ministers shall be replaced by a five-year term. By way of derogation from the third sentence in conjunction with Sections 15 through 17 and 21a (5) of the Act on Federal Ministers, the Federal Commissioner's pension shall be calculated, counting his or her term as Federal Commissioner as a pensionable period of service, on the basis of the Federal Act Governing Civil Servants' Pensions and Allowances, if this is more favourable and if, before his or election as Federal Commissioner, he or she was a civil servant or judge in at least the last position to be held before reaching pay grade B 11.

Section 13

Rights and obligations

(1) The Federal Commissioner shall refrain from any action incompatible with his or her duties and shall not, during his or her term of office, engage in any incompatible occupation, whether gainful or not. In particular, the Federal Commissioner shall not hold any other paid office or pursue any commercial activity or occupation in addition to his or her official duties and shall not belong to the management or supervisory board of a profit-oriented enterprise, nor to a government or legislative body of the Federation or a *Land*. The Federal Commissioner shall not deliver extra-judicial opinions in exchange for payment.

(2) The Federal Commissioner shall inform the President of the Bundestag of any gifts received in connection with his or her office. The President of the Bundestag shall decide how such gifts shall be used. He or she may issue procedural rules and regulations.

(3) The Federal Commissioner shall have the right to refuse to give testimony concerning persons who have confided in him or her in his or her capacity as Federal Commissioner and concerning the information confided. This shall also apply to the staff of the Federal Commissioner, on the condition that the Federal Commissioner decides on the exercise of this right. Within the scope of the Federal Commissioner's right of refusal to give testimony, he or she shall not be required to submit or surrender files or other documents.

(4) Even after his or her official relationship has ended, the Federal Commissioner shall be obligated to secrecy concerning matters of which he or she is aware by reason of his or her official duties. This obligation shall not apply to official communications or to matters which are common knowledge or which by their nature do not require confidentiality. The Federal Commissioner shall decide at his or her due discretion whether and to what extent he or she will testify in or outside court or make statements concerning such matters; if he or she is no longer in office, the permission of the Federal Commissioner in office shall be required. This shall not affect the legal obligation to report crimes and to

uphold the free and democratic order wherever it is threatened. Sections 93, 97, 105 (1), Section 111 (5) in conjunction with Section 105 (1) and Section 116 (1) of the German Fiscal Code shall not apply to the Federal Commissioner or his or her staff. The fifth sentence shall not apply where the financial authorities require such knowledge in order to conduct legal proceedings due to a tax offence and related tax proceedings, in the prosecution of which there is compelling public interest, or where the person required to provide information or persons acting on his or her behalf have intentionally provided false information. If the Federal Commissioner determines that data protection provisions have been violated, he or she shall be authorized to report the violation and inform the data subject accordingly.

(5) The Federal Commissioner may testify as a witness unless such testimony would

1. be detrimental to the welfare of the Federation or a *Land*, in particular to the security of the Federal Republic of Germany or its relations with other countries, or

2. would violate fundamental rights.

If the testimony concerns ongoing or completed processes which are or could be considered core aspects of executive responsibility, the Federal Commissioner may testify only with the approval of the Federal Government. Section 28 of the Federal Constitutional Court Act shall remain unaffected.

(6) Subsections 3 and 4, fifth to seventh sentences, shall apply accordingly to the public bodies responsible for monitoring compliance with the data protection provisions in the *Länder*.

Section 14

Tasks

(1) In addition to the tasks listed in Regulation (EU) 2016/679, the Federal Commissioner shall have the following tasks:

1. to monitor and enforce the application of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680;

2. to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data, paying special attention to measures specifically for children;

3. to advise the German Bundestag, the Bundesrat, the Federal Government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data;

4. to promote the awareness of controllers and processors of their obligations under this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680;

5. upon request, to provide information to any data subject concerning the exercise of their rights under this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680, and if appropriate, to cooperate with the supervisory authorities in other Member States to that end;

6. to handle complaints lodged by a data subject, or by a body, organization or association in accordance with Article 55 of Directive (EU) 2016/680, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

7. to cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities, to ensure the consistency of application and enforcement of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680;

8. to conduct investigations on the application of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680, also on the basis of information received from another supervisory authority or other public authority;

9. to monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

10. to provide advice on the processing operations referred to in Section 69; and

11. to contribute to the activities of the European Data Protection Board.

Within the scope of Directive (EU) 2016/680, the Federal Commissioner shall also perform the task pursuant to Section 60.

(2) To carry out the task listed in subsection 1, first sentence, no. 3, the Federal Commissioner may, on request or at its own initiative, make recommendations to the German Bundestag or one of its committees, the Bundesrat, the Federal Government, other institutions and bodies and the public concerning all matters related to the protection of personal data. At the request of the German Bundestag, one of its committees or of the Federal Government, the Federal Commissioner shall also investigate data protection matters and incidents at public bodies of the Federation.

(3) The Federal Commissioner shall facilitate the submission of complaints referred to in subsection 1, first sentence, no. 6 by measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(4) The performance of the duties of the Federal Commissioner shall be free of charge for the data subject. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the Federal Commissioner may charge a reasonable fee based on administrative costs, or refuse to act on the request. The Federal Commissioner shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Section 15

Activity reports

The Federal Commissioner shall produce an annual activity report which may contain a list of the types of violations reported and the types of measures taken, including penalties and measures taken in accordance with Article 58 (2) of Regulation (EU) 2016/679. The Federal Commissioner shall submit this report to the German Bundestag, the Bun-

desrat and the Federal Government and shall make it available to the public, the European Commission and the European Data Protection Board.

Section 16

Powers

(1) The Federal Commissioner shall have, within the scope of Regulation (EU) 2016/679, the powers referred to in Article 58 of Regulation (EU) 2016/679. If the Federal Commissioner concludes that data protection legislation has been violated or that there are other problems with the processing of personal data, he or she shall inform the competent authority for legal or technical matters and, before exercising the powers referred to in Article 58 (2) (b) to (g), (i) and (j) of Regulation (EU) 2016/679, shall give this authority the opportunity to provide its opinion to the controller within a reasonable period. The opportunity to provide an opinion may be dispensed with if an immediate decision seems necessary due to imminent danger or in the public interest, or if it would conflict with compelling public interests. The opinion should also include a description of the measures taken on the basis of the information from the Federal Commissioner.

(2) If the Federal Commissioner finds that, in data processing for purposes beyond the scope of Regulation (EU) 2016/679, public bodies of the Federation have violated this Act or other data protection legislation or there are other insufficiencies with their processing or use of personal data, the Federal Commissioner shall lodge a complaint with the competent supreme federal authority and shall require this authority to respond within a period to be determined by the Federal Commissioner. The Federal Commissioner may dispense with a complaint or a response, especially if the problems involved are insignificant or have been remedied in the meantime. The response should also describe the measures taken as a result of the Federal Commissioner's complaint. The Federal Commissioner may also warn a controller that intended processing operations are likely to violate provisions of this Act and other data protection provisions which apply to the data processing in question.

(3) The powers of the Federal Commissioner shall also extend to

1. personal data obtained by public bodies of the Federation concerning the contents of and specific circumstances relating to postal communications and telecommunications, and

2. personal data subject to professional or special official secrecy, especially tax secrecy under Section 30 of the German Fiscal Code.

The fundamental right to privacy of correspondence, posts and telecommunications in Article 10 of the Basic Law shall be limited accordingly.

(4) The public bodies of the Federation shall be obligated to provide the Federal Commissioner and his or her assistants with the following:

1. access to all official premises at all times, including to any data processing equipment and means, and to all personal data and all information necessary to perform their tasks; and

2. all information necessary to perform their tasks.

(5) The Federal Commissioner shall work to cooperate with the public bodies responsible for monitoring compliance with data protection provisions in the *Länder* and with

the supervisory authorities under Section 40. Section 40 (3), first sentence, second half-sentence, shall apply accordingly.

Chapter 5

Representation on the European Data Protection Board, single contact point, cooperation among the federal supervisory authorities and those of the *Länder* concerning European Union matters

Section 17

Representation on the European Data Protection Board, single contact point

(1) The Federal Commissioner shall serve as the joint representative on the European Data Protection Board and single contact point (joint representative). The Bundesrat shall elect the head of the supervisory authority of a *Land* to serve as the joint representative's deputy (deputy). The term shall be five years. When the head of the supervisory authority of a *Land* leaves office, his or her function as deputy shall end at the same time. The deputy may be re-elected.

(2) At the deputy's request, the joint representative shall delegate to him or her the leadership of negotiations and the voting right in the European Data Protection Board in matters dealing with the performance of a task for which the *Länder* alone have the right to legislate, or which affect the establishment or procedures of *Land* authorities.

Section 18

Procedures for cooperation among the federal and *Länder* supervisory authorities

(1) The Federal Commissioner and the supervisory authorities of the *Länder* (supervisory authorities of the Federation and the *Länder*) shall work together in European Union matters with the aim of consistently applying Regulation (EU) 2016/679 and Directive (EU) 2016/680. Before submitting a common position to the supervisory authorities of the other Member States, the European Commission or the European Data Protection Board, the supervisory authorities of the Federation and the *Länder* shall give each other the opportunity to comment at an early stage. For this purpose, they shall share all relevant information. The supervisory authorities of the Federation and the *Länder* shall consult the specific supervisory authorities established under Articles 85 and 91 of Regulation (EU) 2016/679 if these authorities are affected by the matter.

(2) If the supervisory authorities of the Federation and the *Länder* fail to achieve agreement on a common position, the lead supervisory authority, or, in the absence of a lead authority, the joint representative and his or her deputy, shall present a recommendation for a common position. If the joint representative and his or her deputy fail to agree on a recommendation for a common position, the deputy shall determine the recommendation for a common position in matters dealing with the performance of a task for which the *Länder* alone have the right to legislate, or which affect the establishment or procedures of *Land* authorities. For matters other than those referred to in the second sentence in which the joint representative and deputy fail to agree, the joint representative shall determine the common position. The negotiations shall be based on the position recommended pursuant to the first to third sentences unless the supervisory authorities of the Federation

and the *Länder* adopt a different position with a simple majority. The Federation and each *Land* each have one vote. Abstentions shall not be counted.

(3) The joint representative and his or her deputy shall be bound by the common position pursuant to subsections 1 and 2 and shall determine by mutual agreement the conduct of negotiations according to this common position. Should they fail to reach agreement, the deputy shall decide the further conduct of negotiations for the matters referred to in Section 18 (2), second sentence. For other matters, the joint representative shall have the deciding vote.

Section 19

Responsibilities

(1) The lead supervisory authority of a *Land* in the one-stop-shop mechanism pursuant to Chapter VII of Regulation (EU) 2016/679 shall be the supervisory authority of the *Land* in which the controller or processor has its main establishment, as referred to in Article 4 no. 16 of Regulation (EU) 2016/679 or its single establishment in the European Union, as referred to in Article 56 (1) of Regulation (EU) 2016/679. Article 56 (1) in conjunction with Article 4 no. 16 of Regulation (EU) 2016/679 shall apply accordingly within the Federal Commissioner's area of responsibility. If there is no agreement on determining the lead supervisory authority, the procedure described in Section 18 (2) shall be applied accordingly.

(2) The supervisory authority with which a data subject has lodged a complaint shall forward the complaint to the lead supervisory authority referred to in subsection 1; in the absence of such a lead supervisory authority, the complaint shall be forwarded to the supervisory authority of a *Land* in which the controller or processor has an establishment. If a complaint is lodged with a supervisory authority which is not responsible for the matter, this authority shall forward the complaint to the supervisory authority where the applicant resides, if it is not possible to forward the complaint as referred to in the first sentence. The receiving supervisory authority shall be regarded as the supervisory authority according to Chapter VII of Regulation (EU) 2016/679 with whom the complaint was lodged, and shall fulfil the obligations referred to in Article 60 (7) to (9) and Article 65 (6) of Regulation (EU) 2016/679.

Chapter 6

Legal remedies

Section 20

Judicial remedy

(1) Recourse to the administrative courts shall be provided for disputes between natural or legal persons and a supervisory authority of the Federation or a *Land* concerning rights according to Article 78 (1) and (2) of Regulation (EU) 2016/679 and Section 61. The first sentence shall not apply to administrative fine proceedings.

(2) The Code of Administrative Court Procedure shall be applied in compliance with subsections 3 to 7.

(3) For proceedings pursuant to subsection 1, first sentence, the administrative court in whose district the supervisory authority is located shall be locally competent.

(4) In proceedings pursuant to subsection 1, first sentence, the supervisory authority shall be competent to take part.

(5) Parties to proceedings pursuant to subsection 1, first sentence, shall be

1. the natural or legal person as plaintiff or applicant, and

2. the supervisory authority as defendant or respondent.

Section 63 nos. 3 and 4 of the Code of Administrative Court Procedure shall remain unaffected.

(6) No preliminary proceedings shall take place.

(7) With respect to an authority or its legal entity, the supervisory authority shall not order immediate execution in accordance with Section 80 (2), first sentence, no. 4 of the Code of Administrative Court Procedure.

Section 21

Application of the supervisory authority for a court decision if it believes that an adequacy decision by the European Commission violates the law

(1) If a supervisory authority believes that an adequacy decision of the European Commission or a decision on the recognition of standard protection clauses or on the general validity of approved codes of conduct, on the validity of which a decision of the supervisory authority depends, violates the law, the supervisory authority shall suspend its procedure and lodge an application for a court decision.

(2) Recourse to the administrative courts shall be provided for proceedings pursuant to subsection 1. The Code of Administrative Court Procedure shall be applied in compliance with subsections 3 to 6.

(3) The Federal Administrative Court shall decide in the first and last instance on an application by the supervisory authority pursuant to subsection 1.

(4) In proceedings pursuant to subsection 1, the supervisory authority shall be competent to take part. The supervisory authority shall be a party to proceedings pursuant to subsection 1 as applicant; Section 63 nos. 3 and 4 of the Code of Administrative Court Procedure shall remain unaffected. The Federal Administrative Court may give the European Commission the opportunity to comment within a period of time to be determined.

(5) If a proceeding to review the validity of a European Commission decision pursuant to subsection 1 is pending at the European Court of Justice, the Federal Administrative Court may order its proceeding to be suspended until the proceeding at the European Court of Justice has been concluded.

(6) In proceedings pursuant to subsection 1, Section 47 (5), first sentence and (6) of the Code of Administrative Court Procedure shall apply accordingly. If the Federal Administrative Court finds that the European Commission’s decision pursuant to subsection 1 is valid, it shall state this in its decision. Otherwise it shall refer the question as to the validity of the decision in accordance with Article 267 of the Treaty on the Functioning of the European Union to the European Court of Justice.

Part 2

Implementing provisions for processing for purposes in accordance with Article 2 of Regulation (EU) 2016/679

Chapter 1

Legal basis for processing personal data

Sub-chapter 1

Processing of special categories of personal data and processing for other purposes

Section 22

Processing of special categories of personal data

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted

1. by public and private bodies if

   a) processing is necessary to exercise the rights derived from the right of social security and social protection and to meet the related obligations;

   b) processing is necessary 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; or

   c) processing is necessary 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; in addition to the measures referred to in subsection 2, in particular occupational and criminal law provisions to ensure professional secrecy shall be complied with;

2. by public bodies if

   a) processing is urgently necessary for reasons of substantial public interest;

   b) processing is necessary to prevent a substantial threat to public security;

   c) processing is urgently necessary to prevent substantial harm to the common good or to safeguard substantial concerns of the common good; or

d) processing is necessary for urgent reasons of defence or to fulfil supra- or intergovernmental obligations of a public body of the Federation in the field of crisis management or conflict prevention or for humanitarian measures;

and as far as the interests of the controller in data processing in the cases of no. 2 outweigh the interests of the data subject.

(2) In the cases of subsection 1, appropriate and specific measures shall be taken to safeguard the interests of the data subject. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:

1. technical organizational measures to ensure that processing complies with Regulation (EU) 2016/679;

2. measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;

3. measures to increase awareness of staff involved in processing operations;

4. designation of a data protection officer;

5. restrictions on access to personal data within the controller and by processors;

6. the pseudonymization of personal data;

7. the encryption of personal data;

8. measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access 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;

10. specific rules of procedure to ensure compliance with this Act and with Regulation (EU) 2016/679 in the event of transfer or processing for other purposes.

Section 23

Processing for other purposes by public bodies

(1) Public bodies shall be permitted to process personal data for a purpose other than the one for which the data were collected where such processing is necessary for them to perform their duties and if

1. it is obviously in the interest of the data subject and there is no reason to assume that the data subject would refuse consent if he or she were aware of the other purpose;

2. it is necessary to check information provided by the data subject because there is reason to believe that this information is incorrect;

3. processing is necessary to prevent substantial harm to the common good or a threat to public security, defence or national security; to safeguard substantial concerns of the common good; or to ensure tax and customs revenues;

4. processing is necessary to prosecute criminal or administrative offences, to carry out or enforce punishment or measures as referred to in Section 11 (1) no. 8 of the Criminal Code or educational or disciplinary measures as referred to in the Juvenile Court Act or to enforce fines;

5. processing is necessary to prevent serious harm to the rights of another person; or

6. processing is necessary to exercise powers of supervision and monitoring, to conduct audits or organizational analyses of the controller; this shall also apply to processing for training and examination purposes by the controller, as long as it does not conflict with the legitimate interests of the data subject.

(2) The processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 for a purpose other than the one for which the data were collected shall be permitted if the conditions of subsection 1 are met and an exception pursuant to Article 9 (2) of Regulation (EU) 2016/679 or pursuant to Section 22 applies.

Section 24

Processing for other purposes by private bodies

(1) Private bodies shall be permitted to process personal data for a purpose other than the one for which the data were collected if

1. processing is necessary to prevent threats to state or public security or to prosecute criminal offences; or

2. processing is necessary for the establishment, exercise or defence of legal claims,

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

(2) The processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 for a purpose other than the one for which the data were collected shall be permitted if the conditions of subsection 1 are met and an exception pursuant to Article 9 (2) of Regulation (EU) 2016/679 or pursuant to Section 22 applies.

Section 25

Transfer of data by public bodies

(1) The transfer of personal data by public bodies to public bodies shall be permitted if it is necessary for the transferring body or the third party to whom the data are transferred to perform their duties and the conditions are met which would permit processing pursuant to Section 23. The third party to whom the data are transferred shall process the transferred data only for the purpose for which they were transferred. Processing for other purposes shall be permitted only if the conditions of Section 23 are met.

(2) Public bodies shall be permitted to transfer personal data to private bodies if

1. transfer is necessary for the transferring body to perform its duties and the conditions are met which would permit processing pursuant to Section 23;

2. the third party to whom the data are transferred credibly presents a legitimate interest in knowledge of the data to be transferred and the data subject does not have a legitimate interest in not having the data transferred; or

3. processing is necessary for the establishment, exercise or defence of legal claims;

and the third party has promised the public body transferring the data that it will process them only for the purpose for which they were transferred. Processing for other purposes shall be permitted if transfer pursuant to the first sentence would be permitted and the transferring body has consented to the transfer.

(3) The transfer of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted if the conditions of subsection 1 or 2 are met and an exception pursuant to Article 9 (2) of Regulation (EU) 2016/679 or pursuant to Section 22 applies.

Sub-chapter 2

Special processing situations

Section 26

Data processing for employment-related purposes

(1) Personal data of employees may be processed for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract or to exercise or satisfy rights and obligations of employees' representation laid down by law or by collective agreements or other agreements between the employer and staff council. Employees' personal data may be processed to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason.

(2) If personal data of employees are processed on the basis of consent, then the employee's level of dependence in the employment relationship and the circumstances under which consent was given shall be taken into account in assessing whether such consent was freely given. Consent may be freely given in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests. Consent shall be given in written form, unless a different form is appropriate because of special circumstances. The employer shall inform the employee in text form of the purpose of data processing and of the employee's right to withdraw consent pursuant to Article 7 (3) of Regulation (EU) 2016/679.

(3) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 for employment-related purposes shall be permitted if it 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 in not processing the data. Subsection 2 shall also apply to consent to the processing of special categories of personal data; consent must explicitly refer to these data. Section 22 (2) shall apply accordingly.

(4) The processing of personal data, including special categories of personal data of employees for employment-related purposes, shall be permitted on the basis of collective agreements. The negotiating partners shall comply with Article 88 (2) of Regulation (EU) 2016/679.

(5) The controller must take appropriate measures to ensure compliance in particular with the principles for processing personal data described in Article 5 of Regulation (EU) 2016/679.

(6) The rights of participation of staff councils shall remain unaffected.

(7) Subsections 1 to 6 shall also apply when personal data, including special categories of personal data, of employees are processed without forming or being intended to form part of a filing system.

(8) For the purposes of this Act, employees are

1. dependently employed workers, including temporary workers contracted to the borrowing employer;

2. persons employed for occupational training purposes;

3. participants in benefits to take part in working life, in assessments of occupational aptitude or work trials (persons undergoing rehabilitation);

4. persons employed in accredited workshops for persons with disabilities;

5. volunteers working pursuant to the Youth Volunteer Service Act or the Federal Volunteer Service Act;

6. persons who should be regarded as equivalent to dependently employed workers because of their economic dependence; these include persons working at home and their equivalents;

7. federal civil servants, federal judges, military personnel and persons in the alternative civilian service.

Applicants for employment and persons whose employment has been terminated shall be regarded as employees.

Section 27

Data processing for purposes of scientific or historical research and for statistical purposes

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted also without consent for scientific or historical research purposes or statistical purposes, if such processing is necessary for these purposes and the interests of the controller in processing substantially outweigh those of the data subject in not processing the data. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

(2) The rights of data subjects provided in Articles 15, 16, 18 and 21 of Regulation (EU) 2016/679 shall be limited to the extent that these rights are likely to 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. Further, the right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if the data are necessary for purposes of scientific research and the provision of information would involve disproportionate effort.

(3) In addition to the measures listed in Section 22 (2), special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 processed for scientific or historical research purposes or statistical purposes shall be rendered anonymous as soon as the research or statistical purpose allows, unless this conflicts with legitimate interests of the data subject. Until such time, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. They may be combined with the information only to the extent required by the research or statistical purpose.

(4) The controller may publish personal data only if the data subject has provided consent or if doing so is indispensable for the presentation of research findings on contemporary events.

Section 28

Data processing for archiving purposes in the public interest

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted if necessary for archiving purposes in the public interest. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

(2) The right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if the 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.

(3) The right of the data subject to rectification according to Article 16 of Regulation (EU) 2016/679 shall not apply if the personal data are processed for archiving purposes in the public interest. If the data subject disputes the accuracy of the personal data, he or she shall have the opportunity to present his or her version. The responsible archive shall be obligated to add this version to the files.

(4) The rights provided in Article 18 (1) (a), (b) and (d) and in Articles 20 and 21 of Regulation (EU) 2016/679 shall not apply as far as these rights are likely to render impossible or seriously impair the achievement of the archiving purposes in the public interest, and the exceptions are necessary to fulfil those purposes.

Section 29

Rights of the data subject and powers of the supervisory authorities in the case of secrecy obligations

(1) In addition to the exceptions in Article 14 (5) of Regulation (EU) 2016/679, the obligation to provide information to the data subject according to Article 14 (1) to (4) of Regulation (EU) 2016/679 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. The right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply as far as access 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. In addition to the exception in Article 34 (3) of Regulation (EU) 2016/679, the obligation to inform the data subject of a personal data breach according to Article 34 of Regulation (EU) 2016/679 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. By derogation from the exception pursuant to the third sentence, the data subject pursuant to Article 34 of Regulation (EU) 2016/679 shall be informed if the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

(2) If in the context of a client-lawyer relationship the data of third persons are transferred to persons subject to a legal obligation of professional secrecy, the transferring body shall not be obligated to inform the data subject according to Article 13 (3) of Regulation (EU) 2016/679 unless the data subject has an overriding interest in being informed.

(3) The supervisory authorities shall not have the investigative powers according to Article 58 (1) (e) and (f) of Regulation (EU) 2016/679 with regard to the persons listed in Section 203 (1), (2a) and (3) of the Criminal Code or their processors as far as exercising these powers would violate these persons' obligations to secrecy. If in the context of an investigation a supervisory authority becomes aware of data subject to an obligation of secrecy as referred to in the first sentence, the obligation of secrecy shall also apply to the supervisory authority.

Section 30

Consumer loans

(1) Any body which for the purpose of transfer commercially collects, stores or modifies personal data which may be used to evaluate the creditworthiness of consumers shall treat requests for information from lenders in other European Union Member States the same way it treats information requests from domestic lenders.

(2) Anyone who refuses to conclude a consumer loan contract or a contract concerning financial assistance for payment with a consumer as the result of information provided by a body as referred to in subsection 1 shall immediately notify the consumer of this refusal and the information received. Such notification shall not be made if doing so would endanger public security or order. Section 37 shall remain unaffected.

Section 31

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

(1) For the purpose of deciding on the creation, execution or termination of a contractual relationship with a natural person, the use of a probability value for certain future action by this person (scoring) shall be permitted only if

1. the provisions of data protection law have been followed;

2. the data used to calculate the probability value are demonstrably essential for calculating the probability of the action on the basis of a scientifically recognized mathematic-statistical procedure;

3. other data in addition to address data are used to calculated the probability value; and

4. if address data are used, the data subject was notified ahead of time of the planned use of these data; this notification shall be documented.

(2) 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 in the case of including information on claims only as far as the conditions of subsection 1 are met and

only claims concerning a performance owed which has not been rendered on time are considered

1. which have been established by a final decision or a decision declared enforceable for the time being, or if an executory title has been issued under Section 794 of the Code of Civil Procedures,

2. which have been established under Section 178 of the Insolvency Act and have not been disputed by the debtor at the verification meeting,

3. which the debtor has explicitly acknowledged,

4. for which

   a) the debtor has received at least two written reminders after the due date of the claim,

   b) at least four weeks have elapsed since the first reminder,

   c) the debtor was previously informed, at least in the first reminder, of possible consideration by a credit reporting agency and

   d) the debtor has not disputed the claim, or

5. the contractual relationship on which the claim is based can be terminated without prior notice for payment in arrears and the debtor has been informed of possible consideration by a credit reporting agency.

The lawfulness of processing, including the calculation of probability values, other data relevant for credit reports pursuant to general data protection law shall remain unaffected.

Chapter 2

Rights of the data subject

Section 32

Information to be provided where personal data are collected from the data subject

(1) In addition to the exception in Article 13 (4) of Regulation (EU) 2016/679, the obligation to provide information to the data subject according to Article 13 (3) of Regulation (EU) 2016/679 shall not apply if providing information about the planned further use

1. concerns the further processing of data stored in analogue form, for which the controller directly contacts the data subject through the further processing; the purpose is compatible with the original purpose for which the data were collected in accordance with Regulation (EU) 2016/679; the communication with the data subject does not take place in digital form; and the interest of the data subject in receiving the information can be regarded as minimal, given the circumstances of the individual case, in particular with regard to the context in which the data were collected;

2. would, in the case of a public body, endanger the proper performance of tasks as referred to in Article 23 (1) (a) to (e) of Regulation (EU) 2016/679 for which the con-

troller is responsible, and the controller's interests in not providing the information outweigh the interests of the data subject;

3. would endanger public security or order or would otherwise be detrimental to the welfare of the Federation or a *Land*, and the controller's interests in not providing the information outweigh the interests of the data subject;

4. 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; or

5. would endanger a confidential transfer of data to public bodies.

(2) If information is not provided to the data subject pursuant to subsection 1, the controller shall take appropriate measures to protect the legitimate interests of the data subject, including providing the information referred to in Article 13 (1) and (2) of Regulation (EU) 2016/679 for the public in precise, transparent, understandable and easily accessible form in clear and simple language. The controller shall set down in writing the reasons for not providing information. The first and second sentences shall not apply in the cases of subsection 1 nos. 4 and 5.

(3) If notification is not provided in the cases of subsection 1 because of a temporary obstacle, the controller shall meet the obligation to provide information, while taking into account the specific circumstances of processing, within an appropriate period after the obstacle has ceased to exist, but no later than two weeks.

Section 33

Information to be provided where personal data have not been obtained from the data subject

(1) In addition to the exception in Article 14 (5) of Regulation (EU) 2016/679 and in Section 29 (1), first sentence, the obligation to provide information to the data subject according to Article 14 (1), (2) and (4) of Regulation (EU) 2016/679 shall not apply if providing information

1. in the case of a public body

   a) would endanger the proper performance of tasks as referred to in Article 23 (1) (a) to (e) of Regulation (EU) 2016/679 for which the controller is responsible, or

   b) would threaten the public security or order or otherwise be detrimental to the Federation or a *Land*,

and therefore the data subject's interest in receiving the information must not take precedence;

2. in the case of a private body

   a) would interfere with the establishment, exercise or defence of legal claims, or processing includes data from contracts under private law and is intended to prevent harm from criminal offences, unless the data subject has an overriding legitimate interest in receiving the information; or

   b) the responsible public body has determined with respect to the controller that disclosing the data would endanger public security or order or would otherwise be

detrimental to the welfare of the Federation or a *Land*; in the case of data processing for purposes of law enforcement, no determination pursuant to the first half-sentence shall be required.

(2) If information is not provided to the data subject pursuant to subsection 1, the controller shall take appropriate measures to protect the legitimate interests of the data subject, including providing the information referred to in Article 14 (1) and (2) of Regulation (EU) 2016/679 for the public in precise, transparent, understandable and easily accessible form in clear and simple language. The controller shall set down in writing the reasons for not providing information.

(3) If 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 and, as far as the security of the Federation is affected, other authorities of the Federal Ministry of Defence, such provision shall be permitted only with the approval of these bodies.

Section 34

Right of access by the data subject

(1) In addition to the exceptions in Section 27 (2), 28 (2) and 29 (1), second sentence, the data subject's right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if

1. the data subject shall not be informed pursuant to Section 33 (1) no. 1, no. 2 (b) or (3), or

2. the data

   a) were recorded only because they may not be erased due to legal or statutory provisions on retention, or

   b) only serve purposes of monitoring data protection or safeguarding data,

   and providing information would require a disproportionate effort, and appropriate technical and organizational measures make processing for other purposes impossible.

(2) The reasons for the refusal to provide information shall be documented. The data subject shall be informed of the reasons for refusing to provide information, unless providing the reasons in law and in fact on which the decision is based would undermine the intended purpose of refusing to provide the information. 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 Article 18 of Regulation (EU) 2016/679.

(3) If a public body of the Federation does not provide information to a data subject, such information shall be provided to the Federal Commissioner at the request of the data subject, unless the responsible supreme federal authority determines in the individual case that doing so would endanger the security of the Federation or a *Land*. The notification from the Federal Commissioner to the data subject with the results of the data protection assessment shall not permit any conclusions to be drawn concerning the information held by the controller unless the latter agrees to the provision of more extensive information.

(4) The data subject shall have the right to information about personal data processed by a public body neither in automated nor in non-automated form and stored in a filing system only if the data subject provides information enabling the data to be located and if the effort required is not disproportionate to the data subject's interest in the information.

Section 35

Right to erasure

(1) If in the case of non-automated data processing erasure 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 the controller shall not be obligated to erase personal data in accordance with Article 17 (1) of Regulation (EU) 2016/679 in addition to the exceptions given in Article 17 (3) of Regulation (EU) 2016/679. In this case, restriction of processing in accordance with Article 18 of Regulation (EU) 2016/679 shall apply in place of erasure. The first and second sentences shall not apply if the personal data were processed unlawfully.

(2) In addition to Article 18 (1) (b) and (c) of Regulation (EU) 2016/679, subsection 1, first and second sentences shall apply accordingly in the case of Article 17 (1) (a) and (d) of Regulation (EU) 2016/679 as long and as far as the controller has reason to believe that erasure would adversely affect legitimate interests of the data subject. The controller shall inform the data subject of the restriction of processing if doing so is not impossible or would not involve a disproportionate effort.

(3) In addition to Article 17 (3) (b) of Regulation (EU) 2016/679, subsection 1 shall apply accordingly in the case of Article 17 (1) (a) of Regulation (EU) 2016/679 if erasure would conflict with retention periods set by statute or contract.

Section 36

Right to object

The right to object according to Article 21 (1) of Regulation (EU) 2016/679 with regard to a public body shall not apply if there is an urgent public interest in the processing which outweighs the interests of the data subject or if processing is required by law.

Section 37

Automated individual decision-making, including profiling

(1) In addition to the exceptions given in Article 22 (2) (a) and (c) of Regulation (EU) 2016/679, the right according to Article 22 (1) of Regulation (EU) 2016/679 not to be subject to a decision based solely on automated processing shall not apply if the decision is made in the context of providing services pursuant to an insurance contract and

1. the request of the data subject was fulfilled, or

2. the decision is based on the application of binding rules of remuneration for therapeutic treatment and the controller takes suitable measures, in the event that the request is not granted in full, to safeguard the data subject's legitimate interests, at least the

right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision; the controller shall inform the data subject of these rights no later than the notification indicating that the data subject's request will not be granted in full.

(2) Decisions pursuant to subsection 1 may be based on the processing of health data as referred to in Article 4 no. 15 of Regulation (EU) 2016/679. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

Chapter 3

Obligations of controllers and processors

Section 38

Data protection officers of private bodies

(1) In addition to Article 37 (1) (b) and (c) of Regulation (EU) 2016/679, the controller and processor shall designate a data protection officer if they constantly employ as a rule at least ten persons dealing with the automated processing of personal data. If the controller or processor undertake processing subject to a data protection impact assessment pursuant to Article 35 of Regulation (EU) 2016/679, or if they commercially process personal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research, they shall designate a data protection officer regardless of the number of persons employed in processing.

(2) Section 6 (4), (5), second sentence, and (6) shall apply, Section 6 (4) however shall apply only if designating a data protection officer is mandatory.

Section 39

Accreditation

The power to act as a certification body in accordance with Article 43 (1), first sentence of Regulation (EU) 2016/679 shall be granted by the supervisory authority of the Federation or the *Länder* responsible for data protection supervision of the certification body on the basis of accreditation by the German accreditation body. Section 2 (3), second sentence, Section 4 (3) and Section 10 (1), first sentence, no. 3 of the Accreditation Body Act shall apply on the condition that data protection falls within the scope of Section 1 (2), second sentence.

Chapter 4

Supervisory authorities for data processing by private bodies

Section 40

Supervisory authorities of the *Länder*

(1) The authorities pursuant to *Land* law shall monitor the application by private bodies of data protection legislation within the scope of Regulation (EU) 2016/679.

(2) If the controller or processor has more than one establishment in Germany, Article 4 no. 16 of Regulation (EU) 2016/679 shall apply accordingly in determining which supervisory authority is competent. If more than one authority considers itself competent or not competent, or when the competence is unclear for other reasons, the supervisory authorities shall make a joint decision in accordance with Section 18 (2). Section 3 (3) and (4) of the Administrative Procedure Act shall apply accordingly.

(3) The supervisory authority may process the data it has stored only for purposes of supervision; to this end, it may transfer data to other supervisory authorities. Processing for another purpose shall be permitted in addition to Article 6 (4) of Regulation (EU) 2016/679 if

1. it is obviously in the interest of the data subject and there is no reason to assume that the data subject would refuse consent if he or she were aware of the other purpose;

2. processing is necessary to prevent substantial harm to the common good or a threat to public security or to safeguard substantial concerns of the common good; or

3. processing is necessary to prosecute crimes or administrative offences, to carry out or enforce punishment or measures as referred to in Section 11 (1) no. 8 of the Criminal Code or educational or disciplinary measures as referred to in the Juvenile Court Act or to enforce fines.

If the 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. Section 13 (4), fourth to seventh sentences shall apply accordingly.

(4) The bodies subject to monitoring and the persons responsible for their management shall provide a supervisory authority on request with the information necessary to perform their tasks. The person required to provide information may refuse to answer those questions which would expose him- or herself or a relative as referred to in Section 383 (1) nos. 1 to 3 of the Code of Civil Procedure to the risk of criminal prosecution or proceedings under the Administrative Offences Act. The person required to provide information shall be informed accordingly.

(5) 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. Section 16 (4) shall apply accordingly.

(6) 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 Article 38 (6) of Regulation (EU) 2016/679.

(7) The application of the Trade Regulation Code shall remain unaffected.

Chapter 5

Penalties

Section 41

Application of provisions concerning criminal proceedings and proceedings to impose administrative fines

(1) Unless this Act provides otherwise, the provisions of the Administrative Offences Act shall apply accordingly to violations pursuant to Article 83 (4) to (6) of Regulation (EU) 2016/679. Sections 17, 35 and 36 of the Administrative Offences Act shall not apply. Section 68 of the Administrative Offences Act shall apply on the condition that the regional court shall decide if the administrative fine exceeds the amount of one hundred thousand euros.

(2) Unless this Act provides otherwise, the provisions of the Administrative Offences Act and the general laws on criminal procedures, namely the Code of Criminal Procedure and the Judicature Act, shall apply accordingly in proceedings for violations pursuant to Article 83 (4) to (6) of Regulation (EU) 2016/679. Sections 56 to 58, 87, 88, 99 and 100 of the Administrative Offences Act shall not apply. Section 69 (4), second sentence of the Administrative Offences Act shall apply on the condition that the public prosecutor's office may stop the proceedings only with the approval of the supervisory authority which issued the administrative decision imposing a fine.

Section 42

Penal provisions

(1) The following actions done deliberately and without authorization with regard to the personal 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:

1. transferring the data to a third party or

2. otherwise making them accessible

for commercial purposes.

(2) The following actions done with regard to personal data which are not publicly accessible shall be punishable with imprisonment of up to two years or a fine:

1. processing without authorization, or

2. fraudulently acquiring

and doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

(3) Such offences shall be prosecuted only if a complaint is filed. The data subject, the controller, the Federal Commissioner and the supervisory authority shall be entitled to file complaints.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communication pursuant to Article 34 (1) of Regulation (EU) 2016/679 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.

Section 43

Provisions on administrative fines

(1) Intentionally or negligently engaging in the following shall be deemed an administrative offence:

1. in violation of Section 30 (1) failing to treat a request for information properly, or

2. in violation of Section 30 (2), first sentence, failing to inform a consumer or doing so incorrectly, incompletely or too late.

(2) An administrative offence may be punished by a fine of up to fifty thousand euros.

(3) Authorities and other public bodies as referred to in Section 2 (1) shall not be subject to any administrative fines.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communication pursuant to Article 34 (1) of Regulation (EU) 2016/679 may be used in proceedings pursuant to the Administrative Offences Act 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.

Chapter 6

Legal remedies

Section 44

Proceedings against a controller or processor

(1) Proceedings against a controller or a processor for a violation of data protection law within the scope of Regulation (EU) 2016/679 or the rights of the data subject contained therein may be brought by a data subject before the court in the place where the controller or processor has an establishment. Proceedings pursuant to the first sentence may also be brought before the court in the place where the data subject has his or her habitual residence.

(2) Subsection 1 shall not apply to proceedings against public authorities acting in the exercise of their sovereign powers.

(3) If the controller or processor has designated a representative pursuant to Article 27 (1) of Regulation (EU) 2016/679, this representative shall also be an authorized recipient in civil law proceedings pursuant to subsection 1. Section 184 of the Code of Civil Procedure shall remain unaffected.

Part 3

Implementing provisions for processing for purposes in accordance with Article 1 (1) of Directive (EU) 2016/680

Chapter 1

Scope, definitions and general principles for processing personal data

Section 45

Scope

The provisions of this Part shall apply to the processing of personal data by public bodies competent for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal or administrative penalties, as far as they process data for the purpose of carrying out these tasks. The public bodies shall be regarded in that case as controllers. The prevention of criminal offences as referred to in the first sentence shall include protection against and prevention of threats to public security. The first and second sentences shall also apply to those public bodies responsible for executing penalties, measures as referred to in Section 11 (1) no. 8 of the Criminal Code, educational or disciplinary measures as referred to in the Juvenile Court Act or fines. As far as this Part contains provisions for processors, it shall also apply to them.

Section 46

Definitions

For the purposes of this Act

1. ‘personal data’ means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

2. ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval,

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction;

3. ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

4. ‘profiling’ means any form of automated processing of personal data involving the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

5. ‘pseudonymization’ means the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data cannot be attributed to an identified or identifiable natural person;

6. ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

7. ‘controller’ means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;

8. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

9. ‘recipient’ means a natural or legal person, public authority, agency or other body to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or other law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

10. ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data processed;

11. ‘genetic data’ means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

12. ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, in particular facial images or dactyloscopic data;

13. ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

14. ‘special categories of personal data’

    a) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;

b) genetic data;

c) biometric data for the purpose of uniquely identifying a natural person;

d) data concerning health; and

e) data concerning a natural person's sex life or sexual orientation;

15. 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 41 of Directive (EU) 2016/680;

16. 'international organization' means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

17. 'consent' means any freely given, specific, informed and unambiguous indication of the data subject's wishes in a particular case by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Section 47

General principles for processing personal data

Personal data shall be

18. processed lawfully and fairly;

19. collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

20. adequate, relevant and not excessive in relation to the purposes for which they are processed;

21. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

22. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

23. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Chapter 2

Legal basis for processing personal data

Section 48

Processing of special categories of personal data

(1) The processing of special categories of personal data shall be allowed only where strictly necessary for the performance of the controller's tasks.

(2) If special categories of personal data are processed, appropriate safeguards for the legally protected interests of the data subject shall be implemented. Appropriate safeguards may be in particular

1. specific requirements for data security or data protection monitoring;
2. special time limits within which data must be reviewed for relevance and erasure;
3. measures to increase awareness of staff involved in processing operations;
4. restrictions on access to personal data within the controller;
5. separate processing of such data;
6. the pseudonymization of personal data;
7. the encryption of personal data; or
8. specific codes of conduct to ensure lawful processing in case of transfer or processing for other purposes.

Section 49

Processing for other purposes

Processing personal data for a purpose other than the one for which they were collected shall be permitted if the other purpose is one of the purposes listed in Section 45, the controller is authorized to process data for this purpose, and processing is necessary and proportionate to this purpose. Processing personal data for another purpose not listed in Section 45 shall be permitted if it is allowed by law.

Section 50

Processing for archiving, scientific and statistical purposes

Personal data may be processed in the context of purposes listed in Section 45 in archival, scientific or statistical form if doing so is in the public interest and appropriate safeguards for the legally protected interests of data subjects are implemented. Such safeguards may consist of rendering the personal data anonymous as quickly as possible, taking measures to prevent unauthorized disclosure to third parties, or in processing them organizationally and spatially separate from other tasks.

Section 51

Consent

(1) If personal data may be processed by law on the basis of consent, the controller must be able to present evidence of the data subject’s consent.

(2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

(3) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The data subject shall be informed of this before giving consent.

(4) Consent shall be effective only when based on the data subject’s free decision. When assessing whether consent was freely given, the circumstances in which it was given must be taken into account. The data subject shall be informed of the intended purpose of the processing. If necessary in the individual case or on request, the data subject shall also be informed of the consequences of withholding consent.

(5) If special categories of personal data are to be processed, the consent must explicitly refer to these data.

Section 52

Processing on instructions from the controller

Any person acting under the authority of the controller or of the processor who has access to personal data shall not process those data except on instructions from the controller, unless required to do so by law.

Section 53

Confidentiality

Persons employed in data processing shall not process personal data without authorization (confidentiality). They shall be obligated when taking up their duties to maintain confidentiality. The obligation of confidentiality shall continue after their employment ends.

Section 54

Automated individual decision

(1) A decision based solely on automated processing which produces an adverse legal effect concerning the data subject or significantly affects him or her shall be permitted only when authorized by law.

(2) Decisions referred to in subsection 1 shall not be based on special categories of personal data unless suitable measures to safeguard the data subject's legally protected and legitimate interests are in place.

(3) Profiling that results in discrimination against natural persons on the basis of special categories of personal data shall be prohibited.

Chapter 3

Rights of the data subject

Section 55

General information on data processing

The controller shall provide general and publicly accessible information on

1. the purposes of the processing,
2. the rights of data subjects with regard to the processing of their personal data to access, rectification, erasure and restriction of processing,
3. the names and contact details of the controller and the data protection officer,
4. the right to lodge a complaint with the Federal Commissioner, and
5. the contact details of the Federal Commissioner.

Section 56

Notification of data subjects

(1) If special legislation provides for or requires notifying data subjects of the processing of their personal data, especially in the case of undercover operations, such notification shall include at least the following information:

1. the information listed in Section 55;
2. the legal basis for the processing;
3. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
4. the categories of recipients of the personal data, if any;
5. where necessary, further information, in particular where the personal data were collected without the knowledge of the data subject.

(2) In the cases of subsection 1, the controller may postpone, limit or refrain from notification if and so long as

1. the performance of the tasks listed in Section 45,
2. public security, or
3. the legally protected interests of third parties

would otherwise be threatened, if the interest in avoiding these threats overrides the interest of the data subject in the information.

(3) If the notification relates to the transfer of personal data to the authorities for the protection of the Constitution, the Federal Intelligence Service, the Military Counterintelligence Service and, as far as the security of the Federation is affected, other authorities of the Federal Ministry of Defence, such notification shall be permitted only with the approval of these bodies.

(4) Section 57 (7) shall apply accordingly in case of restriction pursuant to subsection 2.

Section 57

Right of access

(1) The controller shall inform data subjects on request whether data concerning them are being processed. Data subjects shall also have the right to information about

1. the personal data being processed and the categories to which they belong;
2. the available information on the origin of the data;
3. the purposes of and legal basis for the processing;
4. the recipients or categories of recipients to whom the data have been disclosed, in particular recipients in third countries or international organizations;
5. the period for which the data will be stored, or if that is not possible, the criteria used to determine that period;
6. the existence of the right to rectification or erasure of data or restriction of processing of data by the controller;
7. the right pursuant to Section 60 to lodge a complaint with the Federal Commissioner, and
8. the contact details of the Federal Commissioner.

(2) Subsection 1 shall not apply to personal data recorded only because they may not be erased due to legal or statutory provisions on retention, or only for purposes of monitoring data protection or safeguarding data, if providing information would require a disproportionate effort, and appropriate technical and organizational measures make processing for other purposes impossible.

(3) No information shall be provided if the data subject does not provide information enabling the data to be located and if the effort required is therefore disproportionate to the data subject's interest in the information.

(4) Subject to the conditions of Section 56 (2), the controller may dispense with the provision of information pursuant to subsection 1, first sentence, or restrict, wholly or partly, the provision of information pursuant to subsection 1, second sentence.

(5) If the information to be provided relates to the transfer of personal data to the authorities for the protection of the Constitution, the Federal Intelligence Service, the Military Counterintelligence Service and, as far as the security of the Federation is affected, other authorities of the Federal Ministry of Defence, such provision shall be permitted only with the approval of these bodies.

(6) The controller shall notify the data subject, without delay, in writing of any refusal or restriction of access. This shall not apply if providing this information would entail a threat as referred to in Section 56 (2). The notification pursuant to the first sentence shall

include the reasons for the refusal or the restriction unless providing the reasons would undermine the intended purpose of the refusal or restriction of access.

(7) If the data subject is notified pursuant to subsection 6 of the refusal or restriction of access, he or she may exercise his or her right of access also via the Federal Commissioner. The controller shall inform the data subject of this possibility and that, in accordance with Section 60, the data subject may lodge a complaint with the Federal Commissioner or seek a judicial remedy. If the data subject exercises his or her right pursuant to the first sentence, the information shall be provided to the Federal Commissioner at the request of the data subject, unless the responsible supreme federal authority determines in the individual case that doing so would threaten the security of the Federation or a *Land*. The Federal Commissioner shall at least inform the data subject that all necessary checks have been conducted or that the Federal Commissioner has conducted a review. This notification may include information as to whether violations of data protection law were found. The notification from the Federal Commissioner to the data subject shall not permit any conclusions to be drawn concerning the information held by the controller unless the latter agrees to the provision of more extensive information. The controller may refuse to such provision only as far as and for as long as he or she could dispense with or restrict information pursuant to subsection 4. The Federal Commissioner shall also inform the data subject of his or her right to seek a judicial remedy.

(8) The controller shall document the factual or legal reasons on which the decision is based.

Section 58

Right to rectification and erasure and to restriction of processing

(1) The data subject shall have the right to obtain from the controller without delay the rectification of inaccurate data concerning him or her. In particular in the case of statements or assessments, the question of accuracy is not relevant for the content of the statement or assessment. If the accuracy or inaccuracy of the data cannot be ascertained, the controller shall restrict processing instead of erasing the data. In this case, the controller shall inform the data subject before lifting the restriction of processing. The data subject may also ask to have incomplete personal data completed, if doing so is appropriate when taking into account the purposes of processing.

(2) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without delay where processing such data is unlawful, knowledge of the data is no longer necessary for the performance of tasks, or the data must be erased to comply with a legal obligation.

(3) Instead of erasure, the controller may restrict processing where

1. there is reason to assume that erasure would adversely affect legitimate interests of the data subject,

2. the data must be retained for the purposes of evidence in proceedings serving the purposes of Section 45, or

3. erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage.

Data subject to restricted processing pursuant to the first sentence may be processed only for the purpose which prevented their erasure.

(4) In automated filing systems, technical measures shall ensure that the restriction of processing is clearly recognizable and processing for other purposes is not possible without further examination.

(5) If the controller has rectified inaccurate data, he or she shall communicate the rectification to the body from which he or she received the personal data. In cases of rectification, erasure or restriction of processing pursuant to subsections 1 to 3, the controller shall inform recipients to whom the data were transferred about these measures. The recipient shall rectify or erase the data or restrict their processing.

(6) The controller shall inform the data subject in writing of any refusal to rectify or erase personal data or restrict its processing. This shall not apply if providing this information would entail a threat as referred to in Section 56 (2). The information pursuant to the first sentence shall include the reasons for the refusal unless providing the reasons would undermine the intended purpose of the refusal.

(7) Section 57 (7) and (8) shall apply accordingly.

Section 59

Modalities for exercising the rights of the data subject

(1) The controller shall communicate with data subjects in a concise, intelligible and easily accessible form, using clear and plain language. Regardless of special formal requirements, when responding to requests, the controller shall provide the information in the same form as the request.

(2) When responding to requests, without prejudice to Section 57 (6) and Section 58 (6) the controller shall inform the data subject in writing about the follow-up to his or her request without delay.

(3) Information provided pursuant to Section 55, any communication made pursuant to Sections 56 and 66, and requests processed pursuant to Sections 57 and 58 shall be free of charge. Where a request pursuant to Sections 57 and 58 is manifestly unfounded or excessive, the controller may charge a reasonable fee based on its administrative costs, or may refuse to act on the request. In this case, the controller must be able to demonstrate the manifestly unfounded or excessive character of the request.

(4) Where the controller has reasonable doubts concerning the identity of a data subject making the request pursuant to Sections 57 or 58, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Section 60

Right to lodge a complaint with the Federal Commissioner

(1) Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with the Federal Commissioner, if the data subject believes that the processing by public bodies of personal data relating to him or her for the purposes listed in Section 45 infringes his or her rights. This shall not apply to the processing of personal data by courts, if they have processed these data in the context of their judicial activities. The Federal Commissioner shall inform the data subject of the progress and the outcome of the complaint and of the possibility of a judicial remedy pursuant to Section 61.

(2) If a complaint about processing is lodged with the Federal Commissioner instead of the competent supervisory authority in another Member State of the European Union, the Federal Commissioner shall transmit the complaint to the competent supervisory authority without delay. In this case, the Federal Commissioner shall inform the data subject about the transmission of his or her complaint and shall provide further support at the data subject's request.

Section 61

Legal remedies against decisions of the Federal Commissioner or if he or she fails to take action

(1) Without prejudice to any other legal remedy, every natural or legal person shall have the right to take legal action against a legally binding decision of the Federal Commissioner.

(2) Subsection 1 shall apply accordingly to data subjects if the Federal Commissioner does not handle a complaint pursuant to Section 60 or does not inform the data subject within three months of the progress or outcome of the complaint.

Chapter 4

Obligations of controllers and processors

Section 62

Processing carried out on behalf of a controller

(1) Where personal data are processed by other persons or bodies on behalf of a controller, the controller shall ensure compliance with the provisions of this Act and other data protection provisions. The data subject shall assert his or her rights to access, rectification, erasure, restriction of processing and the right to receive compensation against the controller.

(2) A controller may use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the law and ensure the protection of the rights of the data subjects.

(3) Processors shall not engage other processors without prior written authorization by the controller. If the controller has given the processor general authorization to engage other processors, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors. In this case, the controller may object to such changes.

(4) Where a processor engages another processor, the former shall impose on the latter the same data protection obligations as set out in the contract between the controller and the processor as referred to in subsection 5 if these obligations are not already binding for the latter processor because of other legislation. Where that other processor fails to fulfil these obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

(5) Processing by a processor shall be governed by a contract or other legal instrument that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal instrument shall stipulate, in particular, that the processor

1. acts only on instructions from the controller; if the processor believes that an instruction is unlawful, the processor shall inform the controller without delay;

2. ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

3. assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;

4. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless law requires storage of the personal data;

5. makes available to the controller all information necessary, in particular the logs kept in accordance with Section 76, to demonstrate compliance with these obligations;

6. allows for and contributes to audits conducted by the controller or another auditor mandated by the controller;

7. complies with the conditions referred to in subsections 3 and 4 for engaging another processor;

8. takes all measures required pursuant to Section 64; and

9. assists the controller in ensuring compliance with the obligations pursuant to Sections 64 to 67 and 69 taking into account the nature of processing and the information available to the processor.

(6) The contract referred to in subsection 5 shall be in writing or in an electronic form.

(7) A processor that determines, in violation of this provision, the purposes and means of processing, shall be considered a controller in respect of that processing.

Section 63

Joint controllers

Where two or more controllers jointly determine the purposes and means of processing, they shall be considered joint controllers. Joint controllers shall determine their respective tasks and responsibilities under data protection law in a transparent manner in an agreement, unless these tasks and responsibilities are already determined by law. In particular, this agreement must indicate which of them must meet which information obligations, and how and with respect to whom data subjects may exercise their rights. Such an agreement shall not prevent data subjects from asserting their rights against each of the joint controllers.

Section 64

Requirements for the security of data processing

(1) The controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the legally protected interests of natural persons, shall implement the necessary technical and organizational measures to ensure a level of security appropriate to the risk when processing personal data, in particular as regards the processing of special categories of personal data. In doing so, the controller shall take into account the relevant Technical Guidelines and recommendations from the Federal Office for Information Security.

(2) The measures referred to in subsection 1 may include pseudonymization and encryption of personal data, if such means are possible in view of the purposes of processing. The measures pursuant to subsection 1 should ensure

1. the ongoing confidentiality, integrity, availability and resilience of processing systems and services in connection with processing; and

2. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

(3) In respect of automated processing, the controller and processor, following an evaluation of the risks, shall implement measures designed to

1. deny unauthorized persons access to processing equipment used for processing (‘equipment access control’);

2. prevent the unauthorized reading, copying, modification or erasure of data media (‘data media control’);

3. prevent the unauthorized input of personal data and the unauthorized inspection, modification or deletion of stored personal data (‘storage control’);

4. prevent the use of automated processing systems by unauthorized persons using data communication equipment (‘user control’);

5. ensure that persons authorized to use an automated processing system have access only to the personal data covered by their access authorization (‘data access control’);

6. ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment (‘communication control’);

7. ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input (‘input control’);

8. ensure that the confidentiality and integrity of personal data are protected during transfers of personal data or during transport of data media (‘transport control’);

9. ensure that installed systems may, in the case of interruption, be restored (‘recovery’);

10. ensure that all system functions perform and that the appearance of faults in the functions is reported (‘reliability’);

11. ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system (‘integrity’);

12. ensure that personal data processed on behalf of the controller can only be processed in compliance with the controller’s instructions (‘processing control’);

13. ensure that personal data are protected against loss and destruction (‘availability control’);

14. ensure that personal data collected for different purposes can be processed separately (‘separability’).

A purpose pursuant to the first sentence, nos. 2 to 5 may be achieved in particular by using state-of-the-art encryption.

Section 65

Notifying the Federal Commissioner of a personal data breach

(1) In the case of a personal data breach, the controller shall notify the Federal Commissioner without delay and, if possible, not later than 72 hours after having become aware of it, of the personal data breach, unless the personal data breach is unlikely to result in a risk to the legally protected interests of natural persons. If the Federal Commissioner is not notified within 72 hours, the notification shall be accompanied by reasons for the delay.

(2) A processor shall notify the controller of a personal data breach without delay.

(3) The notification referred to in subsection 1 shall include at least the following information:

1. a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2. the name and contact details of the data protection officer or other contact point where more information can be obtained;

3. a description of the likely consequences of the personal data breach; and

4. a description of the measures taken or proposed by the controller to address the personal data breach, including measures to mitigate its possible adverse effects.

(4) If it is not possible to provide the information pursuant to subsection 3 with the notification, the controller shall provide this information as soon as it is available.

(5) The controller shall document any personal data breaches. This documentation shall include all the facts relating to the personal data breach, its effects and the remedial action taken.

(6) If the personal data breach involves personal data that have been transmitted by or to a controller in another Member State of the European Union, the information referred to in subsection 3 shall be communicated to the controller in that Member State without delay.

(7) Section 42 (4) shall apply accordingly.

(8) Additional obligations of the controller regarding notifications of personal data breaches shall remain unaffected.

Section 66

Notifying data subjects affected by a personal data breach

(1) If a personal data breach is likely to result in a substantial risk to the legally protected interests of natural persons, the controller shall notify the data subject of the personal data breach without delay.

(2) The notification of the data subject pursuant to subsection 1 shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in Section 65 (3) nos. 2 to 4.

(3) Notification shall not be required if any of the following conditions are met:

1. the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access them, such as encryption;

2. the controller has taken subsequent measures which ensure that the substantial risk referred to in subsection 1 is no longer likely to exist;

3. it would involve a disproportionate effort; in this case, a public communication shall be made or a similar measure taken to inform the data subjects in an equally effective manner.

(4) If the controller has not informed the data subjects of a personal data breach, the Federal Commissioner may formally determine that, in his or her opinion, the conditions referred to in subsection 3 have not been met. In doing so, the Federal Commissioner shall consider the likelihood of the personal data breach resulting in a high risk as referred to in subsection 1.

(5) The notification of data subjects pursuant to subsection 1 may be delayed, restricted or omitted under the conditions referred to in Section 56 (2) unless the interests of the data subjects outweigh those of the controller owing to the high risk resulting from the personal data breach as referred to in subsection 1.

(6) Section 42 (4) shall apply accordingly.

Section 67

Conducting a data protection impact assessment

(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a substantial risk to the legally protected interests of data subjects, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the data subjects.

(2) A joint assessment may address a set of similar processing operations that present similar substantial risks.

(3) The controller shall involve the Federal Commissioner in carrying out the impact assessment.

(4) The impact assessment shall take the rights of the data subjects affected by the processing into account and shall contain at least the following:

1. a systematic description of the envisaged processing operations and the purposes of the processing;

2. an assessment of the necessity and proportionality of the processing operations in relation to their purposes;

3. an assessment of the risks to the legally protected interests of the data subjects; and

4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the law.

(5) Where necessary, the controller shall carry out a review to assess whether processing is performed in accordance with the data protection impact assessment.

Section 68

Cooperation with the Federal Commissioner

The controller shall cooperate with the Federal Commissioner in carrying out the latter's tasks.

Section 69

Prior consultation of the Federal Commissioner

(1) The controller shall consult the supervisory authority prior to processing which will form part of a new filing system if

1. a data protection impact assessment pursuant to Section 67 indicates that the processing would result in a substantial risk to the legally protected interests of data subjects in the absence of measures taken by the controller to mitigate the risk; or

2. the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a substantial risk to the legally protected interests of data subjects.

The Federal Commissioner may draw up a list of the processing operations which are subject to prior consultation pursuant to the first sentence.

(2) In the case of subsection 1, the Federal Commissioner shall be presented with

1. the data protection impact assessment carried out pursuant to Section 67;

2. where applicable, information on the respective responsibilities of the controller, joint controllers and processors involved in the processing;

3. information on the purposes and means of the envisaged processing;

4. information on the measures and safeguards intended to protect the legally protected interests of the data subjects; and

5. the name and contact details of the data protection officer.

On request, the Federal Commissioner shall be given any other information he or she requires to assess the lawfulness of the processing and, in particular, the existing risks to the protection of the data subjects' personal data and the related safeguards.

(3) If the Federal Commissioner believes that the planned processing would violate the law, in particular because the controller has not sufficiently identified the risk or has not taken sufficient measures to mitigate the risk, he or she may provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller and, where applicable, to the processor, as to which additional measures should be taken. The Federal Commissioner may extend this period by a month, if the planned processing is especially complex. In this case, the Federal Commissioner shall inform the controller and, where applicable, the processor of the extension within one month of receipt of the request for consultation.

(4) If the envisaged processing has substantial significance for the controller's performance of tasks and is therefore especially urgent, the controller may initiate processing after the consultation has started but before the period referred to in subsection 3, first sentence, has expired. In this case, the recommendations of the Federal Commissioner shall be taken into account after the fact, and the way the processing is carried out shall be adjusted where applicable.

Section 70

Records of processing activities

(1) The controller shall keep a record of all categories of processing activities under its responsibility. This record shall contain all of the following information:

1. the name and contact details of the controller and, where applicable, of the joint controller; and the name and contact details of the data protection officer;

2. the purposes of the processing;

3. the categories of recipients to whom the personal data have been or are to be disclosed;

4. a description of the categories of data subjects and of the categories of personal data;

5. where applicable, the use of profiling;

6. where applicable, the categories of transfers of personal data to bodies in a third country or to an international organization;

7. information about the legal basis for the processing;

8. the envisaged time limits for the erasure or for a review of the need to store the various categories of personal data; and

9. a general description of the technical and organizational security measures referred to in Section 64.

(2) The processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing

1. the name and contact details of the processor, of each controller on behalf of which the processor is acting and, where applicable, the data protection officer;

2. where applicable, transfers of personal data to bodies in a third country or to an international organization, including the identification of that third country or international organization; and

3. a general description of the technical and organizational security measures according to Section 64.

(3) The records referred to in subsections 1 and 2 shall be in writing or in electronic form.

(4) Controllers and processors shall make these records available to the Federal Commissioner on request.

Section 71

Data protection by design and by default

(1) The controller, both at the time the means of processing are determined and at the time of the processing itself, shall take appropriate measures to implement data protection principles, such as data minimization, in an effective manner, to ensure compliance with legal requirements and to protect the rights of data subjects. In doing so, the controller shall take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the legally protected interests of the data subject posed by the processing. In particular, personal data shall be processed, and processing systems shall be selected and designed in accordance with the aim of processing as few personal data as possible. Personal data shall be rendered anonymous or pseudonymized as early as possible, as far as possible in accordance with the purpose of processing.

(2) The controller shall implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That applies to the amount of data collected, the extent of their processing, the period of their storage and their accessibility. In particular, the measures must ensure that by default the data are not made accessible by automated means to an indefinite number of persons.

Section 72

Distinction between different categories of data subjects

When processing personal data, the controller shall, as far as possible, make a clear distinction between different categories of data subjects. This applies in particular to the following categories:

1. persons with regard to whom there are serious grounds for believing that they have committed a criminal offence;

2. persons with regard to whom there are serious grounds for believing that they are about to commit a criminal offence;

3. persons convicted of a criminal offence;

4. victims of a criminal offence or persons with regard to whom certain facts indicate that they could be the victim of a criminal offence; and

5. other persons, such as witnesses, persons who can provide information, or contacts or associates of the persons referred to in nos. 1 to 4.

Section 73

Distinction between facts and personal assessments

In processing, the controller shall distinguish, as far as possible, personal data based on facts from personal data based on personal assessments. To this end, the controller shall identify evaluations based on personal assessments as such, as far as possible and reasonable in the context of the processing in question. It must also be possible to determine which body keeps the records on which an evaluation based on a personal assessment is based.

Section 74

Procedures for data transfers

(1) The controller shall take appropriate measures to ensure that personal data which are inaccurate or no longer up to date are not transmitted or otherwise made available. To that end, the controller shall, as far as possible with reasonable effort, verify the quality of the data before they are transmitted or made available. The controller shall also, as far as possible and reasonable, in all transmissions of personal data include the necessary information to enable the recipient to assess the degree of accuracy, completeness and reliability of the data, and the extent to which they are up to date.

(2) If the processing of personal data is subject to special conditions, in transmissions of data the transmitting body shall inform the recipient of these conditions and the requirement to respect them. The obligation of providing information may be met by marking the data accordingly.

(3) The transmitting body shall not apply conditions to recipients in other Member States of the European Union or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the Third Part of the Treaty on the Functioning of the European Union other than those applicable to similar domestic transmissions.

Section 75

Rectification and erasure of personal data and restriction of processing

(1) The controller shall rectify inaccurate personal data.

(2) The controller shall erase personal data without delay if their processing is unlawful, they must be erased to comply with a legal obligation, or knowledge of the data is no longer necessary for the controller to perform its tasks.

(3) Section 58 (3) to (5) shall apply accordingly. The recipient shall also be informed if inaccurate personal data have been transmitted, or if personal data have been transmitted unlawfully.

(4) Without prejudice to any time limits for storing or erasing data defined in law, the controller shall provide for appropriate time limits for the erasure of personal data or for a periodic review of the need for the storage of personal data and shall take procedural measures to ensure that these time limits are observed.

Section 76

Logging

(1) Controllers and processors shall provide for logs to be kept for at least the following processing operations in automated processing systems:

1. collection,

2. alteration,

3. consultation,

4. disclosure including transfers,

5. combination, and

6. erasure.

(2) The logs of consultation and disclosure must make it possible to ascertain the justification, date and time of such operations and, as far as possible, the identity of the person who consulted or disclosed personal data, and the identity of the recipients of the data.

(3) The logs may be used only by the data protection officer, the Federal Commissioner or the data subject to verify the lawfulness of the processing; and for self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

(4) The log data shall be erased at the end of the year following the year in which they were generated.

(5) The controller and the processor shall make the logs available to the Federal Commissioner on request.

Section 77

Confidential reporting of violations

The controller shall ensure that it is able to receive confidential reports of violations of data protection law which have occurred in its area of responsibility.

Chapter 5

Transfers of data to third countries and to international organizations

Section 78

General requirements

(1) If all other conditions applicable to data transfers are met, the transfer of personal data to bodies in third countries or to international organizations shall be permitted if

1. the body or international organization is responsible for the purposes referred to in Section 45, and

2. the European Commission has adopted an adequacy decision pursuant to Article 36 (3) of Directive (EU) 2016/680.

(2) No transfer of personal data shall be permitted, despite an adequacy decision as referred to in subsection 1 no. 2 and the public interest in the data transfer to be taken into account, if in the individual case it cannot be ensured that the data will be handled appropriately in terms of data protection law and in accordance with fundamental human rights in the area of responsibility of the recipient, or if a transfer would conflict with other overriding legitimate interests of a data subject. The controller shall base its assessment on whether the recipient in the individual case guarantees appropriate protection of the transferred data.

(3) If personal data which have been transmitted or made available from another European Union Member State are to be transferred pursuant to subsection 1, the competent body of the other Member State must provide prior authorization of the transfer. Transfers without the prior authorization shall be permitted only if the transfer is necessary to prevent an immediate and serious threat to the public security of a country or to essential interests of a Member State and the prior authorization cannot be obtained in time. In the case of the second sentence, the other Member State's body responsible for giving prior authorization shall be informed of the transfer without delay.

(4) The controller transferring data pursuant to subsection 1 shall take appropriate measures to ensure that the recipient will transfer the data onward to other third countries or other international organizations only with the prior authorization of the controller. When deciding whether to authorize the transfer, the controller shall take into account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data were originally transferred and the level of personal data protection in the third country or international organization to which the data are to be transferred onward. The transfer shall be authorized only if a direct transfer to the other third country or international organization would be lawful. The responsibility for issuing authorization may also be otherwise provided for.

Section 79

Data transfers with appropriate safeguards

(1) In the absence of a decision pursuant to Article 36 (3) of Directive (EU) 2016/680, transfers which meet the remaining requirements of Section 78 shall be permitted also if

1. appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

2. the controller has assessed all the circumstances surrounding the transfer and concludes that appropriate safeguards exist for the protection of personal data.

(2) The controller shall document transfers pursuant to subsection 1 no. 2. The documentation shall include the date and time of the transfer, the identity of the recipient, the reason for the transfer and the personal data transferred. It shall be provided to the Federal Commissioner on request.

(3) The controller shall file a report to the Federal Commissioner at least once a year covering transfers conducted on the basis of an assessment pursuant to subsection 1 no. 2. In this report, the controller may categorize the recipients and the purpose of the transfers appropriately.

Section 80

Data transfers without appropriate safeguards

(1) If in derogation from Section 78 (1) no. 2, no decision pursuant to Article 36 (3) of Directive (EU) 2016/680 or appropriate safeguards as referred to in Section 79 (1) exist, transfers which meet the remaining requirements of Section 78 shall be permitted also if they are necessary

1. to protect the vital interests of a natural person;

2. to safeguard legitimate interests of the data subject;

3. to prevent an immediate and serious threat to the public security of a country;

4. in individual cases for the purposes referred to in Section 45; or

5. in an individual case for the establishment, exercise or defence of legal claims relating to the purposes referred to in Section 45.

(2) The controller shall not transfer data pursuant to subsection 1 if the fundamental rights of the data subject override the public interest in the transfer.

(3) Section 79 (2) shall apply accordingly to transfers pursuant to subsection 1.

Section 81

Other data transfers to recipients in third countries

(1) In special individual cases and if all other requirements for data transfers to third countries are met, controllers may transfer personal data directly to recipients in third countries not referred to in Section 78 (1) no. 1 if the transfer is strictly necessary for the performance of their tasks and

1. in the specific case no fundamental rights of the data subject override the public interest in the transfer;

2. transfer to the bodies referred to in Section 78 (1) no. 1 would be ineffective or inappropriate, in particular because the transfer cannot be carried out in time; and

3. the controller informs the recipient of the purposes of processing and instructs the recipient that the transferred data may be processed only to the extent necessary for these purposes.

(2) In the case of subsection 1, the controller shall inform the bodies referred to in Section 78 (1) no. 1 of the transfer without delay, unless this is ineffective or inappropriate.

(3) Section 79 (2) and (3) shall apply accordingly to transfers pursuant to subsection 1.

(4) In the case of transfers pursuant to subsection 1, the transmitting controller shall obligate the recipient to process the transferred personal data without the controller's consent only for the purpose for which they were transferred.

(5) Agreements in the field of judicial cooperation in criminal matters and police cooperation shall remain unaffected.

Chapter 6

Cooperation among supervisory authorities

Section 82

Mutual assistance

(1) The Federal Commissioner shall provide the supervisory authorities in other European Union Member States with information and mutual assistance as far as necessary to implement and apply Directive (EU) 2016/680 in a consistent manner. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out consultations, inspections and investigations.

(2) The Federal Commissioner shall take all appropriate measures required to reply to a request for mutual assistance without delay and no later than one month after receiving the request.

(3) The Federal Commissioner may refuse to comply with the request only if

1. he or she is not competent for the subject matter of the request or for the measures he or she is asked to execute; or

2. compliance with the request would violate the law.

(4) The Federal Commissioner shall inform the other state's requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in response to the request. In the case of subsection 3, he or she shall provide reasons for refusing to comply with the request.

(5) The Federal Commissioner shall, as a rule, supply the information requested by the other state's supervisory authority by electronic means and using a standardized format.

(6) The Federal Commissioner shall not charge a fee for action taken pursuant to a request for mutual assistance unless he or she has agreed with the other state's supervisory authority in the individual case on the reimbursement of expenses incurred.

(7) The Federal Commissioner's requests for assistance shall contain all the necessary information, including in particular the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

Chapter 7

Liability and penalties

Section 83

Compensation

(1) If a controller has caused a data subject to suffer damage by processing personal data in violation of this Act or other law applicable to this processing, the controller or its legal entity shall be obligated to provide compensation to the data subject. This obligation to provide compensation shall not apply if, in the case of non-automated processing, the damage was not the result of fault by the controller.

(2) The data subject may request appropriate financial compensation for non-material damage.

(3) If, in the case of automated processing of personal data, it is not possible to determine which of several controllers caused the damage, each controller or its legal entity shall be liable.

(4) Section 254 of the Civil Code shall apply to contributory negligence on the part of the data subject.

(5) The limitation provisions stipulated for tortious acts in the Civil Code shall apply accordingly with regard to statutory limitation.

Section 84

Penal provisions

Section 42 shall apply accordingly to the processing of personal data by public bodies in the context of activities pursuant to Section 45, first, third or fourth sentences.

Part 4

Special provisions for processing in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680

Section 85

Processing of personal data in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680

(1) The transfer of personal data to a third country, to supranational or intergovernmental bodies or to international organizations in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 shall be permitted in addition to the cases permitted under Regulation (EU) 2016/679 also if the processing is necessary to perform tasks for urgent reasons of defence or to fulfil supra- or intergovernmental obligations of a public body of the Federation in the field of crisis management or conflict prevention or for humanitarian measures. The recipient shall be instructed that the transferred data may be used only for the purpose for which they were transferred.

(2) Section 16 (4) shall not apply to processing in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 by workplaces within the remit of the Federal Ministry of Defence if the Federal Ministry of Defence determines in the individual case that meeting the obligations referred to in that provision would endanger the security of the Federation.

(3) Processing by public bodies of the Federation in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 shall not be subject to the obligation to provide information in accordance with Article 13 (1) and (2) of Regulation (EU) 2016/679

1. in the cases referred to in Section 32 (1) nos. 1 to 3, or

2. if meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of legitimate interests of a third party which outweigh the interests of the data subject in obtaining the information.

If the data subject is not to be informed in the cases of the first sentence, no right of access shall apply. Sections 32 (2) and 33 (2) shall not apply.

Article 2

Amendment of the Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution

The Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution of 20 December 1990 (*Bundesverfassungsschutzgesetz*,

BVerfSchG) (Federal Law Gazette I p. 2954, 2970), last amended by Article 2 (1) of the Act of 16 June 2017 (Federal Gazette I, p. 1634), shall be amended as follows:

[…]

Article 3

Amendment of the Military Counterintelligence Service Act

The Military Counterintelligence Service Act of 20 December 1990 (*Gesetz über den Militärischen Abschirmdienst*, MADG) (Federal Gazette I, p. 2954, 2977), last amended by Article 6 of the Act of 27 March 2017 (Federal Gazette I, p. 562), shall be amended as follows:

[…]

Article 4

Amendment of the Federal Intelligence Service Act

The Federal Intelligence Service Act of 20 December 1990 (*BND-Gesetz*, BNDG) (Federal Law Gazette I p. 2954, 2979), last amended by Article 3 of the Act of 10 March 2017 (Federal Gazette I, p. 410), shall be amended as follows:

[…]

Article 5

Amendment of the Act on Prerequisites and Procedures for Security Clearance Checks Undertaken by the Federal Government

The Act on Prerequisites and Procedures for Security Clearance Checks Undertaken by the Federal Government 20 April 1994 (*Sicherheitsüberprüfungsgesetz*, SÜG) (Federal Law Gazette I p. 867), last amended by Article 1 of the Act of 16 June 2017 (Federal Gazette I, p. 1634), shall be amended as follows:

[…]

Article 6

Amendment of the Act to restrict the Privacy of Correspondence, Posts and Telecommunications

The Act to restrict the Privacy of Correspondence, Posts and Telecommunications of 26 June 2001 (*Artikel 10-Gesetz*, G 10) (Federal Law Gazette I, p. 1254, 2298; 2017 I,

p. 154), last amended by Article 2 (2) of the Act of 16 June 2017 (Federal Gazette I, p. 1634), shall be amended as follows:

Article 7

Amendment of the Federal Data Protection Act

The Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) in the version published on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of 28 April 2017 (Federal Law Gazette I, p. 968), shall be amended as follows:

3. In the table of contents, the following text shall be inserted after the reference to Section 42a:

"Section 42b Application of the supervisory authority for a court decision if it believes that a decision by the Commission violates European law"

4. The following subsection 5a shall be added after Section 22 (5):

"(5a) The Federal Commissioner may delegate human resources administration and management tasks to other federal bodies as long as doing so does not affect the Federal Commissioner's independence. Personal data of staff members may be transferred to these bodies as needed for them to perform their delegated tasks."

5. The following Section 42b shall be added after Section 42a:

"Section 42b

Application of the supervisory authority for a court decision if it believes that a decision by the European Commission violates the law

(1) If a supervisory authority believes that an adequacy decision of the European Commission or a decision on the recognition of standard protection clauses or on the general validity of approved codes of conduct, on the validity of which a decision of the supervisory authority depends, violates the law, the supervisory authority shall suspend its procedure and lodge an application for a court decision.

(2) Recourse to the administrative courts shall be provided for proceedings pursuant to subsection 1. The Code of Administrative Court Procedure shall be applied in compliance with subsections 3 to 6.

(3) The Federal Administrative Court shall decide in the first and last instance on an application by the supervisory authority pursuant to subsection 1.

(4) In proceedings pursuant to subsection 1, the supervisory authority shall be competent to take part. The supervisory authority shall be a party to proceedings pursuant to subsection 1 as applicant; Section 63 nos. 3 and 4 of the Code of Administrative Court Procedure shall remain unaffected. The Federal Administrative Court may give the European Commission the opportunity to comment within a period of time to be determined.

(5) If a proceeding to review the validity of a European Commission decision pursuant to subsection 1 is pending at the European Court of Justice, the Federal Administrative Court may order its proceeding to be suspended until the proceeding at the European Court of Justice has been concluded.

(6) In proceedings pursuant to subsection 1, Section 47 (5), first sentence and (6) of the Code of Administrative Court Procedure shall apply accordingly. If the Federal Administrative Court finds that the European Commission's decision pursuant to subsection 1 is valid, it shall state this in its decision. Otherwise it shall refer the question as to the validity of the decision in accordance with Article 267 of the Treaty on the Functioning of the European Union to the European Court of Justice."

Article 8

Entry into force and expiry

(1) This Act shall enter into force on 25 May 2018, subject to subsection 2. The Federal Data Protection Act in the version published on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 7 of this Act shall expire at the same time.

(2) Article 7 shall enter into force on the day following its promulgation.