Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG)

StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.)
[CELEX-Nr.: 395L0046]

Änderung

BGBl. I Nr. 136/2001 (NR: GP XXI RV 742 AB 824 S. 81. BR: 6458 AB 6459 S. 681.)
BGBl. I Nr. 13/2005 (NR: GP XXII IA 515/A AB 821 S. 96. BR: AB 7228 S. 719.)
BGBl. I Nr. 2/2008 (1. BVRBG) (NR: GP XXIII RV 314 AB 370 S. 41. BR: 7799 AB 7830 S. 751.)
BGBl. I Nr. 133/2009 (NR: GP XXIV RV 472 AB 531 S. 49. BR: 8220 AB 8225 S. 780.)
BGBl. I Nr. 135/2009 (NR: GP XXIV RV 485 AB 558 S. 49. BR: 8217 AB 8228 S. 780.)
BGBl. I Nr. 112/2011 (NR: GP XXIV RV 1494 AB 1500 S. 130. BR: 8602 AB 8603 S. 802.) [CELEX-Nr.: 32009L0133, 32010L0024]
BGBl. I Nr. 51/2012 (NR: GP XXIV RV 1618 AB 1771 S. 155. BR: 8730 AB 8731 S. 809.)
BGBl. I Nr. 57/2013 (NR: GP XXIV RV 2131 AB 2245 S. 194. BR: AB 8940 S. 819.)
BGBl. I Nr. 83/2013 (NR: GP XXIV RV 2168 AB 2268 S. 200. BR: AB 8968 S. 820.) [CELEX-Nr.: 31995L0046]
BGBl. I Nr. 132/2015 (VfGH)
BGBl. I Nr. 120/2017 (NR: GP XXV RV 1664 AB 1761 S. 190. BR: 9824 AB 9856 S. 871.) [CELEX-Nr.: 32016L0680]

BGBl. I Nr. 23/2018 (NR: GP XXVI IA 188/A AB 99 S. 21. BR: AB 9958 S. 879.)
BGBl. I Nr. 24/2018 (NR: GP XXVI IA 189/A AB 98 S. 21. BR: AB 9948 S. 879.)

Federal Act concerning the Protection of Personal Data (DSG)

⇐ Original version

as amended by:
(list of amendments published in the Federal Law Gazette [F. L. G. = BGBl.])

⇐ amendment entailing the latest update of the present translation
(the German version is updated to reflect also recent amendments; interim changes are highlighted as ~~deletions~~ and respectively)

Click here for checking the up-to-date list of amendments in the Austrian Legal Information System.

Inhaltsverzeichnis

Table of contents

Artikel 1
(Verfassungsbestimmung)

Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

(Anm.: Abs. 5 aufgehoben durch BGBl. I Nr. 51/2012)

Zuständigkeit

§ 2. (1) Bundessache ist die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr.

(2) Die Vollziehung solcher Bundesgesetze steht dem Bund zu. Soweit solche Daten von einem Land, im Auftrag eines Landes, von oder im Auftrag von juristischen Personen, die durch Gesetz eingerichtet sind und deren Einrichtung hinsichtlich der Vollziehung in die Zuständigkeit der Länder fällt, verwendet werden, sind diese Bundesgesetze von den Ländern zu vollziehen, soweit nicht durch Bundesgesetz die Datenschutzbehörde, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden.

Räumlicher Anwendungsbereich

Article 1
(Constitutional provision)

Fundamental right to data protection

§ 1. (1) Every person shall have the right to secrecy of the personal data concerning that person, especially with regard to the respect for his or her private and family life, insofar as that person has an interest which deserves such protection. Such an interest is precluded if data cannot be subject to the right to secrecy due to the data's general availability or because they cannot be traced back to the data subject.

(2) Insofar as personal data are not used in the vital interest of the data subject or with the data subject's consent, restrictions of the right to secrecy are permitted only to safeguard overriding legitimate interests of another person, namely in the case of interference by a public authority only on the basis of laws which are necessary for the reasons stated in Article 8 para. 2 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Federal Law Gazette No 210/1958. Such laws may provide for the use of data that, due to their nature, deserve special protection only in order to safeguard substantial public interests and, at the same time, shall provide for adequate safeguards for the protection of the data subjects' interests in confidentiality. Even in the case of permitted restrictions, a fundamental right may only be interfered with using the least intrusive of all effective methods.

(3) Insofar as personal data concerning a person are intended for automated processing or processing in files managed manually, i.e. files managed without automated processing, every person shall, as provided for by law, have

1. the right to obtain information as to who processes what data concerning the person, where the data originated from, for which purpose they are used, and in particular to whom the data are transmitted;
2. the right to rectification of incorrect data and the right to erasure of illegally processed data.

(4) Restrictions of the rights according to para. 3 are only permitted under the conditions laid out in para. 2.

(Note: para. 5 repealed by Federal Law Gazette I No 51/2012)

Legislative power and enforcement

§ 2. (1) The Federal Government shall have the power to pass laws concerning the protection of personal data that are automatically processed.

(2) The Federal Government shall have the power to execute such federal laws. Insofar as such data are used by a province, on behalf of a province, by or on behalf of legal persons established by law and whose establishment falls within the powers of the provinces regarding execution, these federal laws shall be executed by the provinces unless their execution has been entrusted to the Data Protection Authority, the Data Protection Council or the courts by federal law.

Territorial scope

§ 3. (1) Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von personenbezogenen Daten im Inland anzuwenden. Darüber hinaus ist dieses Bundesgesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung (§ 4 Z 15) eines Auftraggebers (§ 4 Z 4) geschieht.

(2) Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.

(3) Weiters ist dieses Bundesgesetz nicht anzuwenden, soweit personenbezogene Daten durch das Inland nur durchgeführt werden.

(4) Von den Abs. 1 bis 3 abweichende gesetzliche Regelungen sind nur in Angelegenheiten zulässig, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

§ 3. (1) The provisions of this federal law shall be applied to the use of personal data in Austria. This federal law shall also be applied to the use of data outside of Austria, insofar as the data are used in other Member States of the European Union for purposes of a controller's (§ 4 subpara. 4) main establishment or branch establishment (§ 4 subpara. 15) in Austria.

(2) By derogation from para. 1, the law of the state where the controller has its seat shall apply to data processing operations in Austria if a private-sector controller (§ 5 para. 3) whose seat is in another Member State of the European Union uses personal data in Austria for a purpose that cannot be ascribed to any of the controller's establishments in Austria.

(3) Furthermore, this law shall not be applied insofar as personal data are only transmitted through Austrian territory.

(4) Legal provisions deviating from paras. 1 to 3 shall be permissible only in matters not subject to the law of the European Union.

Artikel 2

1. Hauptstück

Durchführung der Datenschutz-Grundverordnung und ergänzende Regelungen

1. Abschnitt

Allgemeine Bestimmungen

Anwendungsbereich und Durchführungsbestimmung

§ 4. (1) Die Bestimmungen der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1, (im Folgenden: DSGVO) und dieses Bundesgesetzes gelten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, soweit nicht die spezifischeren Bestimmungen des 3. Hauptstücks dieses Bundesgesetzes vorgehen.

(2) Kann die Berichtigung oder Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO bis zu diesem Zeitpunkt einzuschränken.

(3) Die Verarbeitung von personenbezogenen Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen ist unter Einhaltung der Vorgaben der DSGVO zulässig, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verarbeitung solcher Daten besteht oder
2. sich sonst die Zulässigkeit der Verarbeitung dieser Daten aus gesetzlichen Sorgfaltspflichten ergibt oder die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten gemäß Art. 6 Abs. 1 lit. f DSGVO erforderlich ist, und die Art und Weise, in der die Datenverarbeitung vorgenommen wird, die Wahrung der Interessen der betroffenen Person nach der DSGVO und diesem Bundesgesetz gewährleistet.

(4) Bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, ist die Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO zur Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das vierzehnte Lebensjahr vollendet hat.

für Zwecke solcher Angelegenheiten bestehen, in denen die Zuständigkeit zur

Article 2

Chapter 1

Implementation of the General Data Protection Regulation and supplementary provisions

Part 1

General provisions

Scope of application and implementing provision

§ 4. (1) The provisions of Regulation (EU) 2016/679 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 No L 119 of 4 May 2016, p. 1 (in the following: General Data Protection Regulation) and this federal law 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 the more specific provisions of Chapter 3 of this federal law prevail.

(2) If personal data processed by automated means cannot be rectified or erased immediately because they can be rectified or erased only at certain times for economic or technical reasons, processing of the personal data concerned shall be restricted until that time, with the effect as stipulated in Article 18 para. 2 of the General Data Protection Regulation.

(3) Processing personal data on acts or omissions punishable by courts or administrative authorities, in particular concerning suspected criminal offences, as well as data on criminal convictions and precautionary measures involving the deprivation of liberty, is permitted if the requirements of the General Data Protection Regulation are met and if

1. an explicit legal authorisation or obligation to process such data exists; or
2. the legitimacy of the processing of such data is otherwise based on statutory duties of diligence, or processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party pursuant to Article 6 para. 1 (f) of the General Data Protection Regulation, and the manner in which the data are processed safeguards the interests of the data subject according the General Data Protection Regulation and this federal law.

(4) In the case of an offer of information society services directly to a child, consent to the processing of the personal data of a child pursuant to Article 6 para. 1 (a) of the General Data Protection Regulation shall be lawful where the child is at least 14 years old.

(5) Insofar as files managed manually, i.e. files managed without automatic

Gesetzgebung Bundessache ist, gelten sie als Datenverarbeitungen im Sinne der DSGVO und dieses Bundesgesetzes.

Datenschutzbeauftragter

§ 5. (1) Der Datenschutzbeauftragte und die für ihn tätigen Personen sind unbeschadet sonstiger Verschwiegenheitspflichten bei der Erfüllung der Aufgaben zur Geheimhaltung verpflichtet. Dies gilt insbesondere in Bezug auf die Identität betroffener Personen, die sich an den Datenschutzbeauftragten gewandt haben, sowie über Umstände, die Rückschlüsse auf diese Personen zulassen, es sei denn, es erfolgte eine ausdrückliche Entbindung von der Verschwiegenheit durch die betroffene Person. Der Datenschutzbeauftragte und die für ihn tätigen Personen dürfen die zugänglich gemachten Informationen ausschließlich für die Erfüllung der Aufgaben verwenden und sind auch nach Ende ihrer Tätigkeit zur Geheimhaltung verpflichtet.

(2) Erhält ein Datenschutzbeauftragter bei seiner Tätigkeit Kenntnis von Daten, für die einer der Kontrolle des Datenschutzbeauftragten unterliegenden Stelle beschäftigten Person ein gesetzliches Aussageverweigerungsrecht zusteht, steht dieses Recht auch dem Datenschutzbeauftragten und den für ihn tätigen Personen insoweit zu, als die Person, der das gesetzliche Aussageverweigerungsrecht zusteht, davon Gebrauch gemacht hat. Im Umfang des Aussageverweigerungsrechts des Datenschutzbeauftragten unterliegen seine Akten und andere Schriftstücke einem Sicherstellungs- und Beschlagnahmeverbot.

(3) Der Datenschutzbeauftragte im öffentlichen Bereich ist bezüglich der Ausübung seiner Aufgaben weisungsfrei. Das oberste Organ hat das Recht, sich über die Gegenstände der Geschäftsführung beim Datenschutzbeauftragten im öffentlichen Bereich zu unterrichten. Dem ist vom Datenschutzbeauftragten nur insoweit zu entsprechen, als dies nicht der Unabhängigkeit des Datenschutzbeauftragten im Sinne von Art. 38 Abs. 3 DSGVO widerspricht.

(4) Im Wirkungsbereich jedes Bundesministeriums sind unter Bedachtnahme auf Art und Umfang der Datenverarbeitungen sowie je nach Einrichtung des Bundesministeriums ein oder mehrere Datenschutzbeauftragte vorzusehen. Diese müssen dem jeweiligen Bundesministerium oder der jeweiligen nachgeordneten Dienststelle oder sonstigen Einrichtung angehören.

(5) Die Datenschutzbeauftragten im öffentlichen Bereich gemäß Abs. pflegen einen regelmäßigen Erfahrungsaustausch, insbesondere im Hinblick auf die Gewährleistung eines einheitlichen Datenschutzstandards.

Datengeheimnis

§ 6. (1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für

processing, exist for the purposes of matters in which the Federal Government has the power to pass laws, these files are deemed to be data processing operations as referred to in the General Data Protection Regulation and in this federal law.

Data protection officer

§ 5. (1) Without prejudice to other obligations of confidentiality, the data protection officer and the persons working for the data protection officer shall be bound by confidentiality when fulfilling their duties. This shall apply in particular in relation to the identity of data subjects who applied to the data protection officer, and to circumstances that allow identification of these persons, unless the data subject has expressly granted a release from confidentiality. The data protection officer and the persons working for the data protection officer may exclusively use information made available to fulfil their duties and shall be bound by confidentiality even after the end of their activities.

(2) If, during bis or ber activities, a data protection officer obtains knowledge of data in respect of which a person employed with a body subject to the supervision of the data protection officer has a statutory right to refuse to give evidence, the data protection officer and the persons working for the data protection officers shall also have such a right to the extent to wbich the person who has the right to refuse to give evidence exercised that right. The files and other documents of the data protection officer are subject to a prohibition of seizure and confiscation to the extent of the right of the data protection officer to refuse to give evidence.

(3) Public-sector data protection officers are not bound by any instructions when exercising their duties. The highest governing bodies or officers have the right to obtain information on matters to be dealt with from a public-sector data protection officer. The data protection officer shall provide information only insofar as the independence of the data protection officer as described in Article 38 para. 3 of the General Data Protection Regulation is not impaired by doing so.

(4) Considering the type and scope of data processing activities and depending on the facilities of a federal ministry, one or several data protection officers shall be appointed in the sphere of responsibilities of each federal ministry. These data protection officers shall be employed by the relevant federal ministry or the relevant subordinate office or other entity.

(5) Public-sector data protection officers pursuant to para. 3 shall regularly exchange information, in particular with regard to ensuring uniform data protection standards.

Confidentiality of data

§ 6. (1) The controller, the processor and their employees, i.e. employees and persons in a quasi-employee relationship, shall ensure the confidentiality of personal data from data processing activities that have been entrusted or have become accessible to them solely due to their employment, without prejudice to other statutory obligations of confidentiality, unless a legitimate reason for the transmission of the data that have been entrusted or have become accessible to them exists (confidentiality of data).

(2) Employees may transmit personal data only if expressly ordered to do so by their employer. Unless such an obligation of their employees already exists by law, the controller and the processor shall contractually bind their employees to transmit personal data from data processing activities only on the basis of orders and to maintain the confidentiality of data even after the end of their employment with the controller or processor.

(3) The controller and the processor shall inform the employees affected by these orders about the transmission orders applicable to them and about the consequences of a violation of data confidentiality.

(4) Without prejudice to the right to give instructions under constitutional law, an employee must not incur any disadvantage from refusing to comply with an order for a prohibited transmission of data.

(5) The statutory right of a controller to refuse to give evidence shall not be avoided by questioning a processor working for the controller, and in particular not

diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

2. Abschnitt

Datenverarbeitungen zu spezifischen Zwecken

Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke

§ 7. (1) Für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Verantwortliche alle personenbezogenen Daten verarbeiten, die

1. öffentlich zugänglich sind,
2. er für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für ihn pseudonymisierte personenbezogene Daten sind und der Verantwortliche die Identität der betroffenen Person mit rechtlich zulässigen Mitteln nicht bestimmen kann.

(2) Bei Datenverarbeitungen für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke, die nicht unter Abs. 1 fallen, dürfen personenbezogene Daten nur

1. gemäß besonderen gesetzlichen Vorschriften,
2. mit Einwilligung der betroffenen Person oder
3. mit Genehmigung der Datenschutzbehörde gemäß Abs. 3

verarbeitet werden.

(3) Eine Genehmigung der Datenschutzbehörde für die Verarbeitung von personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke ist auf Antrag des Verantwortlichen der Untersuchung zu erteilen, wenn

1. die Einholung der Einwilligung der betroffenen Person mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet,
2. ein öffentliches Interesse an der beantragten Verarbeitung besteht und
3. die fachliche Eignung des Verantwortlichen glaubhaft gemacht wird.

Sollen besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) ermittelt werden, muss ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muss gewährleistet sein, dass die personenbezogenen Daten beim Verantwortlichen der Untersuchung nur von Personen verarbeitet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist. Die Datenschutzbehörde hat die Genehmigung an die Erfüllung von Bedingungen und Auflagen zu knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der betroffenen Person notwendig ist.

(4) Einem Antrag nach Abs. 3 ist jedenfalls eine vom Verfügungsbefugten über die Datenbestände, aus denen die personenbezogenen Daten ermittelt werden sollen, unterfertigte Erklärung anzuschließen, dass er dem Verantwortlichen die Datenbestände für die Untersuchung zur Verfügung stellt. Anstelle dieser Erklärung kann auch ein diese Erklärung ersetzender Exekutionstitel (§ 367 Abs. 1 der Exekutionsordnung – EO, RGBl. Nr. 79/1896) vorgelegt werden.

(5) Auch in jenen Fällen, in welchen die Verarbeitung von personenbezogenen Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der Personenbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit personenbezogenen Daten gemäß Abs. 1 Z 3 das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, ist der Personenbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

(6) Rechtliche Beschränkungen der Zulässigkeit der Benützung von

by seizing or confiscating documents processed by automated means.

Part 2

Data processing for specific purposes

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

§ 7. (1) For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes whose goal is not to obtain results in a form relating to specific data subjects, the controller may process all personal data that

1. are publicly accessible,
2. the controller has lawfully collected for other research projects or other purposes, or
3. are pseudonymised personal data for the controller, and the controller cannot establish the identity of the data subject by legal means.

(2) In the case of processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes that do not fall under para. 1, personal data may be processed only

1. pursuant to specific legal provisions,
2. with the consent of the data subject, or
3. with a permit of the Data Protection Authority pursuant to para. 3.

(3) A permit of the Data Protection Authority for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall be granted at the request of the controller ordering the research project, if

1. the consent of the data subject is impossible to obtain because the data subject cannot be reached or the effort would otherwise be unreasonable,
2. there is a public interest in the processing for which a permit is sought, and
3. the professional aptitude of the controller has been satisfactorily demonstrated.

If special categories of personal data (Article 9 of the General Data Protection Regulation) are to be collected, an important public interest in the research project must exist; furthermore, it must be ensured that the personal data are processed at the premises of the controller ordering the research project only by persons who are subject to a statutory obligation of confidentiality regarding the subject matter of the research project or whose reliability in this respect is credible. The Data Protection Authority shall issue the permit subject to terms and conditions, insofar as this is necessary to safeguard the data subjects' interests which deserve protection.

(4) A request according to para. 3 must, however, be accompanied by a statement signed by the person authorised to exercise rights in respect of the data files from which the personal data are to be collected, stating that this person is making the data files available for the research project. Instead of this statement, a writ of enforcement (§ 367 para. 1 of the Enforcement Code, Imperial Law Gazette No 79/1896) replacing this statement may be submitted.

(5) Even in cases where the processing of personal data for scientific research purposes or statistical purposes is permitted in a form which allows the identification of data subjects, the data shall be coded without delay so that the data subjects are no longer identifiable if specific phases of scientific or statistical work can be performed with personal data pursuant to para. 1 subpara. 3. Unless otherwise expressly provided for by law, data in a form which allows the identification of data subjects shall be rendered unidentifiable as soon as it is no longer necessary for scientific or statistical work to keep them identifiable.

(6) Legal restrictions on the right to use personal data for other reasons, in

personenbezogenen Daten aus anderen, insbesondere urheberrechtlichen Gründen, bleiben unberührt.

Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen

§ 8. (1) Soweit gesetzlich nicht ausdrücklich anderes bestimmt ist, bedarf die Übermittlung von Adressdaten eines bestimmten Kreises von betroffenen Personen zum Zweck ihrer Benachrichtigung oder Befragung der Einwilligung der betroffenen Personen.

(2) Wenn allerdings eine Beeinträchtigung der Geheimhaltungsinteressen der betroffenen Personen angesichts der Auswahlkriterien für den Betroffenenkreis und des Gegenstands der Benachrichtigung oder Befragung unwahrscheinlich ist, bedarf es keiner Einwilligung, wenn

1. Daten desselben Verantwortlichen verarbeitet werden oder
2. bei einer beabsichtigten Übermittlung der Adressdaten an Dritte
   a) an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht oder
   b) keiner der betroffenen Personen nach entsprechender Information über Anlass und Inhalt der Übermittlung innerhalb angemessener Frist Widerspruch gegen die Übermittlung erhoben hat.

(3) Liegen die Voraussetzungen des Abs. 2 nicht vor und würde die Einholung der Einwilligung der betroffenen Personen gemäß Abs. 1 einen unverhältnismäßigen Aufwand erfordern, ist die Übermittlung der Adressdaten mit Genehmigung der Datenschutzbehörde gemäß Abs. 4 zulässig, falls die Übermittlung an Dritte

1. zum Zweck der Benachrichtigung oder Befragung aus einem wichtigen Interesse des Betroffenen selbst,
2. aus einem wichtigen öffentlichen Benachrichtigungs- oder Befragungsinteresse oder
3. zur Befragung der betroffenen Personen für wissenschaftliche oder statistische Zwecke

erfolgen soll.

(4) Die Datenschutzbehörde hat auf Antrag eines Verantwortlichen, der Adressdaten verarbeitet, die Genehmigung zur Übermittlung zu erteilen, wenn der Antragsteller das Vorliegen der in Abs. 3 genannten Voraussetzungen glaubhaft macht und überwiegende schutzwürdige Geheimhaltungsinteressen der betroffenen Personen der Übermittlung nicht entgegenstehen. Die Datenschutzbehörde hat die Genehmigung an die Erfüllung von Bedingungen und Auflagen zu knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der betroffenen Personen notwendig ist.

(5) Die übermittelten Adressdaten dürfen ausschließlich für den genehmigten Zweck verarbeitet werden und sind zu löschen, sobald sie für die Benachrichtigung oder Befragung nicht mehr benötigt werden.

(6) Sofern es gemäß den vorstehenden Bestimmungen zulässig ist, Namen und Adresse von Personen, die einem bestimmten Betroffenenkreis angehören, zu übermitteln, dürfen auch die zum Zweck der Auswahl der zu übermittelnden Adressdaten notwendigen Verarbeitungen vorgenommen werden.

Freiheit der Meinungsäußerung und Informationsfreiheit

Soweit dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen, finden von der DSGVO die Kapitel II (Grundsätze), mit Ausnahme des Art. 5, Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), mit Ausnahme der Art. 28, 29 und 32, Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) auf die Verarbeitung, die zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, keine Anwendung. Von den Bestimmungen dieses Bundesgesetzes ist in solchen Fällen § 6 (Datengeheimnis) anzuwenden.

Verarbeitung personenbezogener Daten im Katastrophenfall

§ 10. (1) Verantwortliche des öffentlichen Bereichs und Hilfsorganisationen

particular for copyright reasons, shall not be affected.

Providing addresses to inform and interview data subjects

§ 8. (1) Unless otherwise expressly provided for by law, providing address data of a certain group of data subjects in order to inform or interview them shall require the consent of the data subjects.

(2) If, however, an infringement of the data subject's interests in confidentiality is unlikely, considering the selection criteria for the group of data subjects and the subject of the information or interview, no consent shall be required

1. if data from the same controller are processed, or
2. in the case of an intended transfer of address data to third parties,
   a) if there is also a public interest in the information or interview, or
   b) if none of the data subjects, after having received appropriate information on the reason and content of the transfer, has objected to the transfer within a reasonable period.

(3) If the requirements of para. 2 are not met and if obtaining the consent of the data subjects pursuant to para. 1 would require a disproportionate effort, the transfer of the address data shall be permissible with a permit of the Data Protection Authority pursuant to para. 4 if the data are to be transferred to third parties

1. for the purpose of information or an interview due to an important interest of the data subject,
2. due to an important public interest in the information or interview, or
3. for an interview of the data subjects for scientific or statistical purposes.

(4) At the request of a controller processing address data, the Data Protection Authority shall grant the permit for their transfer if the controller has satisfactorily demonstrated that the requirements stipulated in para. 3 have been met and no overriding interests in confidentiality wbich deserve protection on the part of the data subjects represent an obstacle to the transfer. The Data Protection Authority shall issue the permit subject to terms and conditions, insofar as this is necessary to safeguard interests of the data subjects which deserve protection.

(5) The transferred address data shall only be processed for the permitted purpose and shall be erased as soon as they are no longer needed for information or interviews.

(6) If it is lawful pursuant to the aforementioned provisions to transfer the names and addresses of persons belonging to a certain group of data subjects, the processing required for selecting the address data to be transferred shall also be permitted.

Freedom of expression and information

§ 9. If it is necessary to reconcile the rigbt to the protection of personal data with the freedom of expression and information, in particular with regard to the processing of personal data by media undertakings, media services and their employees directly for their journalistic purposes as referred to in the Media Act, Federal Law Gazette No 314/1981, Chapter II (principles), with the exception of Article 5, Chapter III (rights of the data subject), Chapter IV (controller and processor), with the exception of Articles 28, 29 and 32, Cbapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) of the General Data Protection Regulation shall not apply to processing for journalistic purposes or the purposes of academic, artistic or literary expression. Of the provisions of this federal law, § 6 (confidentiality of data) shall be applied in such cases.

Processing of personal data in case of emergency

§ 10. (1) In case of emergency, public-sector controllers and relief

sind im Katastrophenfall ermächtigt, personenbezogene Daten gemeinsam zu verarbeiten, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig ist.

(2) Wer rechtmäßig über personenbezogene Daten verfügt, darf diese an Verantwortliche des öffentlichen Bereichs und Hilfsorganisationen übermitteln, sofern diese die personenbezogenen Daten zur Bewältigung der Katastrophe für die in Abs. 1 genannten Zwecke benötigen.

(3) Eine Übermittlung von personenbezogenen Daten in das Ausland ist zulässig, soweit dies für die Erfüllung der in Abs. 1 genannten Zwecke unbedingt notwendig ist. Daten, die für sich allein die betroffene Person strafrechtlich belasten, dürfen nicht übermittelt werden, es sei denn, dass diese zur Identifizierung im Einzelfall unbedingt notwendig sind. Die Datenschutzbehörde ist von den veranlassten Übermittlungen und den näheren Umständen des Anlass gebenden Sachverhaltes unverzüglich zu verständigen. Die Datenschutzbehörde hat zum Schutz der Betroffenenrechte weitere Datenübermittlungen zu untersagen, wenn der durch die Datenweitergabe bewirkte Eingriff in das Grundrecht auf Datenschutz durch die besonderen Umstände der Katastrophensituation nicht gerechtfertigt ist.

(4) Auf Grund einer konkreten Anfrage eines nahen Angehörigen einer tatsächlich oder vermutlich von der Katastrophe unmittelbar betroffenen Person sind Verantwortliche ermächtigt, dem Anfragenden personenbezogene Daten zum Aufenthalt der betroffenen Person und dem Stand der Ausforschung zu übermitteln, wenn der Angehörige seine Identität und das Naheverhältnis glaubhaft darlegt.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) dürfen an nahe Angehörige nur übermittelt werden, wenn sie ihre Identität und ihre Angehörigeneigenschaft nachweisen und die Übermittlung zur Wahrung ihrer Rechte oder jener der betroffenen Person erforderlich ist. Die Sozialversicherungsträger und Behörden sind verpflichtet, die Verantwortlichen des öffentlichen Bereichs und Hilfsorganisationen zu unterstützen, soweit dies zur Überprüfung der Angaben des Anfragenden erforderlich ist.

(5) Als nahe Angehörige im Sinne dieser Bestimmung sind Eltern, Kinder, Ehegatten, eingetragene Partner und Lebensgefährten der betroffenen Personen zu verstehen. Andere Angehörige dürfen die erwähnten Auskünfte unter denselben Voraussetzungen wie nahe Angehörige dann erhalten, wenn sie eine besondere Nahebeziehung zu der von der Katastrophe tatsächlich oder vermutlich unmittelbar betroffenen Person glaubhaft machen.

(6) Die zu Zwecken der Bewältigung des Katastrophenfalles verarbeiteten personenbezogenen Daten sind unverzüglich zu löschen, wenn sie für die Erfüllung des konkreten Zwecks nicht mehr benötigt werden.

Verarbeitung personenbezogener Daten im Beschäftigungskontext

§ 11. Das Arbeitsverfassungsgesetz – ArbVG, BGBl. Nr. 22/1974, ist, soweit es die Verarbeitung personenbezogener Daten regelt, eine Vorschrift im Sinne des Art. 88 DSGVO. Die dem Betriebsrat nach dem ArbVG zustehenden Befugnisse bleiben unberührt.

organisations shall be authorised to jointly process data to the extent that this is necessary to assist persons directly affected by a disaster, to locate and identify missing or deceased persons and to provide information to their relatives.

(2) Anybody who lawfully possesses personal data shall be permitted to transfer these data to public-sector controllers and relief organisations if these controllers and organisations need this personal data to manage a disaster for the purposes specified in para. 1.

(3) The transfer abroad of personal data is permitted insofar as this is absolutely necessary to fulfil the purposes mentioned in para 1. Data that by themselves would make the data subject liable to criminal prosecution shall not be transferred unless they are absolutely necessary for identification in a particular case. The Data Protection Authority shall be informed immediately about the data transfers performed and about the circumstances of the motivating incident. The Data Protection Authority shall prohibit further data transfers if the interference with the fundamental right to data protection resulting from the data transfer is not justified by the special circumstances caused by a disaster.

(4) Based on a specific inquiry of a close relative of a person who has actually or presumably been directly affected by a disaster, controllers are authorised to transfer to the inquiring person personal data regarding the whereabouts of the data subject and on the progress of the search, if the relative satisfactorily demonstrates his or her identity and close relationship to the data subject.

Special categories of personal data (Article 9 of the General Data Protection Regulation) may be transferred to close relatives only if they prove their identity and their capacity as a relative and if the transfer is necessary to safeguard their rights or the rights of the data subject. The social insurance agencies and authorities are obliged to assist the public-sector controllers and relief organisations if this is necessary to verify the information provided by the inquiring person.

(5) Close relatives pursuant to this provision means parents, children, spouses, registered partners and companions in life of the data subjects. Other relatives may receive the aforementioned information under the same conditions as close relatives if they satisfactorily demonstrate a special close relationship to the person actually or presumably directly affected by a disaster.

(6) The personal data processed for the purposes of managing a disaster shall be deleted immediately if they are no longer required to fulfil the specific purpose.

Processing of personal data in the context of employment

§ 11. To the extent that it regulates the processing of personal data, the Collective Labour Relations Act, Federal Law Gazette No 22/1974, is a rule as referred to in Article 88 of the General Data Protection Regulation. The powers of the works council pursuant to the Collective Labour Relations Act shall remain unaffected.

3. Abschnitt
Bildverarbeitung

Zulässigkeit der Bildaufnahme

§ 12. (1) Eine Bildaufnahme im Sinne dieses Abschnittes bezeichnet die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken. Zur Bildaufnahme gehören auch dabei mitverarbeitete akustische Informationen. Für eine derartige Bildaufnahme gilt dieser Abschnitt, soweit nicht durch andere Gesetze Besonderes bestimmt ist.

(2) Eine Bildaufnahme ist unter Berücksichtigung der Vorgaben gemäß § 13 zulässig, wenn

1. sie im lebenswichtigen Interesse einer Person erforderlich ist,

Part 3
Processing of images

Permissibility of recording images

§ 12. (1) For the purposes of this Part, recording images means observing occurrences in public or non-public space for private purposes, using technical devices for the processing of images. Recording images also includes acoustic information processed together with the images. This Part shall apply to such recording of images unless other laws provide for more specific provisions.

(2) Considering the requirements pursuant to § 13, recording images is permitted if

1. it is necessary in the vital interest of a person,

2. die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat,

3. sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist, oder

4. im Einzelfall überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.

(3) Eine Bildaufnahme ist gemäß Abs. 2 Z 4 insbesondere dann zulässig, wenn

1. sie dem vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, dient, und räumlich nicht über die Liegenschaft hinausreicht, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen,

2. sie für den vorbeugenden Schutz von Personen oder Sachen an öffentlich zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials erforderlich ist, oder

3. sie ein privates Dokumentationsinteresse verfolgt, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist.

(4) Unzulässig ist

1. eine Bildaufnahme ohne ausdrückliche Einwilligung der betroffenen Person in deren höchstpersönlichen Lebensbereich,

2. eine Bildaufnahme zum Zweck der Kontrolle von Arbeitnehmern,

3. der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten mit anderen personenbezogenen Daten oder

4 die Auswertung von mittels Bildaufnahmen gewonnenen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) als Auswahlkriterium.

(5) Im Wege einer zulässigen Bildaufnahme ermittelte personenbezogene Daten dürfen im erforderlichen Ausmaß übermittelt werden, wenn für die Übermittlung eine der Voraussetzungen des Abs. 2 Z 1 bis 4 gegeben ist. Abs. 4 gilt sinngemäß.

Besondere Datensicherheitsmaßnahmen und Kennzeichnung

§ 13. (1) Der Verantwortliche hat dem Risiko des Eingriffs angepasste geeignete Datensicherheitsmaßnahmen zu ergreifen und dafür zu sorgen, dass der Zugang zur Bildaufnahme und eine nachträgliche Veränderung derselben durch Unbefugte ausgeschlossen ist.

(2) Der Verantwortliche hat – außer in den Fällen einer Echtzeitüberwachung – jeden Verarbeitungsvorgang zu protokollieren.

(3) Aufgenommene personenbezogene Daten sind vom Verantwortlichen zu löschen, wenn sie für den Zweck, für den sie ermittelt wurden, nicht mehr benötigt werden und keine andere gesetzlich vorgesehene Aufhewahrungspflicht besteht. Eine länger als 72 Stunden andauernde Aufbewahrung muss verhältnismäßig sein und ist gesondert zu protokollieren und zu begründen.

(4) Die Abs. 1 bis 3 finden keine Anwendung auf Bildaufnahmen nach § 12 Abs. 3 Z 3.

(5) Der Verantwortliche einer Bildaufnahme hat diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen, es sei denn, dieser ist den betroffenen Personen nach den Umständen des Falles bereits bekannt.

(6) Die Kennzeichnungspflicht gilt nicht in den Fällen des § 12 Abs. 3 Z 3 und für zeitlich strikt zu begrenzende Verarbeitungen im Einzelfall, deren Zweck ausscbließlich mittels einer verdeckten Ermittlung erreicht werden kann, unter der Bedingung, dass der Verantwortliche ausreichende Garantien zur Wahrung der Betroffeneninteressen vorsieht, insbesondere durch eine nachträgliche Information der betroffenen Personen.

(7) Werden entgegen Abs. 5 keine ausreichenden Informationen bereitgestellt, kann jeder von einer Verarbeitung potenziell Betroffene vom Eigentümer oder Nutzungsberechtigten einer Liegenschaft oder eines Gebäudes

2 the data subject has consented to the processing of the data subject's personal data,

3. it is ordered or permitted by special statutory provisions, or

4. there are overriding legitimate interests of the controller or a third party in a particular case, and proportionality is given.

(3) Recording images pursuant to para. 2 subpara. 4 is permitted, in particular, if

1. it serves the precautionary protection of persons and items on private land exclusively used by the controller and does not reach beyond the boundaries of the piece of land, except when it includes public traffic areas, which may be unavoidable to fulfil the purpose of the image recording.

2. it is required for the precautionary protection of persons or items in publicly accessible places that are subject to the controller's right to undisturbed possession because that right has already been infringed or because the place, by its nature, has a special risk potential, and no less restrictive appropriate measures are available, or

3. it serves a private documentary interest and does not aim to record uninvolved persons to identify them or to record, in a targeted manner, items that are appropriate for indirectly identifying such persons.

(4) It is not permitted to:

1. record images in a data subject's most private sphere without the express consent of the data subject,

2. record images to monitor employees,

3. align, in an automated manner, personal data obtained from image recordings with other personal data, or

4. analyse personal data obtained from image recordings on the basis of special categories of personal data (Article 9 of the General Data Protection Regulation) as selection criteria.

(5) Data collected by means of permitted image recording may be transferred to the extent required, if one of the requirements of para. 2 subparas. 1 to 4 is met. Para. 4 shall apply accordingly.

Special data security measures and warning sign

§ 13. (1) The controller shall take appropriate measures corresponding to the risk posed by an interference and ensure that unauthorised persons cannot access or subsequently change the image recording.

(2) Except in the case of real-time surveillance, the controller shall keep logs of every processing operation.

(3) The controller shall erase personal data recorded if they are no longer necessary in relation to the purposes for whicb they were collected and if there is no other statutory obligation to maintain the data. Maintaining data for more than 72 hours must be proportionate; separate logs must kept of these data, and reasons must be stated.

(4) Paras. 1 to 3 shall not be applied to image recordings pursuant to § 12 para. 3 subpara. 3.

(5) The controller of an image recording must appropriately mark the recording. The warning sign shall clearly specify the controller, unless the controller is already known to the data subjects based on the circumstances of the case.

(6) The obligation to warning sign the data shall not apply in the cases referred to in § 12 para. 3 subpara. 3 and, in particular cases, to processing operations that must be strictly limited in terms of time and whose purpose can exclusively be achieved by means of covert investigation, provided that the controller ensures there are sufficient safeguards for the data subjects' interests, in particular by subsequent notification of the data subject.

(7) If, in violation of para. 5, sufficient information is not provided, every data subject potentially affected by a processing operation can request information on the identity of the controller from the owner of, or person authorised to use, the

oder sonstigen Objekts, von dem aus eine solche Verarbeitung augenscheinlich ausgeht, Auskunft über die Identität des Verantwortlichen begehren. Die unbegründete Nichterteilung einer derartigen Auskunft ist einer Verweigerung der Auskunft nach Art. 15 DSGVO gleichzuhalten.

2. Hauptstück
Organe

1. Abschnitt
Datenschutzrat

Einrichtung und Aufgaben

§ 14. (1) Beim ist ein Datenschutzrat eingerichtet. Dieser nimmt zu Fragen von grundsätzlicher Bedeutung für den Datenschutz Stellung, fördert die einheitliche Fortentwicklung des Datenschutzes und berät die Bundesregierung in rechtspolitischer Hinsicht bei datenschutzrechtlich relevanten Vorhaben.

(2) Zur Erfüllung seiner Aufgaben nach Abs. 1

1. kann der Datenschutzrat Empfehlungen in datenschutzrechtlicher Hinsicht an die Bundesregierung und die Bundesminister richten;
2. kann der Datenschutzrat Gutachten erstellen oder in Auftrag geben;
3. ist dem Datenschutzrat Gelegenheit zur Stellungnahme zu Gesetzesentwürfen der Bundesministerien, soweit diese datenschutzrechtlich von Bedeutung sind, sowie zu Verordnungen im Vollzugsbereich des Bundes, die wesentliche Fragen des Datenschutzes betreffen, zu geben;
4. hat der Datenschutzrat das Recht, von Verantwortlichen des öffentlichen Bereichs Auskünfte und Berichte zu verlangen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist;
5. kann der Datenschutzrat seine Beobachtungen, Bedenken und Anregungen veröffentlichen und den Verantwortlichen des öffentlichen Bereichs zur Kenntnis bringen.

(3) Abs. 2 Z 3 und 4 gilt nicht, soweit innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften betroffen sind.

Zusammensetzung

§ 15. (1) Dem Datenschutzrat gehören an:

1. Vertreter der politischen Parteien: Zwölf Mitglieder entsenden die politischen Parteien nach dem System von d'Hondt im Verhältnis ihrer Mandatsstärke im Hauptausschuss des Nationalrates. Jede im Hauptausschuss des Nationalrates vertretene politische Partei hat Anspruch, im Datenschutzrat vertreten zu sein. Eine im Hauptausschuss des Nationalrates vertretene Partei, der nach der obigen Berechnung kein Mitglied zukommt, kann ein Mitglied namhaft machen;
2. je ein Vertreter der Bundeskammer für Arbeiter und Angestellte und der Wirtschaftskammer Österreich;
3. zwei Vertreter der Länder;
4. je ein Vertreter des Gemeindebundes und des Städtebundes;
5. ein vom zu entsendender Vertreter des Bundes;
6. ein von der Bundesregierung zu entsendender Vertreter aus dem Kreis der Datenschutzbeauftragten der Bundesministerien;
7. zwei vom Datenschutzrat nach seiner Konstituierung zu benennende nationale oder internationale Experten aus dem Bereich des Datenschutzes.

(2) Die in Abs. 1 genannten Vertreter sollen Kenntnisse sowie Erfahrungen auf den Gebieten des Datenschutzrechtes, des Unionsrechtes und der Grundrechte haben.

(3) Für jedes Mitglied gemäß Abs. 1 Z 1 bis 6 ist ein Ersatzmitglied zu entsenden, welches bei Verhinderung des Mitgliedes an dessen Stelle tritt. Die

piece of land or building or other property from which the processing operation evidently originates. Failure to provide such information without giving reasons shall be deemed a refusal to provide access pursuant to Article 15 of the General Data Protection Regulation.

Chapter 2
Bodies

Part 1
Data Protection Council

Establishment and duties

§ 14. (1) A Data Protection Council has been established at the Federal Chancellery. The Data Protection Council shall comment on questions of fundamental importance for data protection, promote the uniform further development of data protection, and advise the Federal Government on legal policy in the case of projects relevant to data protection.

(2) To fulfil its duties pursuant to para. 1,

1. the Data Protection Council can make recommendations relating to data protection to the Federal Government and the federal ministers;
2. the Data Protection Council can prepare opinions or commission such opinions;
3. the Data Protection Council shall be given the opportunity to comment on draft bills of federal ministries, insofar as these are significant for data protection law, and on regulations to be implemented by the Federal Government concerning essential issues of data protection;
4. the Data Protection Council shall have the right to request information and reports from public-sector controllers insofar as this is necessary to evaluate, from the viewpoint of data protection law, projects of significant impact on data protection in Austria;
5. the Data Protection Council can publish its observations, concerns and suggestions and submit them to the public-sector controllers.

(3) Para. 2 subparas. 3 and 4 shall not apply insofar as internal affairs of recognised churches and religious communities are concerned.

Composition

§ 15. (1) The Data Protection Council shall have the following members:

1. representatives of the political parties: The political parties shall delegate twelve members according to the d'Hondt method in proportion to the seats they have in the Main Committee of the National Council. Every political party represented in the Main Committee of the National Council has the right to be represented in the Data Protection Council. A party represented in the Main Committee of the National Council that cannot delegate a member according to the above calculation method can name a member;
2. one representative each of the Federal Chamber of Labour and the Austrian Federal Economic Chamber;
3. two representatives of the provinces;
4. one representative each of the Association of Austrian Municipalities and the Association of Austrian Cities and Towns;
5. one representative of the Federal Government to be delegated by the Federal Chancellor;
6. one representative to be delegated by the Federal Government from among the data protection officers of the federal ministries;
7. two national or international experts in data protection to be named by the Data Protection Council after its constitution.

(2) The representatives mentioned in para. 1 should have knowledge of and experience in data protection law, Union law, and fundamental rights.

(3) For each member pursuant to para. 1 subparas. 1 to 6, a substitute member shall be delegated who shall replace the member if the member is incapacitated or

Entsendung der Mitglieder und Ersatzmitglieder ist dem schriftlich mitzuteilen.

(4) Nicht angehören können dem Datenschutzrat Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre und weiters Personen, die zum Nationalrat nicht wählbar sind.

(5) Die Funktionsperiode der Mitglieder und Ersatzmitglieder gemäß Abs. 1 Z 1 bis 6 beginnt mit deren Entsendung in den Datenschutzrat und endet

1. mit der Abberufung durch die Stelle (Abs. 1) im Wege einer Mitteilung an das unter gleichzeitiger Namhaftmachung eines neuen Mitgliedes oder Ersatzmitgliedes,
2. mit der Bekanntgabe des Ausscheidens durch das Mitglied oder Ersatzmitglied im Wege einer schriftliche Mitteilung an das oder
3. spätestens mit der Neuwahl des Hauptausschusses des Nationalrates nach den §§ 29 und 30 des Geschäftsordnungsgesetzes 1975, BGBl. Nr. 410/1975.

Auf gemäß Abs. 1 Z 7 benannte Mitglieder des Datenschutzrates findet Z 3 Anwendung.

(6) Nach Neuwahl des Hauptausschusses des Nationalrates (Abs. 5 Z 3) führt das bisherige Präsidium gemäß § 17 Abs. 4 die Geschäfte bis zur konstituierenden Sitzung der neubestellten Mitglieder und Ersatzmitglieder fort. Binnen eines Zeitraumes von zwei Wochen ab der Neuwahl des Hauptausschusses des Nationalrates haben die entsendenden Stellen eine dem Abs. 1 entsprechende Anzahl von Mitgliedern und Ersatzmitgliedern dem schriftlich bekannt zu geben. Die Wiederbestellung von Mitgliedern und Ersatzmitgliedern ist zulässig.

(7) Die konstituierende Sitzung des Datenschutzrates hat spätestens sechs Wochen nach der Wahl des Hauptausschusses des Nationalrates stattzufinden und ist vom einzuberufen.

(8) Die Tätigkeit der Mitglieder und Ersatzmitglieder des Datenschutzrates ist ehrenamtlich. Mitglieder und Ersatzmitglieder des Datenschutzrates, die außerhalb von Wien wohnen, haben im Fall der Teilnahme an Sitzungen des Datenschutzrates Anspruch auf Ersatz der angemessenen Reisekosten nach Maßgabe der Reisegebührenvorschriften des Bundes. Die Vergütungen und Erstattungen sind im Nachhinein quartalsweise vom anzuweisen.

Vorsitz und Geschäftsführung

§ 16. (1) Der Datenschutzrat gibt sich mit Beschluss eine Geschäftsordnung.

(2) Der Datenschutzrat hat in der konstituierenden Sitzung aus den vorliegenden Wahlvorschlägen mit einfacher Mehrheit aus seiner Mitte einen Vorsitzenden und zwei stellvertretende Vorsitzende zu wählen. Stichwahlen sind zulässig. Die Wahlvorschläge sind den Mitgliedern und Ersatzmitgliedern gleichzeitig mit der Einladung zur konstituierenden Sitzung bekannt zu geben. Die Wiederwahl ist zulässig.

(3) Die Funktionsperiode des Vorsitzenden und der stellvertretenden Vorsitzenden endet

1. mit Eintritt einer der Voraussetzungen des § 15 Abs. 5 Z 1 bis 3,
2. mit Bekanntgabe der Zurücklegung der Funktion durch den Vorsitzenden oder einen der stellvertretenden Vorsitzenden im Wege einer Erklärung in der Sitzung des Datenschutzrates oder einer schriftlichen Mitteilung an das oder
3. nach Abwahl durch den Datenschutzrat mit einfacher Mehrheit der abgegebenen Stimmen und Anwesenheit von mehr als zwei Drittel seiner Mitglieder oder Ersatzmitglieder.

Nach dem Ende der Funktionsperiode des Vorsitzenden oder eines stellvertretenden Vorsitzenden ist umgehend ein neuer Vorsitzender oder ein neuer stellvertretender Vorsitzender zu wählen.

(4) Der gemäß Abs. 2 gewählte Vorsitzende vertritt den Datenschutzrat nach außen.

(5) Die Geschäftsführung des Datenschutzrates obliegt dem

unavailable. The Federal Chancellery shall be notified in writing of the delegation of the members and substitute members.

(4) Members of the Federal Government or of a provincial government and state secretaries as well as persons who may not be elected to the National Council cannot be members of the Data Protection Council.

(5) The term of office of the members and substitute members pursuant to para. 1 subparas. 1 to 6 starts when they are delegated to the Data Protection Council and ends

1. when they are dismissed by the entity or body delegating them (para. 1) by means of a written notification to the Federal Chancellery, with a new member or substitute member being named at the same time,
2. when the member or substitute member announces his or her resignation by means of a written notification to the Federal Chancellery, or
3. no later than when a new Main Committee of the National Council is elected pursuant to § 29 and § 30 of the Rules of Procedure Law of 1975, Federal Law Gazette No 410/1975.

Subpara. 3 shall not apply to members of the Data Protection Council named pursuant to para. 1 subpara. 7.

(6) After the election of the new Main Committee of the National Council (para. 5 subpara. 3), the previous Executive Board pursuant to § 17 para. 4 shall continue to manage the business of the Council until the constitutive meeting of the newly appointed members and substitute members. The entities or bodies delegating the members and substitute members shall notify the Federal Chancellery in writing within a period of two weeks of the election of the new Main Committee of the National Council of the members and substitute members, the number of whom must correspond to para. 1. Reappointment of the members and substitute members is permitted.

(7) The constitutive meeting of the Data Protection Council shall take place no later than six weeks after the election of the Main Committee of the National Council and shall be convened by the Federal Chancellery.

(8) The members and substitute members of the Data Protection Council shall serve in an honorary capacity. Members and substitute members of the Data Protection Council living outside of Vienna shall be entitled to receive compensation for reasonable travel expenses according to the federal regulations on travelling fees if they attend meetings of the Data Protection Council. The Federal Chancellery shall order reimbursements and refunds of the travel expenses to be paid every quarter in arrears.

Chair and management

§ 16. (1) The Data Protection Council shall adopt its rules of procedure by a resolution.

(2) In the constitutive meeting, the Data Protection Council shall elect, by a simple majority, a chair and two deputy chairs from among its members on the basis of the list of candidates proposed for election. Run-off elections are permitted. The list of candidates proposed for election shall be made known to the members and substitute members together with the invitation to the constitutive meeting. Re-election is permitted.

(3) The term of office of the chair and the deputy chairs ends

1. when the requirements of § 15 para. 5 subparas. 1 to 3 are met,
2. when the chair or one of the deputy chairs announces his or her resignation from his or her function by means of a declaration in the meeting of the Data Protection Council or a written notification to the Federal Chancellery, or
3. after the chair or one of the deputy chairs has been voted out of office by the Data Protection Council by a simple majority of the votes cast, with more than two thirds of its members or substitute members having to be present at the vote.

After the end of the term of office of the chair or one of the deputy chairs, a new chair or a new deputy chair shall be elected without delay.

(4) The chair elected pursuant to para. 2 shall represent the Data Protection Council vis-á-vis third parties.

(5) The Federal Chancellery shall be responsible for the management of the

Bundeskanzleramt. hat das hierfür notwendige Personal zur Verfügung zu stellen. Bei ihrer Tatigkeit für den Datenschutzrat sind die Bediensteten des fachlich an die Weisungen des Vorsitzenden des Datenschutzrates gebunden.

Sitzungen und Beschlussfassung

§ 17. (1) Die Sitzungen des Datenschutzrates werden vom Vorsitzenden nach Bedarf einberufen. Jedes Mitglied des Datenschutzrates kann schriftlich die Einberufung des Datenschutzrates unter Angabe des gewünschten Verhandlungsgegenstandes begehren. Liegt ein solches Begehren vor, so hat der Vorsitzende die Sitzung so anzuberaumen, dass sie spatestens vier Wochen nach Einlangen des Begehrens stattfindet.

(2) Jedes Mitglied des Datenschutzrates ist – außer im Fall der gerechtfertigten Verhinderung – verpflichtet, an den Sitzungen des Datenschutzrates teilzunehmen. Nur bei Verhinderung des Mitglieds nimmt das Ersatzmitglied an der Sitzung teil.

(3) Für Beratungen und Beschlussfassung im Datenschutzrat ist die Anwesenheit von mehr als der Halfte seiner Mitglieder oder Ersatzmitglieder erforderlich. Zur Beschlussfassung genugt die einfache Mehrheit der abgegebenen Stimmen. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulassig Minderheitenvoten sind zulassig.

(4) Bei dringlichen Angelegenheiten kann der Vorsitzende die stellvertretenden Vorsitzenden und je einen Vertreter der politischen Parteien (§ 15 Abs. 1 Z 1) zu einer außerordentlichen Sitzung (Prasidium) einladen.

(5) Der Datenschutzrat kann aus seiner Mitte ständige oder nichtstandige Arbeitsausschusse bilden, denen er die Vorbereitung, Begutachtung und Bearbeitung einzelner Angelegenheiten ubertragen kann. Er ist auch berechtigt, die Geschaftsführung, Vorbegutachtung und die Bearbeitung einzelner Angelegenheiten einem einzelnen Mitglied (Berichterstatter) zu ubertragen.

(6) Der Leiter der Datenschutzbehörde ist berechtigt, an den Sitzungen des Datenschutzrates oder seiner Arbeitsausschusse teilzunehmen. Ein Stimmrecht steht ihm nicht zu.

(7) Der Vorsitzende kann bei Bedarf Sachverständige zu den Sitzungen des Datenschutzrates oder zu Arbeitsausschussen beiziehen. Auch zur Vorbereitung von Sitzungen des Datenschutzrates oder Arbeitsausschussen kann der Vorsitzende des Datenschutzrates Experten des jeweiligen Fachgebietes beiziehen, soweit dies zur Klärung von Fragen von besonderer Bedeutung für den Datenschutz erforderlich ist.

(8) Die Beratungen in den Sitzungen des Datenschutzrates sind, soweit er nicht selbst anderes beschließt, nicht öffentlich. Die Mitglieder und Ersatzmitglieder des Datenschutzrates, der Leiter der Datenschutzbehörde sowie sein Stellvertreter und die zur Sitzung zugezogenen Sachverständigen sind zur Verschwiegenheit über alle ihnen ausschließlich aus ihrer Tatigkeit im Datenschutzrat bekanntgewordenen Tatsachen verpflichtet.

2. Abschnitt
Datenschutzbehörde

Einrichtung

§ 18. (1) Die Datenschutzbehörde wird als nationale Aufsichtsbehörde gemäß Art. 51 DSGVO eingerichtet.

(2) Der Datenschutzbehörde steht ein Leiter vor. In seiner Abwesenheit leitet sein Stellvertreter die Datenschutzbehörde. Auf ihn finden die Regelungen hinsichtlich des Leiters der Datenschutzbehörde Anwendung.

Unabhängigkeit

§ 19. (1) Die Datenschutzbehörde ist eine Dienstbehörde und Personalstelle.

(2) Der Leiter darf für die Dauer seines Amtes keine Tatigkeit ausuben, die

1. Zweifel an der unabhängigen Ausübung seines Amtes oder seiner Unbefangenheit hervorrufen könnte,
2. ihn bei der Erfüllung seiner dienstlichen Aufgaben behindert oder

Data Protection Council. The Federal Chancellor shall supply the necessary personnel for that purpose. While working for the Data Protection Council, the employees of the Federal Chancellery shall be bound by the instructions of the chair of the Data Protection Council with regard to their work.

Meetings and resolutions

§ 17. (1) The meetings of the Data Protection Council shall be convened by the chair whenever the need arises. Every member of the Data Protection Council can request in writing that the Data Protection Council be convened, stating the requested topic of discussion. If such a request has been made, the chair shall schedule a meeting that must take place no later than four weeks after receipt of the request

(2) Every member of the Data Protection Council must attend the meetings of the Data Protection Council unless the member is incapacitated or unavailable for justifiable reasons. A substitute member shall attend a meeting only if a member is incapacitated or unavailable.

(3) Deliberations and resolutions of the Data Protection Council shall require the presence of more than half of its members or substitute members. Resolutions shall be passed by a simple majority of votes cast. In the case of a parity of votes, the chair shall have a casting vote. An abstention from the vote is not permitted Dissenting opinions are permitted.

(4) In urgent matters, the chair can invite the deputy chairs and one representative of each political party (§ 15 para. 1 subpara. 1) to attend an extraordinary meeting (Executive Board).

(5) The Data Protection Council may establish permanent or non-permanent working groups from among its members which it may entrust with the preparation, appraisal and handling of specific issues. The Data Protection Council may also delegate the management, pre-appraisal and handling of specific issues to an individual member (rapporteur).

(6) The head of the Data Protection Authority shall have the right to attend the meetings of the Data Protection Council or its working groups. The head of the Data Protection Authority shall not have a voting right.

(7) If required, the chair can ask experts to attend the meetings of the Data Protection Council or the working groups. The chair of the Data Protection Council can also ask experts in the relevant field to assist in preparing meetings of the Data Protection Council or of working groups if this is required to clarify issues of special significance for data protection.

(8) The deliberations of the Data Protection Council shall not be public unless the Data Protection Council itself decides otherwise. The members and substitute members of the Data Protection Council, the head and deputy head of the Data Protection Authority, and the experts asked to attend meetings are obliged to keep confidential all facts that have become known to them exclusively on the basis of their activities in the Data Protection Council.

Part 2
Data Protection Authority

Establishment

§ 18. (1) The Data Protection Authority is established as a national supervisory authority pursuant to Article 51 of the General Data Protection Regulation.

(2) The Data Protection Authority is managed by its head. If the head is absent, his or her deputy shall manage the Data Protection Authority. The rules regarding the head of the Data Protection Authority shall also apply to the deputy.

Independent status

§ 19. (1) The Data Protection Authority acts as an authority supervising staff and as a human resource department.

(2) During his or her term of office, the head must not exercise any function that

1. could cast doubt on the independent exercise of his or her office or impartiality,
2. prevents him or her from performing their professional duties, or

3. wesentliche dienstliche Interessen gefährdet.

Er ist verpflichtet, Tätigkeiten, die er neben seiner Tätigkeit als Leiter der Datenschutzbehörde ausübt, unverzüglich dem zur Kenntnis zu bringen.

kann sich beim Leiter der Datenschutzbehörde über die Gegenstände der Geschäftsführung unterrichten. Dem ist vom Leiter der Datenschutzbehörde nur insoweit zu entsprechen, als dies nicht der völligen Unabhängigkeit der Aufsichtsbehörde im Sinne von Art. 52 DSGVO widerspricht.

Leiter der Datenschutzbehörde

§ 20. (1) Der Leiter der Datenschutzbehörde wird vom Bundespräsidenten auf Vorschlag der Bundesregierung für eine Dauer von fünf Jahren bestellt; die Wiederbestellung ist zulässig. Dem Vorschlag hat eine Ausschreibung zur allgemeinen Bewerbung voranzugehen.

(2) Der Leiter der Datenschutzbehörde hat

1. das Studium der Rechtswissenschaften abgeschlossen zu haben,
2. die persönliche und fachliche Eignung durch eine entsprechende Vorbildung und einschlägige Berufserfahrung in den von der Datenschutzbehörde zu besorgenden Angelegenheiten aufzuweisen,
3. über ausgezeichnete Kenntnisse des österreichischen Datenschutzrechtes, des Unionsrechtes und der Grundrechte zu verfügen und
4. über eine mindestens fünfjährige juristische Berufserfahrung zu verfügen.

(3) Zum Leiter der Datenschutzbehörde dürfen nicht bestellt werden:

1. Mitglieder der Bundesregierung, Staatssekretäre, Mitglieder einer Landesregierung, Mitglieder des Nationalrates, des Bundesrates oder sonst eines allgemeinen Vertretungskörpers oder des Europäischen Parlaments, ferner Volksanwälte und der Präsident des Rechnungshofes,
2. Personen, die eine in Z 1 genannte Funktion innerhalb der letzten zwei Jahre ausgeübt haben, und
3. Personen, die von der Wählbarkeit in den Nationalrat ausgeschlossen sind.

(4) Die Enthebung des Leiters ist auf Vorschlag der Bundesregierung durch den Bundespräsidenten vorzunehmen.

(5) Der Stellvertreter des Leiters der Datenschutzbehörde wird vom Bundespräsidenten auf Vorschlag der Bundesregierung nach Maßgabe der Abs. 1 bis 3 bestellt. Auf die Enthebung des Stellvertreters findet Abs. 4 Anwendung.

Aufgaben

§ 21. (1) Die Datenschutzbehörde berät die Ausschüsse des Nationalrates und des Bundesrates, die Bundesregierung und die Landesregierungen auf deren Ersuchen über legislative und administrative Maßnahmen. Die Datenschutzbehörde ist vor Erlassung von Bundesgesetzen sowie von Verordnungen im Vollzugsbereich des Bundes, die Fragen des Datenschutzes unmittelbar betreffen, anzuhören.

(2) Die Datenschutzbehörde hat die Listen nach Art. 35 Abs. 4 und 5 DSGVO im Wege einer Verordnung im Bundesgesetzblatt kundzumachen.

(3) Die Datenschutzbehörde hat die nach Art. 57 Abs. 1 lit. p DSGVO festzulegenden Kriterien im Wege einer Verordnung kundzumachen. Sie fungiert zugleich als einzige nationale Akkreditierungsstelle gemäß Art. 43 Abs. 1 lit. a DSGVO.

Befugnisse

§ 22. (1) Die Datenschutzbehörde kann vom Verantwortlichen oder Auftragsverarbeiter der überprüften Datenverarbeitung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenverarbeitungen und diesbezügliche Unterlagen begehren. Der Verantwortliche oder Auftragsverarbeiter hat die notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Verantwortlichen oder des Auftragsverarbeiters und Dritter auszuüben.

(2) Zum Zweck der Einschau ist die Datenschutzbehörde nach Verständigung

3. puts essential official interests at risk.

The head is required to report functions that he or she exercises alongside his or her office as the head of the Data Protection Authority to the Federal Chancellor without delay.

(3) The Federal Chancellor can request information from the head of the Data Protection Authority on matters to be dealt with by the Authority. The head of the Data Protection Authority has to meet this request only insofar as it does not impair the complete independence of the supervisory authority as described in Article 52 of the General Data Protection Regulation.

The head of the Data Protection Authority

§ 20. (1) The head of the Data Protection Authority is appointed for a term of five years by the Federal President on the basis of a proposal by the Federal Government; re-appointment is permitted. The proposal is to be preceded by an advertisement for the position permitting general applications.

(2) The head of the Data Protection Authority must

1. have completed a law degree,
2. have the necessary personal and professional aptitude through prior education and appropriate professional experience in the matters to be handled by the Data Protection Authority,
3. possess an excellent knowledge of Austrian data protection law, Union law and fundamental rights, and
4. have at least five years of professional experience in the legal field.

(3) The following persons may not be appointed head of the Data Protection Authority:

1. members of the Federal Government, state secretaries, members of a provincial government, members of the National Council, the Federal Council or any other general representative body or of the European Parliament, as well as members of the Ombudsman Board, and the president of the Court of Audit;
2. persons who have held one of the positions listed in subpara. 1 in the last two years;
3. persons who may not be elected to the National Council.

(4) The head of the Data Protection Authority shall be dismissed by the Federal President on the basis of a proposal by the Federal Government.

(5) The deputy head of the Data Protection Authority is appointed for a term of five years by the Federal President on the basis of a proposal by the Federal Government in accordance with paras. 1 to 3. Para. 4 applies to the dismissal of the deputy.

Tasks

§ 21. (1) At their request, the Data Protection Authority advises the committees of the National Council and the Federal Council, the Federal Government and the provincial governments on legislative and administrative measures. Before federal laws as well as regulations to be implemented by the Federal Government that directly concern issues of data protection law are adopted, the Federal Data Protection Authority shall be consulted.

(2) The Data Protection Authority shall make public, by way of a regulation in the Federal Law Gazette, the lists pursuant to Article 35 paras. 4 and 5 of the General Data Protection Regulation.

(3) The Data Protection Authority shall make public, by way of a regulation, the criteria to be specified pursuant to Article 57 para. 1 (p) of the General Data Protection Regulation. At the same time, the Data Protection Authority shall serve as the only national accreditation body pursuant to Article 43 para. 1 (a) of the General Data Protection Regulation.

Powers

§ 22. (1) The Data Protection Authority can request from the controller or the processor of the examined processing all necessary clarifications and inspect data processing activities and relevant documents. The controller or processor shall render the necessary assistance. Supervisory activities are to be exercised in a way that least interferes with the rights of the controller or processor and third parties.

(2) For purposes of the inspection, the Data Protection Authority shall have

des Inhabers der Räumlichkeiten und des Verantwortlichen oder des Auftragsverarbeiters berechtigt, Räume, in welchen Datenverarbeitungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen.

(3) Informationen, die der Datenschutzbehörde oder den von ihr Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Im Übrigen besteht die Pflicht zur Verschwiegenheit auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, dass dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach § 63 dieses Bundesgesetzes oder nach §§ 118a, 119, 119a, 126a bis 126c, 148a oder § 278a des Strafgesetzbuches – StGB, BGBl. Nr. 60/1974, oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch Ersuchen nach § 76 der Strafprozeßordnung – StPO, BGBl. Nr. 631/1975, zu entsprechen ist.

(4) Liegt durch den Betrieb einer Datenverarbeitung eine wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen der betroffenen Personen (Gefahr im Verzug) vor, so kann die Datenschutzbehörde die Weiterführung der Datenverarbeitung mit Bescheid gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG, BGBl. Nr. 51/1991, untersagen. Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenverarbeitung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Ebenso kann die Datenschutzbehörde auf Antrag einer betroffenen Person eine Einschränkung der Verarbeitung nach Art. 18 DSGVO mit Bescheid gemäß § 57 Abs. 1 AVG anordnen, wenn der Verantwortliche einer diesbezüglichen Verpflichtung nicht fristgerecht nachkommt. Wird einer Untersagung nicht unverzüglich Folge geleistet, hat die Datenschutzbehörde nach Art. 83 Abs. 5 DSGVO vorzugehen.

(5) Der Datenschutzbehörde obliegt im Rahmen ihrer Zuständigkeit die Verhängung von Geldbußen gegenüber natürlichen und juristischen Personen.

(6) Bestehen im Zuge einer auf § 29 gestützten Klage einer betroffenen Person, die sich von einer Einrichtung, Organisation oder Vereinigung im Sinne des Art. 80 Abs. 1 DSGVO vertreten lässt, Zweifel am Vorliegen der diesbezüglichen Kriterien, trifft die Datenschutzbehörde auf Antrag des Einbringungsgerichtes entsprechende Feststellungen mit Bescheid. Diese Einrichtung, Organisation oder Vereinigung hat im Verfahren Parteistellung. Gegen einen negativen Feststellungsbescheid steht ihr die Beschwerde an das Bundesverwaltungsgericht offen.

Tätigkeitsbericht und Veröffentlichung von Entscheidungen

§ 23. (1) Die Datenschutzbehörde hat bis zum 31. März eines jeden Jahres einen dem Art. 59 DSGVO entsprechenden Tätigkeitsbericht zu erstellen und dem vorzulegen. Der Bericht ist vom Bundeskanzler der Bundesregierung, dem Nationalrat und dem Bundesrat vorzulegen. Die Datenschutzbehörde hat den Bericht der Öffentlichkeit, der Europäischen Kommission, dem Europäischen Datenschutzausschuss (Art. 68 DSGVO) und dem Datenschutzrat zugänglich zu machen.

(2) Entscheidungen der Datenschutzbehörde von grundsätzlicher Bedeutung für die Allgemeinheit sind von der Datenschutzbehörde unter Beachtung der Erfordernisse der Amtsverschwiegenheit in geeigneter Weise zu veröffentlichen.

3. Abschnitt

Rechtsbehelfe, Haftung und Sanktionen

Beschwerde an die Datenschutzbehörde

§ 24. (1) Jede betroffene Person hat das Recht auf Beschwerde bei der Datenschutzbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO oder gegen § 1 oder Artikel 2 1. Hauptstück verstößt.

(2) Die Beschwerde hat zu enthalten:

the right, after having informed the owner of the premises and the controller or processor, to enter rooms where data processing operations are carried out, put data processing equipment into operation, carry out the processing operations to be examined and make copies of the storage media to the extent strictly necessary to exercise its supervisory powers.

(3) Information acquired by the Data Protection Authority or persons authorised by it during any examination shall be used only for supervisory purposes in the context of the execution of data protection regulations. Incidentally, the obligation of confidentiality also exists before courts and administrative authorities, in particular fiscal authorities, with the reservation that, if the inspection leads to the suspicion that a crime pursuant to § 63 of this federal law or pursuant to § 118a, § 119, § 119a, § 126a to § 126c, § 148a or § 278a of the Criminal Code, Federal Law Gazette No 60/1974, or any crime punishable with more than five years of imprisonment has been committed, this shall be reported to the police, and requests pursuant to § 76 of the Code of Criminal Procedure, Federal Law Gazette No 631/1975, regarding such crimes and offences shall also be complied with.

(4) In case a data processing operation causes serious immediate danger to the interests of confidentiality of the data subject which deserve protection (imminent danger), the Data Protection Authority may prohibit the continuation of the data processing operation by an administrative decision pursuant to § 57 para. 1 of the General Administrative Procedure Act 1991, Federal Law Gazette No 51/1991. The continuation may also be prohibited only partially if this seems technically possible, meaningful with regard to the purpose of the data processing operation and sufficient to eliminate the danger. At the request of a data subject, the Data Protection Authority can also order, by an administrative decision pursuant to § 57 para. 1 of the General Administrative Procedure Act, the restriction of processing pursuant to Article 18 of the General Data Protection Regulation if the controller does not comply with an obligation to that effect within the period specified. If prohibition is not complied with immediately, the Data Protection Authority shall proceed pursuant to Article 83 para. 5 of the General Data Protection Regulation.

(5) As part of its responsibilities, the Data Protection Authority is responsible for imposing administrative fines on natural and legal persons.

(6) If, with regard to a claim based on § 29 by a data subject represented by a body, organisation or association as referred to in Article 80 para. 1 of the General Data Protection Regulation, there are doubts whether the relevant criteria have been met, the Data Protection Authority shall, at the request of the court where the claim is filed, make appropriate findings in an administrative decision. Such body, organisation or association shall have the position of a party in the proceedings. It has the right to lodge a complaint against a negative declaratory decision with the Federal Administrative Court.

Activity reports and the publication of decisions

§ 23. (1) The Data Protection Authority shall prepare an activity report complying with Article 59 of the General Data Protection Regulation by 31 March of every year and submit it to the Federal Chancellor. The Federal Chancellor shall submit the report to the Federal Government, the National Council and the Federal Council. The Data Protection Authority shall make the report accessible to the public, the European Commission, the European Data Protection Board (Article 68 of the General Data Protection Regulation) and the Data Protection Council.

(2) Decisions made by the Data Protection Authority which are of fundamental importance to the general public shall be published by the Data Protection Authority in an appropriate manner while respecting official secrecy rules.

Part 3

Remedies, liability and penalties

Complaints with the Data Protection Authority

§ 24. (1) Every data subject has the right to lodge a complaint with the Data Protection Authority if the data subject is of the opinion that the processing of the personal data concerning the data subject infringes the General Data Protection Regulation or § 1 or Chapter 1, Article 2.

(2) The complaint must contain:

1 die Bezeichnung des als verletzt erachteten Rechts,

2 soweit dies zumutbar ist, die Bezeichnung des Rechtstragers oder Organs, dem die behauptete Rechtsverletzung zugerechnet wird (Beschwerdegegner),

3 den Sachverhalt, aus dem die Rechtsverletzung abgeleitet wird,

4 die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stutzt,

5 das Begehren, die behauptete Rechtsverletzung festzustellen und

6 die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist

(3) Einer Beschwerde sind gegebenenfalls der zu Grunde liegende Antrag und eine allfällige Antwort des Beschwerdegegners anzuschließen Die Datenschutzbehorde hat im Falle einer Beschwerde auf Ersuchen der betroffenen Person weitere Unterstutzung zu leisten

(4) Der Anspruch auf Behandlung einer Beschwerde erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, langstens aber binnen drei Jahren, nachdem das Ereignis behaupteter Maßen stattgefunden hat, einbringt Verspatete Beschwerden sind zuruckzuweisen

(5) Soweit sich eine Beschwerde als berechtigt erweist, ist ihr Folge zu geben Ist eine Verletzung einem Verantwortlichen des privaten Bereichs zuzurechnen, so ist diesem aufzutragen, den Antragen des Beschwerdefuhrers auf Auskunft, Berichtigung, Loschung, Einschrankung oder Datenubertragung in jenem Umfang zu entsprechen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen Soweit sich die Beschwerde als nicht berechtigt erweist, ist sie abzuweisen

(6) Ein Beschwerdegegner kann bis zum Abschluss des Verfahrens vor der Datenschutzbehorde die behauptete Rechtsverletzung nachtraglich beseitigen, indem er den Antragen des Beschwerdefuhrers entspricht Erscheint der Datenschutzbehorde die Beschwerde insofern als gegenstandslos, so hat sie den Beschwerdefuhrer dazu zu horen Gleichzeitig ist er darauf aufmerksam zu machen, dass die Datenschutzbehorde das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begrundet, warum er die ursprunglich behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet Wird durch eine derartige Außerung des Beschwerdefuhrers die Sache ihrem Wesen nach geandert (§ 13 Abs 8 AVG), so ist von der Zurückziehung der ursprünglichen Beschwerde und der gleichzeitigen Einbringung einer neuen Beschwerde auszugehen Auch diesfalls ist das ursprüngliche Beschwerdeverfabren formlos einzustellen und der Beschwerdefuhrer davon zu verstandigen Verspatete Außerungen sind nicht zu berücksichtigen

(7) Der Beschwerdefuhrer wird von der Datenschutzbehorde innerhalb von drei Monaten ab Einbringung der Beschwerde über den Stand und das Ergebnis der Ermittlung unterrichtet

(8) Jede betroffene Person kann das Bundesverwaltungsgericht befassen, wenn die Datenschutzbehorde sich nicht mit der Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der erhobenen Beschwerde in Kenntnis gesetzt hat

(9) Die Datenschutzbehorde kann – soweit erforderlich – Amtssachverstandige im Verfahren beiziehen

(10) In die Entscheidungsfrist gemaß § 73 AVG werden nicht eingerechnet

1 die Zeit, wahrend deren das Verfahren bis zur rechtskraftigen Entscheidung einer Vorfrage ausgesetzt ist,

2 die Zeit wahrend eines Verfahrens nach Art 56, 60 und 63 DSGVO

Begleitende Maßnahmen im Beschwerdeverfahren

§ 25. (1) Macht der Beschwerdefuhrer im Rahmen einer Beschwerde eine wesentliche Beeintrachtigung seiner schutzwurdigen Geheimhaltungsinteressen durch die Verarbeitung seiner personenbezogenen Daten glaubhaft, kann die Datenschutzbehorde nach § 22 Abs 4 vorgehen

(2) Ist in einem Verfahren die Richtigkeit von personenbezogenen Daten strittig, so ist vom Beschwerdegegner bis zum Abschluss des Verfahrens ein Bestreitungsvermerk anzubringen Erforderlichenfalls hat dies die

1 the description of the right considered to have been infringed,

2 to the extent reasonable, the description of the legal entity or the executive body or officer that is deemed to be responsible for the alleged infringement (respondent to the complaint),

3 the facts from which the infringement is derived,

4 the reasons for which the unlawfulness is alleged,

5 the request to find that the alleged infringement has been committed, and

6 the details which are necessary in order to decide whether the complaint has been lodged in due time

(3) A complaint must be accompanied by the request on which it is based and the answer of the respondent to the complaint, if any In the case of a complaint, the Data Protection Authority shall provide further assistance on request of the data subject

(4) The right to have a complaint dealt with expires if the intervening party does not lodge the complaint within a year after having gained knowledge of the incident that gave rise to the complaint, but no later than within three years after the incident allegedly occurred Late complaints shall be rejected

(5) To the extent the complaint is shown to be justified, it is to be granted If an infringement can be attributed to a private-sector controller, the controller shall be instructed to comply with the complainant's requests for information, rectification, erasure, restriction or data communication to the extent required to eliminate the infringement that has been found to exist To the extent that the complaint is not found to be justified, it shall be rejected

(6) A respondent to the complaint can subsequently eliminate the alleged infringement until the end of the proceedings before the Data Protection Authority by complying with the complainant's requests If the Data Protection Authority deems the complaint to be settled thereby, it shall hear the complainant on this Simultaneously, the complainant is to be informed that the Data Protection Authority will informally end the proceedings unless the complainant states reasons, within a reasonable period, why the complainant still considers the originally alleged infringement or at least parts of it as not having been eliminated If such a statement by the complainant modifies the merits of the case (§ 13 para 8 of the General Administrative Procedure Act), the original complaint is to be deemed withdrawn and simultaneously a new complaint to be deemed lodged In this case the original complaint procedure is also to be ended informally and the complainant is to be informed thereof Late statements are to be ignored

(7) The data subject shall be informed by the Data Protection Authority of the progress and the outcome of the investigation within three months of filing the complaint

(8) Each data subject can apply to the Federal Administrative Court if the Data Protection Authority does not handle a complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged

(9) To the extent required, the Data Protection Authority can engage official experts to assist in the proceedings

(10) The term allowed for the decision pursuant to § 73 of the General Administrative Procedure Act shall not include

1 the time during which proceedings are suspended until a final decision on a preliminary issue has been made,

2 the duration of proceedings pursuant to Articles 56, 60 and 63 of the General Data Protection Regulation

Accompanying measures in the complaint procedure

§ 25. (1) If, in the context of a complaint, the complainant satisfactorily demonstrates a serious infringement of his or her interests in confidentiality which deserve protection due to the processing of the complainant's personal data, the Data Protection Authority may proceed according to § 22 para 4

(2) If the correctness of personal data is disputed in proceedings, the respondent to the complaint shall submit, by the end of the proceedings, a note stating that the correctness is disputed If required, the Data Protection Authority

Datenschutzbehörde auf Antrag des Beschwerdeführers mit Bescheid gemaß § 57 Abs. 1 AVG anzuordnen.

(3) Beruft sich ein Verantwortlicher gegenüber der Datenschutzbehörde auf eine Beschränkung im Sinne des Art. 23 DSGVO, so hat diese die Rechtmäßigkeit der Anwendung der Beschränkungen zu überprüfen. Kommt sie zur Auffassung, dass die Geheimhaltung von verarbeiteten personenbezogenen Daten gegenüber der betroffenen Person nicht gerechtfertigt war, ist die Offenlegung der personenbezogenen Daten mit Bescheid aufzutragen. Wird dem Bescheid der Datenschutzbehörde binnen acht Wochen nicht entsprochen, so hat die Datenschutzbehörde die Offenlegung der personenbezogenen Daten gegenüber der betroffenen Person selbst vorzunehmen und ihr die verlangte Auskunft zu erteilen oder ihr mitzuteilen, welche personenbezogenen Daten bereits berichtigt oder gelöscht wurden.

(4) Bescheide, mit denen Übermittlungen von personenbezogenen Daten ins Ausland genehmigt wurden, sind zu widerrufen, wenn die rechtlichen oder tatsächlichen Voraussetzungen für die Erteilung der Genehmigung nicht mehr bestehen.

Verantwortliche des öffentlichen und des privaten Bereichs

§ 26. (1) Verantwortliche des öffentlichen Bereichs alle,

1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder
2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

(2) Verantwortliche des öffentlichen Bereichs sind Partei in Verfahren vor der Datenschutzbehörde.

(3) Verantwortliche des öffentlichen Bereichs können Beschwerde an das Bundesverwaltungsgericht und Revision beim Verwaltungsgerichtshof erheben.

(4) Die dem Abs. 1 nicht unterliegenden Verantwortlichen gelten als Verantwortliche des privaten Bereichs im Sinne dieses Bundesgesetzes.

Beschwerde an das Bundesverwaltungsgericht

§ 27. (1) Das Bundesverwaltungsgericht entscheidet durch Senat über Beschwerden gegen Bescheide, wegen der Verletzung der Unterrichtungspflicht gemäß § 24 Abs. 7 und der Entscheidungspflicht der Datenschutzbehörde.

(2) Der Senat besteht aus einem Vorsitzenden und je einem fachkundigen Laienrichter aus dem Kreis der Arbeitgeber und aus dem Kreis der Arbeitnehmer. Die fachkundigen Laienrichter werden auf Vorschlag der Wirtschaftskammer Österreich und der Bundeskammer für Arbeiter und Angestellte bestellt. Es sind entsprechende Vorkehrungen zu treffen, dass zeitgerecht eine hinreichende Anzahl von fachkundigen Laienrichtern zur Verfügung steht.

(3) Die fachkundigen Laienrichter müssen eine mindestens fünfjährige einschlägige Berufserfahrung und besondere Kenntnisse des Datenschutzrechtes besitzen

(4) Der Vorsitzende hat den fachkundigen Laienrichtern alle entscheidungsrelevanten Dokumente unverzüglich zu übermitteln oder, wenn dies untunlich oder zur Wahrung der Vertraulichkeit von Dokumenten unbedingt erforderlich ist, zur Verfügung zu stellen.

(5) Kommt es zu einem Verfahren gegen den Bescheid der Datenschutzbehörde, der eine Stellungnahme oder ein Beschluss des Europäischen Ausschusses im Rahmen des Kohärenzverfahrens vorangegangen ist, so leitet die Datenschutzbehörde diese Stellungnahme oder diesen Beschluss dem Bundesverwaltungsgericht zu.

Vertretung von betroffenen Personen

§ 28. Die betroffene Person hat das Recht, eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen in ihrem Namen die in den §§ 24 bis 27 genannten Rechte wahrzunehmen.

Haftung und Recht auf Schadenersatz

shall order, by an administrative decision pursuant to § 57 para. 1 of the General Administrative Procedure Act, such note to be submitted at the request of the complainant.

(3) If a controller invokes a restriction pursuant to Article 23 of the General Data Protection Regulation in relation to the Data Protection Authority, the Data Protection Authority shall examine the lawfulness of the application of the restrictions. If the Data Protection Authority comes to the conclusion that it was not justified in keeping the processed personal data secret from the data subject, the disclosure of the data shall be ordered by an administrative decision. If the administrative decision by the Data Protection Authority is not complied with within eight weeks, the Data Protection Authority shall disclose the personal data to the data subject and shall communicate to the data subject the desired information or inform the data subject of the personal data that have already been rectified or erased.

(4) Administrative decisions that permit the transfer of data abroad shall be revoked once the legal or factual prerequisites for the issue of the permit no longer apply.

Public-sector and private-sector controllers

§ 26. (1) Public-sector controllers are all controllers

1. that are established in legal structures of public law, in particular also as an executive officer of a territorial authority, or
2. as far as they execute laws despite having been incorporated according to private law.

(2) Public-sector controllers have the status of a party in proceedings before the Data Protection Authority.

(3) Public-sector controllers can lodge complaints with the Federal Administrative Court and final complaints with the Supreme Administrative Court.

(4) Controllers which are not within the scope of para. 1 are considered to be private-sector controllers according to this federal law.

Complaints with the Federal Administrative Court

§ 27. (1) The Federal Administrative Court shall decide through a panel of judges on complaints against administrative decisions on the ground of a breach of the duty to provide information pursuant to § 24 para. 7 and the duty to reach a decision of the Data Protection Authority.

(2) The panel of judges shall consist of a chair and one expert lay judge each from among employers and from among employees. The expert lay judges shall be appointed on the basis of a proposal by the Austrian Federal Economic Chamber and the Federal Chamber of Labour. Appropriate arrangements shall be made so that a sufficient number of expert lay judges is available in due time.

(3) The expert lay judges must have at least five years of relevant professional experience and special knowledge of data protection law.

(4) The chair shall provide all documents relevant to the decision to the expert lay judges without delay, or, if this is impractical or strictly necessary to safeguard the confidentiality of the documents, make them available in some other way.

(5) Where proceedings are brought against an administrative decision of the Data Protection Authority which was preceded by an opinion or a decision of the European Data Protection Board in the consistency mechanism, the Data Protection Authority shall forward that opinion or decision to the Federal Administrative Court.

Representation of data subjects

§ 28. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in § 24 to § 27 on his or her behalf, and to exercise the right to receive compensation referred to in § 29 on his or her behalf.

Right to compensation and liability

§ 29. (1) Jede Person, der wegen eines Verstoßes gegen die DSGVO oder gegen § 1 oder Artikel 2 1. Hauptstück ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter nach Art 82 DSGVO. Im Einzelnen gelten für diesen Schadenersatzanspruch die allgemeinen Bestimmungen des bürgerlichen Rechts

(2) Für Klagen auf Schadenersatz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Kläger (Antragsteller) seinen gewohnlichen Aufenthalt oder Sitz hat. Klagen (Anträge) konnen aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewohnlichen Aufenthalt oder Sitz oder eine Niederlassung hat.

Allgemeine Bedingungen für die Verhängung von Geldbußen

§ 30. (1) Die Datenschutzbehorde kann Geldbußen gegen eine juristische Person verhangen, wenn Verstoße gegen Bestimmungen der DSGVO und des § 1 oder Artikel 2 1. Hauptstück durch Personen begangen wurden, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt haben und eine Führungsposition innerhalb der juristischen Person aufgrund

1. der Befugnis zur Vertretung der juristischen Person,
2. der Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder
3. einer Kontrollbefugnis innerhalb der juristischen Person

innehaben.

(2) Juristische Personen konnen wegen Verstoßen gegen Bestimmungen der DSGVO und des § 1 oder Artikel 2 1. Hauptstück auch verantwortlich gemacht werden, wenn mangelnde Überwachung oder Kontrolle durch eine in Abs. 1 genannte Person die Begehung dieser Verstoße durch eine für die juristische Person tätige Person ermoglicht hat, sofern die Tat nicht den Tatbestand einer in die Zustandigkeit der Gerichte fallenden strafbaren Handlung bildet.

(3) Die Datenschutzbehorde hat von der Bestrafung eines Verantwortlichen gemäß § 9 des Verwaltungsstrafgesetzes 1991 – VStG, BGBl. Nr 52/1991, abzusehen, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird

(4) Die gemäß § 22 Abs 5 verhängten Geldbußen fließen dem Bund zu und sind nach den Bestimmungen über die Eintreibung von gerichtlichen Geldstrafen einzubringen Rechtskräftige Bescheide der Datenschutzbehorde sind Exekutionstitel Die Bewilligung und der Vollzug der Exekution ist auf Grund des Exekutionstitels der Datenschutzbehorde bei dem Bezirksgericht, in dessen Sprengel der Verpflichtete seinen allgemeinen Gerichtsstand in Streitsachen hat (§§ 66, 75 der Jurisdiktionsnorm – JN, RGBl Nr. 111/1895), oder bei dem in den §§ 18 und 19 EO bezeichneten Exekutionsgericht zu beantragen.

(5) Gegen Behorden und offentliche Stellen konnen keine Geldbußen verhangt werden.

4. Abschnitt

Aufsichtsbehörde nach der Richtlinie (EU) 2016/680

Datenschutzbehörde

§ 31. (1) Die Datenschutzbehorde wird als nationale Aufsichtsbehorde für den in § 36 Abs 1 genannten Anwendungsbereich eingerichtet. Die Datenschutzbehorde ist nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

(2) Hinsichtlich der Unabhängigkeit, der allgemeinen Bedingungen und der Errichtung der Aufsichtsbehorde finden die Art 52, 53 und 54 DSGVO sowie der § 18 Abs. 2, §§ 19 und 20 sinngemäß Anwendung

Aufgaben der Datenschutzbehörde

§ 32. (1) Die Datenschutzbehorde hat im Anwendungsbereich des § 36 Abs 1

1 die Anwendung des § 1 und der im 3. Hauptstück erlassenen Vorschriften sowie Durchführungsvorschriften zur Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behorden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der

§ 29. (1) Pursuant to Article 82 of the General Data Protection Regulation, any person who has suffered material or non-material damage as a result of an infringement of the General Data Protection Regulation or § 1 or Chapter 1 Article 2 shall have the right to receive compensation from the controller or processor for the damage suffered In detail, the general provisions of civil law shall apply to this right to compensation.

(2) The regional court entrusted with exercising jurisdiction in civil matters in whose judicial district the plaintiff (applicant) has his usual place of residence or registered office shall have first-instance jurisdiction over actions for compensation Actions (requests) may, however, also be brought before the regional court in whose judicial district the defendant has his usual place of residence or registered office or a branch office.

General conditions for imposing administrative fines

§ 30. (1) The Data Protection Authority can impose administrative fines on a legal person if infringements of provisions of the General Data Protection Regulation and of § 1 or Chapter 1 Article 2 were committed by persons who acted either individually or as part of an executive body of the legal person and have a leading position within the legal person on the basis of.

1 a power of representation of the legal person,
2. the authority to take decisions on behalf of the legal person, or
3. the authority to exercise control within the legal person

(2) Legal persons may also be held responsible for infringements of provisions of the General Data Protection Regulation and of § 1 or Chapter 1 Article 2 if such infringements by a person acting for the legal person were made possible by a lack of supervision or control by one of the persons referred to in para. 1 unless the act constitutes a criminal offence within the jurisdiction of the courts

(3) The Data Protection Authority shall refrain from imposing a fine on a responsible party pursuant to § 9 of the Administrative Penal Act 1991, Federal Law Gazette 52/1991, if an administrative penalty has already been imposed on the legal person for the same infringement and there are no particular circumstances opposing the refraining from imposing a fine

(4) Administrative fines imposed pursuant to § 22 para. 5 shall be received by the Federal Government and shall be collected pursuant to the provisions on the collection of judicial fines. Final administrative decisions by the Data Protection Authority are writs of enforcement. Approval and implementation of enforcement is to be requested on the basis of the writ of enforcement by the Data Protection Authority from the district court in whose judicial district the obligated party has his or her general place of jurisdiction (§ 66 and § 75 of the Court Jurisdiction Act, Imperial Law Gazette No 111/1895) or from the enforcing court referred to in § 18 and § 19 of the Enforcement Code.

(5) Administrative fines cannot be imposed on authorities and public entities

Part 4

Supervisory authority pursuant to Directive (EU) 2016/680

Data Protection Authority

§ 31. (1) The Data Protection Authority is established as a national supervisory authority for the scope referred to in § 36 para. 1. The Data Protection Authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.

(2) In respect of independence, general provisions and the establishment of the supervisory authority, Articles 52, 53 and 54 of the General Data Protection Regulation and § 18 para. 2, § 19 and § 20 shall apply accordingly.

Tasks of the Data Protection Authority

§ 32. (1) In the scope of § 36 para. 1, the Data Protection Authority shall

1 monitor and enforce the application of § 1 and of the provisions adopted pursuant to Chapter 3 and the implementing measures regarding Directive (EU) 2016/680 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

Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. Nr. L 119 vom 4.5.2016 S. 89, zu überwachen und durchzusetzen;

2. die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung zu sensibilisieren und sie darüber aufzuklären;

3. die in Art. 57 Abs. 1 lit. c bis e, g, h und t DSGVO festgelegten Aufgaben im Hinblick auf das 3. Hauptstück zu erfüllen;

4. sich mit Beschwerden einer betroffenen Person oder einer Stelle, einer Organisation oder einer Vereinigung gemäß § 28 zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer Frist von drei Monaten über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;

5. die Rechtmäßigkeit der Verarbeitung gemäß § 42 Abs. 8 zu überprüfen und die betroffene Person innerhalb einer angemessenen Frist über das Ergebnis der Überprüfung gemäß § 42 Abs. 9 zu unterrichten oder ihr die Gründe mitzuteilen, aus denen die Überprüfung nicht vorgenommen wurde;

6. maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie,

7. Beratung in Bezug auf die in § 53 genannten Verarbeitungsvorgänge zu leisten, und

8. die Rechte der betroffenen Person in den Fällen der §§ 43 Abs. 4, 44 Abs. 3 und 45 Abs. 4 auszuüben.

(2) Die Datenschutzbehörde erleichtert das Einreichen von in Abs. 1 Z 4 genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(3) Art. 57 Abs. 3 und 4 DSGVO finden sinngemäß Anwendung.

Befugnisse der Datenschutzbehörde

§ 33. (1) Die Datenschutzbehörde verfügt im Anwendungsbereich des § 36 Abs. 1 über die zur Vollziehung ihres Aufgabenbereichs erforderlichen wirksamen Untersuchungsbefugnisse. Diese umfassen insbesondere die in § 22 Abs. 2 genannten Befugnisse.

(2) Die Datenschutzbehörde verfügt im Anwendungsbereich des § 36 Abs. 1 über die zur Vollziehung ihres Aufgabenbereichs erforderlichen wirksamen Abhilfebefugnisse. Dazu zählen jedenfalls die Befugnisse, die es ihr gestatten

1. einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die im Anwendungsbereich der Richtlinie (EU) 2016/680 erlassenen Vorschriften verstoßen;

2. den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge, auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den im Anwendungsbereich der Richtlinie (EU) 2016/680 erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung gemäß § 45;

3. eine vorübergebende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen.

(3) Die Datenschutzbehörde verfügt im Anwendungsbereich des § 36 Abs. 1 über die zur Vollziehung erforderlichen wirksamen Beratungsbefugnisse, die es ihr gestatten, gemäß dem Verfahren der vorherigen Konsultation nach § 53 den Verantwortlichen zu beraten und zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Antrag Stellungnahmen an den Nationalrat oder den Bundesrat, die Bundes- oder Landesregierung oder an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten.

(4) Die Ausübung der der Aufsichtsbehörde übertragenen Befugnisse richtet sich im Anwendungsbereich § 36 Abs. 1 sinngemäß nach Art. 58 Abs. 4 DSGVO.

or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ No L 119 of 4 May 2016, p. 89;

2. promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;

3. perform the tasks specified in Article 57 para. 1 (c) to (e), (g), (h) and (t) of the General Data Protection Regulation with regard to Chapter 3;

4. deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with § 28, 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 period of three months, in particular if further investigation or coordination with another supervisory authority is necessary;

5. check the lawfulness of processing pursuant to § 42 para. 8, and inform the data subject within a reasonable period of the outcome of the check pursuant to § 42 para. 9 or of the reasons why the check has not been carried out;

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

7. provide advice on the processing operations referred to in § 53; and

8. exercise the rights of data subjects in the cases referred to in § 43 para. 4, § 44 para. 3 and § 45 para. 4.

(2) The Data Protection Authority shall facilitate the submission of complaints referred to in para. 1 subpara. 4 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

(3) Article 57 paras. 3 and 4 of the General Data Protection Regulation shall apply accordingly.

Powers of the Data Protection Authority

§ 33. (1) In the scope of § 36 para. 1, the Data Protection Authority shall have the effective investigative powers required to perform its tasks. Such powers include, in particular, the powers referred to in § 22 para. 2.

(2) In the scope of § 36 para. 1, the Data Protection Authority shall have the effective corrective powers required to perform its tasks. These include the powers to enable the Data Protection Authority

1. to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions adopted in the scope of Directive (EU) 2016/680;

2. to order the controller or processor to bring processing operations into compliance with the provisions adopted in the scope of Directive (EU) 2016/680 in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data or the restriction of processing pursuant to § 45;

3. to impose a temporary or definitive limitation including a ban on processing.

(3) In the scope of § 36 para. 1, the Data Protection Authority has effective advisory powers required for implementation which allow it to advise the controller in accordance with the prior consultation procedure referred to in § 53 and to issue, on its own initiative or on request, opinions to the National Council or the Federal Council, the Federal Government or a provincial government or to other institutions and bodies as well as to the public on any issue related to the protection of personal data.

(4) In the scope of § 36 para. 1, the exercise of the powers conferred on the supervisory authority is based on Article 58 para. 4 of the General Data Protection Regulation.

(5) § 22 Abs 3 2. Satz gilt sinngemäß für Verstoße im Anwendungsbereich des § 36 Abs. 1.

Allgemeine Bestimmungen

§ 34. (1) Verantwortliche haben im Anwendungsbereich des § 36 Abs. 1 wirksame Vorkehrungen zu treffen, um vertrauliche Meldungen über Verstoße zu fördern. In diesem Sinne haben Verantwortliche insbesondere angemessene Verfahren einzurichten, die es ermöglichen, Verstoße gegen die Bestimmungen des 3. Hauptstücks an eine geeignete Stelle zu melden.

(2) Die in Abs. 1 angeführten Vorkehrungen umfassen zumindest

1. spezielle Verfahren für den Empfang der Meldungen über Verstoße und deren Weiterverfolgung,
2. den Schutz personenbezogener Daten sowohl für die Person, die die Verstoße anzeigt, als auch für die natürliche Person, die mutmaßlich für einen Verstoß verantwortlich ist;
3. klare Regeln, welche die Geheimhaltung der Identität der Person, die die Verstoße anzeigt, gewährleisten, soweit nicht die Offenlegung der Identität im Rahmen eines staatsanwaltschaftlichen, gerichtlichen oder verwaltungsrechtlichen Verfahrens zwingend zu erfolgen hat.

(3) Die Datenschutzbehörde hat im Rahmen des Tätigkeitsberichtes nach § 23 über die Tätigkeiten nach dem 4. und 5. Abschnitt zu berichten. Die Vorgaben des Art 59 DSGVO und § 23 für den Tätigkeitsbericht und die Veröffentlichung von Entscheidungen finden sinngemäß Anwendung.

(4) Auf die gegenseitige Amtshilfe im Anwendungsbereich des § 36 Abs. 1 findet Art 61 Abs. 1 bis 7 DSGVO sinngemäß Anwendung.

(5) Im Anwendungsbereich des § 36 Abs. 1 finden die Regelungen des 3. Abschnitts des 2 Hauptstücks – mit Ausnahme des § 30 – sinngemäß Anwendung.

5. Abschnitt

Besondere Befugnisse der Datenschutzbehörde

§ 35. (1) Die Datenschutzbehörde ist nach den näheren Bestimmungen der DSGVO und dieses Bundesgesetzes zur Wahrung des Datenschutzes berufen.

(2) **(Verfassungsbestimmung)** Die Datenschutzbehörde übt ihre Befugnisse auch gegenüber den in Art 19 B-VG bezeichneten obersten Organen der Vollziehung

3. Hauptstück

Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs

1. Abschnitt

Allgemeine Bestimmungen

Anwendungsbereich und Begriffsbestimmungen

§ 36. (1) Die Bestimmungen dieses Hauptstücks gelten für die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der Eigensicherung.

(2) Im Sinne dieses Hauptstücks bezeichnet der Ausdruck:

1. „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen,

(5) § 22 para. 3 sentence 2 shall apply accordingly to infringements in the scope of § 36 para 1

General provisions

§ 34. (1) In the scope of § 36 para. 1, controllers shall put in place effective mechanisms to encourage confidential reporting of infringements. For this purpose, controllers shall, in particular, establish adequate procedures that enable reports of infringements of the provisions of Chapter 3 to an appropriate entity.

(2) The mechanisms referred to in para. 1 shall at least include

1. specific procedures for the receipt of reports on infringements and their follow-up;
2. protection of personal data concerning both the person who reports the infringements and the natural person who is presumably responsible for an infringement;
3 clear rules to guarantee that the identity of the person who reported the infringement is not disclosed, unless such disclosure of identity is obligatory in relation to public prosecution, court or administrative proceedings.

(3) In its activity report pursuant to § 23, the Data Protection Authority shall report on its activities pursuant to Parts 4 and 5. The requirements of Article 59 of the General Data Protection Regulation and § 23 for the activity report and the publication of decisions shall apply accordingly.

(4) Article 61 paras. 1 to 7 of the General Data Protection Regulation shall apply accordingly to mutual assistance in the scope of § 36 para. 1.

(5) In the scope of § 36 para. 1, the provisions of Chapter 2 Part 3, with the exception of § 30, shall apply accordingly.

Part 5

Special powers of the Data Protection Authority

§ 35. (1) The Data Protection Authority shall safeguard data protection in accordance with the detailed provisions of the General Data Protection Regulation and this federal law.

(2) **(Constitutional provision)** The Data Protection Authority shall exercise its powers also in relation to the highest governing bodies or officers referred to in Article 19 of the Federal Constitutional Law.

Chapter 3

Processing of personal data for purposes of the security police, including the protection of public security by the police, the protection of military facilities by the armed forces, the resolution and prosecution of criminal offences, the enforcement of sentences and the enforcement of precautionary measures involving the deprivation of liberty

Part 1

General provisions

Scope of application, and definitions

§ 36. (1) The provisions of this Chapter apply 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, including the safeguarding against and the prevention of threats to public security, and for the purposes of national security, intelligence, and the protection of military facilities by the armed forces.

(2) For the purposes of this Chapter:

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 natural person;

genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann,

2. „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung,

3 „Einschränkung der Verarbeitung" die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen,

5. „Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

6. „Dateisystem" jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird,

7. „zuständige Behörde"

a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist, oder

b) eine andere Stelle oder Einrichtung, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, übertragen wurde;

8 „Verantwortlicher" die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet,

9. „Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

10 „Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags aufgrund von Gesetzen möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung,

11 „Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

12 „genetische Daten" personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden,

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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or 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 consisting of 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. "pseudonymisation" means the processing of personal data in such a manner that the personal 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 organisational measures to ensure that the personal data are not 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 centralised, decentralised or dispersed on a functional or geographical basis;

7. "competent authority" means

a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

8 "controller" means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data;

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

10 "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 laws 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;

11 "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

12. "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;

13. „biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

14. „Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

15. „Aufsichtsbehörde" ist die Datenschutzbehörde;

16. „internationale Organisation" eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

Grundsätze für die Datenverarbeitung, Kategorisierung und Datenqualität

§ 37. (1) Personenbezogene Daten

1. müssen auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,

2. müssen für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,

3. müssen dem Verarbeitungszweck entsprechen und müssen maßgeblich sein und dürfen in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sein,

4. müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,

5. dürfen nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht,

6. müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

(2) Für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke im Anwendungsbereich des § 36 Abs. 1 gilt § 38.

(3) Der Verantwortliche ist für die Einhaltung der Abs. 1 und 2 verantwortlich und muss deren Einhaltung nachweisen können.

(4) Soweit möglich und zumutbar, ist zwischen den personenbezogenen Daten insbesondere folgender Kategorien betroffener Personen zu unterscheiden:

1. Personen, die aufgrund bestimmter Tatsachen konkret verdächtig sind, eine strafbare Handlung begangen zu haben,

2. Personen, gegen die aufgrund bestimmter Tatsachen der begründete Verdacht besteht, dass sie in naher Zukunft eine strafbare Handlung begehen werden,

3. verurteilte Straftäter,

4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie Opfer einer Straftat sind, und

5. sonstige Personen, die im Zusammenhang mit einer Straftat stehen, insbesondere Personen, die als Zeugen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit den in Z 1 bis 3 genannten Personen in Kontakt oder in Verbindung stehen.

(5) Soweit möglich ist zwischen faktenbasierten und auf persönlichen Einschätzungen beruhenden personenbezogenen Daten zu unterscheiden. Auf persönlichen Einschätzungen beruhende personenbezogene Daten sind entsprechend zu kennzeichnen und können mit einer Begründung versehen werden, welche die Nachvollziehbarkeit der Einschätzung ermöglicht.

(6) Unrichtige, unvollständige, nicht mehr aktuelle oder zu löschende personenbezogene Daten dürfen weder übermittelt noch zum automatisierten Abruf aus Dateisystemen bereitgestellt werden. Die Behörde hat zu diesem Zweck

13. "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, such as facial images or dactyloscopic data;

14. "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;

15. "supervisory authority" means the Data Protection Authority;

16. "international organisation" means an organisation 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.

Principles for processing, classification and data quality

§ 37. (1) Personal data shall be.

1. processed lawfully and fairly;

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

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

4. 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;

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

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

(2) § 38 shall apply to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in the scope of § 36 para. 1.

(3) The controller shall be responsible for, and be able to demonstrate compliance with, paras. 1 and 2.

(4) As far as possible and reasonable, a clear distinction between personal data of different categories of data subjects, such as the following, shall be made:

1. persons who, on the basis of certain facts, are specifically suspected of having committed a criminal offence,

2. persons with regard to whom, on the basis of certain facts, 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 give rise to reasons for believing that they are the victims of a criminal offence, and

5. other persons connected to a criminal offence, such as persons who might be called on to testify, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in subparas. 1 to 3.

(5) Personal data based on facts are to be distinguished, as far as possible, from personal data based on personal assessments. Personal data based on personal assessments must be marked accordingly, and reasons can be added to facilitate the understanding of an assessment.

(6) Incorrect or incomplete personal data, personal data that are no longer current or are to be erased must neither be transferred nor made available for automated retrieval from filing systems. For that purpose, the authority shall check

vor einer Übermittlung die Datenqualität soweit möglich entsprechend zu überprüfen. Zum automatisierten Abruf bereit gehaltene personenbezogene Daten sind entsprechend laufend vollständig und aktuell zu halten.

(7) Bei jeder Übermittlung personenbezogener Daten sind soweit möglich die zur Beurteilung der Aktualität, Richtigkeit, Vollständigkeit und Zuverlässigkeit der personenbezogenen Daten durch den Empfänger erforderlichen Informationen beizufügen.

(8) Wird von Amts wegen oder infolge einer Mitteilung eines Betroffenen festgestellt, dass personenbezogene Daten übermittelt worden sind, die nicht den Anforderungen nach Abs. 6 entsprechen, teilt die übermittelnde bzw. dateisystemführende Dienststelle und Behörde dies der empfangenden Stelle oder Behörde unverzüglich mit Letztere hat unverzüglich die Löschung unrechtmäßig übermittelter Daten, die Berichtigung unrichtiger Daten, die Ergänzung unvollständiger Daten oder eine Einschränkung der Verarbeitung vorzunehmen.

(9) Hat die empfangende Dienststelle oder Behörde Grund zur Annahme, dass übermittelte personenbezogene Daten unrichtig oder nicht aktuell sind oder zu löschen oder in der Verarbeitung einzuschränken wären, so unterrichtet sie die übermittelnde Dienststelle oder Behörde unverzüglich hierüber. Letztere ergreift unverzüglich die erforderlichen Maßnahmen.

Rechtmäßigkeit der Verarbeitung

§ 38. Die Verarbeitung personenbezogener Daten ist, soweit sie nicht zur Wahrung lebenswichtiger Interessen einer Person erforderlich ist, nur rechtmäßig, soweit sie gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, vorgesehen und für die Erfüllung einer Aufgabe erforderlich und verhältnismäßig ist, die von der zuständigen Behörde zu den in § 36 Abs. 1 genannten Zwecken wahrgenommen wird.

Verarbeitung besonderer Kategorien personenbezogener Daten

§ 39. Die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person für die in § 36 Abs. 1 genannten Zwecke ist nur zulässig, wenn die Verarbeitung unbedingt erforderlich ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden und

1. die Verarbeitung gemäß § 38 zulässig ist oder
2. sie sich auf Daten bezieht, die die betroffene Person offensichtlich selbst öffentlich gemacht hat.

Verarbeitung für andere Zwecke und Übermittlung

§ 40. (1) Eine Verarbeitung von personenbezogenen Daten nach den Bestimmungen dieses Hauptstücks durch denselben oder einen anderen Verantwortlichen für einen anderen Verarbeitungszweck, als jenen, für den sie erhoben wurden, ist nur zulässig, wenn dieser andere Zweck vom Anwendungsbereich des § 36 Abs. 1 umfasst ist und die Voraussetzungen der §§ 38 und 39 erfüllt sind.

(2) Die Übermittlung von nach den Bestimmungen dieses Hauptstücks verarbeiteten personenbezogenen Daten für einen nicht in § 36 Abs. 1 genannten Zweck ist nur zulässig, wenn dies gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, ausdrücklich vorgesehen ist und der Empfänger zur Verarbeitung dieser personenbezogenen Daten für diesen anderen Zweck befugt ist.

(3) Unterliegt die Verarbeitung von personenbezogenen Daten besonderen Bedingungen, so hat die übermittelnde zuständige Behörde den Empfänger der personenbezogenen Daten darauf hinzuweisen, dass diese Bedingungen gelten und einzuhalten sind. Die Übermittlung an Empfänger in anderen Mitgliedstaaten oder nach Titel V Kapitel 4 und 5 AEUV errichtete Einrichtungen und sonstige Stellen darf keinen Bedingungen unterworfen werden, die nicht auch für entsprechende Datenübermittlungen im Inland gelten.

Automatisierte Entscheidungsfindung im Einzelfall

§ 41. (1) Ausschließlich auf einer automatischen Verarbeitung beruhende

the data quality accordingly as far as possible before a transmission. Personal data kept ready for automated retrieval must be kept complete and up to date at all times.

(7) As far as possible, the information required for the recipient to assess the up-to-dateness, correctness, completeness and reliability of the personal data shall be added in any transmission of personal data.

(8) If it is found ex officio or following notification by a data subject that personal data that do not comply with the requirements of para. 6 have been transmitted, the transmitting administrative office and authority, or the administrative office and authority keeping the filing system shall notify the receiving office or authority thereof without delay. The receiving office or authority shall immediately erase data which have been unlawfully transmitted, rectify incorrect data, complete incomplete data or restrict processing without delay

(9) If the receiving administrative office or authority has reason to believe that the personal data transmitted are incorrect or not up to date or would have to be erased, or that their processing would have to be restricted, the receiving administrative office or authority shall notify the transmitting administrative office or authority thereof without delay. The latter shall take the required measures without delay.

Lawfulness of processing

§ 38. Unless it is required to protect the vital interests of a person, processing is lawful only to the extent it is provided for by laws or by directly applicable legal provisions that have the status of laws in Austria and is required and proportionate to fulfil a task performed by the competent authority for the purposes referred to in § 36 para. 1.

Processing of special categories of personal data

§ 39. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation for the purposes referred to in § 36 para. 1 shall be allowed only where strictly necessary and if effective measures to protect the rights and freedoms of the data subjects are taken and

1. where authorised pursuant to § 38, or
2. where such processing relates to data which are manifestly made public by the data subject.

Processing for other purposes, and transfer

§ 40. (1) Processing of personal data pursuant to the provisions of this Chapter by the same or another controller for a purpose other than the one for which the data were collected shall be allowed only if this other purpose is covered by the scope of § 36 para. 1 and the requirements of § 38 and § 39 are met.

(2) Transferring personal data processed pursuant to the provisions of this Chapter for a purpose not referred to in § 36 para. 1 shall be allowed only if this is expressly provided for by laws or by directly applicable legal provisions that have the status of laws in Austria, and the recipient is authorised to process these personal data for such other purpose.

(3) If the processing of personal data is subject to special conditions, the transmitting competent authority shall inform the recipient of the personal data that such conditions apply and must be complied with. Transfers to recipients in other Member States or to bodies, offices and agencies established pursuant to Title V Chapters 4 and 5 of the TFEU must not be subject to conditions that do not apply to domestic data transmissions as well.

Automated individual decision-making

§ 41. (1) Decisions based solely on automated processing, including profiling,

Entscheidungen einschließlich Profiling, die für die betroffene Person nachteilige Rechtsfolgen haben oder sie erheblich beeinträchtigen können, sind nur zulässig, soweit sie gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, ausdrücklich vorgesehen sind.

(2) Entscheidungen nach Abs. 1 dürfen nur auf besonderen Kategorien personenbezogener Daten nach § 39 beruhen, wenn und soweit wirksame Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

(3) Entscheidungen nach Abs. 1, die zur Folge haben, dass natürliche Personen auf Grundlage von personenbezogenen Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung diskriminiert werden, sind verboten.

2. Abschnitt
Rechte der betroffenen Person

Grundsätze

§ 42. (1) Der Verantwortliche hat der betroffenen Person alle Informationen und Mitteilungen gemäß §§ 43 bis 45, die sich auf die Verarbeitung beziehen, in möglichst präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die Informationen sind in geeigneter Form, im Falle eines Antrags nach Möglichkeit in der gleichen Form wie der Antrag, zu übermitteln.

(2) Der Verantwortliche hat den betroffenen Personen die Ausübung der ihnen gemäß §§ 43 bis 45 zustehenden Rechte zu erleichtern.

(3) Der Verantwortliche hat die betroffene Person unverzüglich schriftlich darüber in Kenntnis zu setzen, wie mit ihrem Antrag verfahren wurde.

(4) Der Verantwortliche stellt der betroffenen Person Informationen über die aufgrund eines Antrags gemäß §§ 44 bis 45 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(5) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(6) Informationen gemäß § 43 sowie alle Mitteilungen und Maßnahmen gemäß den §§ 44 und 45 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder

1. ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder
2. sich weigern, aufgrund des Antrags tätig zu werden.

Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(7) Der Verantwortliche kann zur Bestätigung der Identität der Person, die einen Antrag gemäß §§ 44 oder 45 gestellt hat, erforderliche zusätzliche Informationen verlangen.

(8) In den Fällen der §§ 43 Abs. 4, 44 Abs. 3 und 45 Abs. 4 ist die betroffene Person berechtigt, eine Überprüfung der Rechtmäßigkeit der bezüglichen Einschränkung ihrer Rechte durch die Datenschutzbehörde zu verlangen. Der Verantwortliche hat die betroffene Person über dieses Recht zu unterrichten.

which have negative legal consequences for the data subject or can significantly affect the data subject, shall be allowed only to the extent they are expressly provided for by laws or by directly applicable legal provisions that have the status of laws in Austria.

(2) Decisions referred to in para. 1 shall not be based on special categories of personal data referred to in § 39 unless effective measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

(3) Decisions pursuant to para. 1 that have the consequence that natural persons are discriminated against on the basis of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Part 2
Rights of the data subject

Principles

§ 42. (1) The controller shall provide any information and make any communication with regard to § 43 to § 45 relating to processing to the data subject in as concise, intelligible and easily accessible a form as possible, using clear and plain language. The information shall be transmitted in an appropriate manner, in the case of a request in the same form as the request, if possible.

(2) The controller shall facilitate the exercise of the rights of the data subject pursuant to § 43 to 45.

(3) The controller shall inform the data subject in writing about the follow-up to his or her request without undue delay.

(4) The controller shall provide the data subject with information on measures taken because of a request pursuant to § 44 to § 45 without delay, but in any event within one month after receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(5) If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

(6) Information provided under § 43 and any communication and any action taken under § 44 and 45 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

1. charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or
2. refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

(7) The controller may request the provision of additional information necessary to confirm the identity of the person who submitted a request pursuant to § 44 or § 45.

(8) In the cases referred to in § 43 para. 4, § 44 para. 3 and § 45 para. 4, the data subject is entitled to request verification of the lawfulness of the relevant restriction of the data subject's rights by the Data Protection Authority. The controller shall inform the data subject of this right.

(9) Wird das in Abs 8 genannte Recht ausgeübt, hat die Datenschutzbehörde die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen oder eine Überprüfung durch die Datenschutzbehörde erfolgt sind. Die Datenschutzbehörde hat zudem die betroffene Person über ihr Recht zu unterrichten, Beschwerde an das Bundesverwaltungsgericht zu erheben.

Information der betroffenen Person

§ 43. (1) Der Verantwortliche hat der betroffenen Person zumindest die folgenden Informationen zur Verfügung zu stellen:

1. den Namen und die Kontaktdaten des Verantwortlichen,
2. gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten,
3 die Zwecke, für die die personenbezogenen Daten verarbeitet werden,
4 das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,
5. das Bestehen eines Rechts auf Auskunft und Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung der personenbezogenen Daten der betroffenen Person durch den Verantwortlichen.

(2) Zusätzlich zu den in Abs. 1 genannten Informationen hat der Verantwortliche der betroffenen Person in besonderen Fällen die folgenden zusätzlichen Informationen zu erteilen, um die Ausübung der Rechte der betroffenen Person zu ermöglichen:

1 die Rechtsgrundlage der Verarbeitung,
2. die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
3. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten, auch der Empfänger in Drittländern oder in internationalen Organisationen,
4 erforderlichenfalls weitere Informationen, insbesondere wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben werden.

(3) Im Fall der Erhebung der personenbezogenen Daten bei der betroffenen Person müssen der betroffenen Person die Informationen nach den Vorgaben des Abs. 1 und 2 zum Zeitpunkt der Erhebung vorliegen. In allen übrigen Fällen findet Art. 14 Abs. 3 DSGVO Anwendung. Die Information gemäß Abs. 1 und 2 kann entfallen, wenn die Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Verantwortlichen oder aus Anwendungen anderer Verantwortlicher ermittelt und die Datenverarbeitung durch Gesetz vorgesehen ist.

(4) Die Unterrichtung der betroffenen Person gemäß Abs 2 kann soweit und solange aufgeschoben, eingeschränkt oder unterlassen werden, wie dies im Einzelfall unbedingt erforderlich und verhältnismäßig ist

1. zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden, insbesondere durch die Behinderung behördlicher oder gerichtlicher Untersuchungen, Ermittlungen oder Verfahren,
2. zum Schutz der öffentlichen Sicherheit,
3. zum Schutz der nationalen Sicherheit,
4. zum Schutz der verfassungsmäßigen Einrichtungen der Republik Österreich,
5 zum Schutz der militärischen Eigensicherung oder
6. zum Schutz der Rechte und Freiheiten anderer.

Auskunftsrecht der betroffenen Person

§ 44. (1) Jede betroffene Person hat das Recht, vom Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie das Recht, Auskunft über personenbezogene Daten und zu folgenden Informationen zu erhalten:

1. die Zwecke der Verarbeitung und deren Rechtsgrundlage,
2. die Kategorien personenbezogener Daten, die verarbeitet werden,
3. die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen,

(9) Where the right referred to in para. 8 is exercised, the Data Protection Authority shall inform the data subject at least that all necessary verifications or a review by the Data Protection Authority have taken place. In addition, the Data Protection Authority shall inform the data subject of the data subject's right to lodge complaints with the Federal Administrative Court.

Information of the data subject

§ 43. (1) The controller shall make available to the data subject at least the following information.

1. the identity and the contact details of the controller;
2. the contact details of the data protection officer, where applicable;
3. the purposes of the processing for which the personal data are intended;
4. the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority;
5. the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

(2) In addition to the information referred to in para. 1, the controller shall give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights:

1. the legal basis for the processing;
2. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,
3. where applicable, the categories of recipients of the personal data, including in third countries or international organisations;
4. where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

(3) Where personal data are collected from the data subject, the data subject must be in possession of the information pursuant to the requirements of paras. 1 and 2 at the time of the collection of the personal data. In all other cases, Article 14 para. 3 of the General Data Protection Regulation shall apply. The information according to paras. 1 and 2 may be omitted where data have not been collected by asking the data subject, but through transmission from another application purpose of the same controller or from a data application of another controller, and where the processing is provided for by law.

(4) The provision of the information to the data subject pursuant to para. 2 can be delayed, restricted or omitted to the extent this is strictly necessary and proportionate in a particular case to

1. avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, in particular by obstructing inquiries, investigations or proceedings of authorities or courts,
2. protect public security,
3. protect national security,
4. protect the constitutional institutions of the Republic of Austria,
5. enable the protection of military facilities by the armed forces, or
6. protect the rights and freedoms of others.

Right of access by the data subject

§ 44. (1) Every data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

1. the purposes of and legal basis for the processing,
2. the categories of personal data concerned,
3. the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations,

4. falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,

5. das Bestehen eines Rechts auf Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung personenbezogener Daten der betroffenen Person durch den Verantwortlichen,

6 das Bestehen eines Beschwerderechts bei der Datenschutzbehörde sowie deren Kontaktdaten und

7 Mitteilung zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten.

Einschränkungen des Auskunftsrechts sind nur unter den in § 43 Abs. 4 angeführten Voraussetzungen zulässig.

(3) Im Falle einer Nichterteilung der Auskunft gemäß Abs. 2 hat der Verantwortliche die betroffene Person unverzüglich schriftlich über die Verweigerung oder die Einschränkung der Auskunft und die Gründe hierfür zu unterrichten Dies gilt nicht, wenn die Erteilung dieser Informationen einem der in § 43 Abs 4 genannten Zwecke zuwiderliefe. Der Verantwortliche hat die betroffene Person über die Möglichkeit zu unterrichten, Beschwerde bei der Datenschutzbehörde einzulegen

(4) Der Verantwortliche hat die Gründe für die Entscheidung über die Nichterteilung der Auskunft gemäß Abs. 2 zu dokumentieren. Diese Angaben sind der Datenschutzbehörde zur Verfügung zu stellen.

(5) In dem Umfang, in dem eine Datenverarbeitung für eine betroffene Person hinsichtlich der zu ihr verarbeiteten Daten von Gesetzes wegen einsehbar ist, hat diese das Recht auf Auskunft nach Maßgabe der das Einsichtsrecht vorsehenden Bestimmungen. Für das Verfahren der Einsichtnahme (einschließlich deren Verweigerung) gelten die näheren Regelungen des Gesetzes, das das Einsichtsrecht vorsieht In Abs. 1 genannte Bestandteile einer Auskunft, die vom Einsichtsrecht nicht umfasst sind, können dennoch nach diesem Bundesgesetz geltend gemacht werden.

Recht auf Berichtigung oder Löschung personenbezogener Daten und auf Einschränkung der Verarbeitung

§ 45. (1) Jede betroffene Person hat das Recht, vom Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten sowie die Vervollständigung unvollständiger personenbezogener Daten zu verlangen. Die Berichtigung oder Vervollständigung kann erforderlichenfalls mittels einer ergänzenden Erklarung erfolgen, soweit eine nachträgliche Änderung mit dem Dokumentationszweck unvereinbar ist. Der Beweis der Richtigkeit der Daten obliegt dem Verantwortlichen, soweit die personenbezogenen Daten nicht ausschließlich aufgrund von Angaben der betroffenen Person ermittelt wurden.

(2) Der Verantwortliche hat personenbezogene Daten aus eigenem oder über Antrag der betroffenen Person unverzuglich zu löschen, wenn

1. die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind,

2. die personenbezogenen Daten unrechtmäßig verarbeitet wurden oder

3. die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist

(3) Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, oder

2 die personenbezogenen Daten für Beweiszwecke im Rahmen der Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe weiter aufbewahrt werden müssen.

Im Falle einer Einschränkung gemäß Z 1 hat der Verantwortliche die betroffene Person vor einer Aufhebung der Einschrankung zu unterrichten.

(4) Der Verantwortliche hat die betroffene Person schriftlich über eine Verweigerung der Berichtigung oder Löschung personenbezogener Daten oder eine Einschränkung der Verarbeitung und über die Gründe für die Verweigerung

4. if possible, the period for which the personal data are planned to be stored, or if that is not possible, the criteria used to determine that period,

5 the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject,

6 the right to lodge a complaint with the Data Protection Authority and the contact details of the Data Protection Authority, and

7. communication of the personal data undergoing processing and of any available information as to their origin.

(2) The periods pursuant to Article 12 of the General Data Protection Regulation shall apply to information pursuant to para. 1. Restrictions of the right of access are permitted only on the conditions referred to in § 43 para. 4

(3) In case access is not granted pursuant to para 2, the controller shall inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under § 43 para 4. The controller shall inform the data subject of the possibility to lodge a complaint with the Data Protection Authority

(4) The controller shall document the reasons for the decision not to grant access pursuant to para. 2. That information shall be made available to the Data Protection Authority.

(5) To the extent that a data processing operation is, by law, open to inspection by a data subject with regard to data processed on the data subject, the data subject shall have a right of access in accordance with the provisions granting the right of inspection. The detailed provisions of the law granting the right of inspection shall apply to the procedure of inspection (and its refusal) Parts of information according to para. 1 that are not covered by the right of inspection may, however, be asserted according to this federal law.

Right to rectification or erasure of personal data and to the restriction of processing

§ 45. (1) Every data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her and the completion of incomplete personal data. Where necessary, the personal data can be rectified or completed by means of a supplementary statement if later changes are incompatible with the documentation purpose. It shall be the obligation of the controller to prove that the data are correct unless the personal data have been collected exclusively based on statements made by the data subject.

(2) The controller shall erase the personal data on the controller's own initiative or at the request of the data subject if

1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed,

2. the personal data have been unlawfully processed,

3. erasure is necessary for compliance with a legal obligation to which the controller is subject.

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

1 the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained, or

2. the personal data must be maintained for the purposes of evidence to perform a task delegated to the controller by law

In the case of a restriction pursuant to subpara. 1, the controller shall inform the data subject before the restriction is lifted.

(4) The controller shall inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. The controller shall inform the data subject of the possibility to lodge a complaint with the Data Protection Authority

zu unterrichten. Der Verantwortliche hat die betroffene Person über die Möglichkeit zu unterrichten, bei der Datenschutzbehörde Beschwerde einzulegen.

(5) Der Verantwortliche hat die Berichtigung von unrichtigen personenbezogenen Daten der zuständigen Behörde, von der die unrichtigen personenbezogenen Daten stammen, mitzuteilen.

(6) In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung gemäß Abs. 1 bis 3 hat der Verantwortliche alle Empfänger der betroffenen personenbezogenen Daten in Kenntnis zu setzen. Die Empfänger sind verpflichtet, die ihrer Verantwortung unterliegenden personenbezogenen Daten unverzüglich zu berichtigen, löschen oder deren Verarbeitung einschränken.

(5) The controller sball communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate.

(6) Where personal data has been rectified or erased or processing has been restricted pursuant to paras. 1 to 3, the controller shall notify all recipients of the personal data concerned. The recipients shall rectify or erase the personal data or restrict processing of the personal data under their responsibility without undue delay.

(7) Article 12 of the General Data Protection Regulation shall apply accordingly.

3. Abschnitt
Verantwortlicher und Auftragsverarbeiter

Pflichten des Verantwortlichen

§ 46. Der Verantwortliche hat die in Art. 24 Abs. 1 und 2 sowie Art. 25 Abs. 1 und 2 DSGVO angeführten Verpflichtungen in Bezug auf die Übereinstimmung der Verarbeitung mit den Bestimmungen dieses Hauptstücks einzuhalten.

Gemeinsam Verantwortliche

§ 47. Zwei oder mehr Verantwortliche, die gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen, sind gemeinsam Verantwortliche. Sie haben in einer Vereinbarung in transparenter Form ihre jeweiligen Aufgaben nach diesem Bundesgesetz festzulegen, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß § 43 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht gesetzlich festgelegt sind. In der Vereinbarung ist eine Anlaufstelle für die betroffenen Personen anzugeben.

Auftragsverarbeiter und Aufsicht über die Verarbeitung

§ 48. (1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieses Bundesgesetzes erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen in Anspruch.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder aufgrund ausdrücklicher gesetzlicher Ermächtigung, der oder das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag oder dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

1. die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Unionsrecht oder durch Gesetze, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
2. gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
3. alle gemäß § 54 erforderlichen Maßnahmen ergreift;
4. die in den Abs. 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

Part 3
Controller and processor

Obligations of the controller

§ 46. The controller shall comply with the obligations referred to in Article 24 paras. 1 and 2 and Article 25 paras. 1 and 2 of the General Data Protection Regulation with regard to the compliance of processing with the provisions of this Chapter.

Joint controllers

§ 47. Two or more controllers who jointly determine the purposes and means of processing shall be joint controllers. They shall, in a transparent manner, determine their respective responsibilities under this federal law, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in § 43, by means of an arrangement between them if, and insofar as, the respective responsibilities of the controllers are not determined by law. The arrangement shall designate a contact point for data subjects.

Processor and the supervision of processing

§ 48. (1) Where processing is carried out on behalf of a controller, the controller shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this federal law and ensure the protection of the rights of the data subject.

(2) The processor shall not engage another processor without prior specific written authorisation of the controller.

(3) Processing by a processor shall be governed by a contract or other legal act under Union law or on the grounds of an explicit legal authorisation 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. This contract or other legal act shall stipulate, in particular, that the processor:

1. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union law or by laws to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
2. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
3. takes all measures necessary pursuant to § 54;
4. respects the conditions referred to in paras. 2 and 4 for engaging another processor;

5 angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in diesem Hauptstück genannten Rechte der betroffenen Person nachzukommen,

6 unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 52 bis 56 genannten Pflichten unterstützt,

7 nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder aufgrund von Gesetzen eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht,

8 dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Abs 1 bis 6 niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beitragt

Im Hinblick auf Z 8 informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen dieses Hauptstücks oder gegen andere Datenschutzbestimmungen der Union oder gesetzliche Datenschutzbestimmungen verstoßt

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder aufgrund von Gesetzen dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemaß Abs 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieses Hauptstücks erfolgt Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters

(5) Der Vertrag oder das andere Rechtsinstrument im Sinne der Abs 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann

(6) Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder aufgrund von Gesetzen zur Verarbeitung verpflichtet sind

(7) Ein Auftragsverarbeiter, der unter Verstoß gegen dieses Hauptstück die Zwecke und Mittel der Verarbeitung bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher

Verzeichnis von Verarbeitungstätigkeiten

§ 49. (1) Jeder Verantwortliche hat sinngemäß nach Maßgabe des Art 30 Abs 1 bis 4 DSGVO ein Verzeichnis von Verarbeitungstatigkeiten zu führen, wobei sich die Verweise in Art 30 Abs 1 lit g und Abs 2 lit DSGVO auf § 54 beziehen und die Bezugnahme auf einen Vertreter des Verantwortlichen oder des Auftragsverarbeiters gegenstandslos ist

(2) Das Verzeichnis gemaß Abs 1 hat auch Angaben zu enthalten über

1 die Verwendung von Profiling, wenn eine solche Verwendung vorgenommen wird, und

2 die Rechtsgrundlage der Verarbeitung, einschließlich der Übermittlungen, für die die personenbezogenen Daten bestimmt sind

5 taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in this Chapter,

6 assists the controller in ensuring compliance with the obligations pursuant to § 52 to § 56, taking into account the nature of processing and the information available to the processor,

7 at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union law or laws require(s) storage of the personal data,

8 makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in paras 1 to 6 and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller

With regard to subpara 8, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Chapter or other data protection provisions of Union law or statutory data protection provisions

(4) Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in para 3 shall be imposed on that other processor by way of a contract or other legal act under Union law or in accordance with laws, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Chapter Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations

(5) The contract or the other legal act referred to in paras 3 and 4 shall be in writing, including in electronic form

(6) The processor and 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 Union law or in accordance with laws

(7) If a processor determines, in infringement of this Chapter, the purposes and means of processing, that processor shall be considered to be a controller in respect of that processing

Records of processing activities

§ 49. (1) Each controller shall maintain a record of processing activities, applying Article 30 paras 1 to 4 of the General Data Protection Regulation accordingly, the references in Article 30 para 1 (g) and para 2 (c) of the General Data Protection Regulation refer to § 54, and the reference to the representative of the controller or the processor shall not apply

(2) The record referred to in para 1 shall also contain information on

1 the use of profiling, if profiling is used, and

2 the legal basis for the processing operation, including transfers, for which the personal data are intended

Protokollierung

§ 50. (1) Jeder Verarbeitungsvorgang ist in geeigneter Weise so zu protokollieren, dass die Zulassigkeit der Verarbeitung nachvollzogen und überprüft werden kann

Logging

§ 50. (1) Every processing operation shall be logged in an appropriate manner so that the legitimacy of processing can be traced and verified

(2) In automatisierten Verarbeitungssystemen sind alle Verarbeitungsvorgänge in automatisierter Form zu protokollieren. Aus diesen Protokolldaten müssen zumindest der Zweck, die verarbeiteten Daten, das Datum und die Uhrzeit der Verarbeitung, die Identifizierung der Person, die die personenbezogenen Daten verarbeitet hat, sowie die Identität eines allfälligen Empfängers solcher personenbezogenen Daten hervorgehen.

(3) In nicht automatisierten Verarbeitungssystemen sind zumindest Abfragen und Offenlegungen einschließlich Übermittlungen, Veränderungen sowie Löschungen zu protokollieren Für diese Protokolldaten gilt Abs. 2 zweiter Satz

(4) Die Protokolle dürfen ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung einschließlich der Eigenüberwachung, der Gewährleistung von Integrität und Sicherheit der personenbezogenen Daten sowie in gerichtlichen Strafverfahren verwendet werden.

(5) Der Verantwortliche und der Auftragsverarbeiter haben der Datenschutzbehörde auf deren Verlangen die Protokolle zur Verfügung zu stellen.

Zusammenarbeit mit der Datenschutzbehörde

§ 51. Der Verantwortliche und der Auftragsverarbeiter sind verpflichtet, über Aufforderung mit der Datenschutzbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten.

Datenschutz-Folgenabschätzung

§ 52. Der Verantwortliche hat zum Schutz der Rechte und berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener eine Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 1, 2, 3, 7 und 11 DSGVO durchzuführen, wobei sich der Nachweis gemäß Art. 35 Abs 7 lit d DSGVO auf die Einhaltung der Vorgaben dieses Hauptstücks bezieht.

Vorherige Konsultation der Datenschutzbehörde

§ 53. Der Verantwortliche hat nach Maßgabe des Art. 36 DSGVO vor der Verarbeitung personenbezogener Daten in neu anzulegenden Dateisystemen die Datenschutzbehörde zu konsultieren, wobei sich die Verweise in Art. 36 Abs. 1 und Abs 3 lit. e DSGVO auf § 52 und der Verweis auf die Bestimmungen hinsichtlich der Befugnisse der Datenschutzbehörde in Art. 36 Abs. 2 DSGVO auf § 33 beziehen und die in Art. 36 Abs. 2 DSGVO angeführten Maßnahmen innerhalb von sechs Wochen mit der Möglichkeit einer Verlängerung um einen weiteren Monat zu treffen sind.

Datensicherheitsmaßnahmen

§ 54. (1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, unter Berücksichtigung der unterschiedlichen Kategorien gemäß § 37, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 39.

(2) Der Verantwortliche und der Auftragsverarbeiter haben im Hinblick auf die automatisierte Verarbeitung nach einer Risikobewertung Maßnahmen zu ergreifen, um folgende Zwecke zu erreichen:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle);
3 Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
5 Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugriffskontrolle);

(2) In automated processing systems, all processing operations shall be logged in an automated manner. These log data shall at least reveal the purpose, the processed data, the date and time of processing, the identification of the person who processed the personal data, and the identity of any recipient of such personal data.

(3) In non-automated processing systems, at least consultations and disclosures, including transmissions, changes and erasures, shall be logged. Para. 2 sentence 2 shall apply to these log data.

(4) The logs shall exclusively be used to verify the lawfulness of the data processing, including self-monitoring and ensuring the integrity and security of the personal data, and in criminal proceedings in court.

(5) The controller and the processor shall provide the logs to the Data Protection Authority at its request.

Cooperation with the Data Protection Authority

§ 51. The controller and the processor shall cooperate, on request, with the Data Protection Authority in the performance of its tasks.

Data protection impact assessment

§ 52. To protect the rights and legitimate interests of data subjects affected by data processing activities and other persons concerned, the controller shall carry out a data protection impact assessment pursuant to Article 35 paras. 1, 2, 3, 7 and 11 of the General Data Protection Regulation, with demonstration pursuant to Article 35 para. 7 (d) of the General Data Protection Regulation referring to compliance with the requirements of this Chapter.

Prior consultation of the Data Protection Authority

§ 53. In accordance with Article 36 of the General Data Protection Regulation, the controller shall consult the Data Protection Authority prior to processing which will form part of a new filing system to be created, references in Article 36 paras. 1 and 3 (e) of the General Data Protection Regulation refer to § 52, and the reference to the provisions regarding the powers of the Data Protection Authority in Article 36 para 2 of the General Data Protection Authority refers to § 33, and the measures referred to in Article 36 para. 2 of the General Data Protection Regulation shall be taken within six weeks, with the possibility to extend that period by an additional month.

Data security measures

§ 54. (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 rights and freedoms of natural persons, shall implement appropriate technical and organisational measures, taking into account the different categories pursuant to § 37, to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in § 39.

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

1. deny unauthorised persons access to processing equipment used for processing ('equipment access control');
2. prevent the unauthorised reading, copying, modification or removal of data media ('data media control');
3. prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control');
4. prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control'),
5. ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control'),

6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle);

7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle);

8. Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle);

9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung);

10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

Meldung von Verletzungen an die Datensehutzbehörde

§ 55. (1) Der Verantwortliche hat nach Maßgabe des Art. 33 DSGVO Verletzungen des Schutzes personenbezogener Daten der Datenschutzbehörde zu melden.

(2) Soweit von der Verletzung des Schutzes personenbezogene Daten betroffen sind, die von dem oder an den Verantwortlichen eines anderen Mitgliedstaates der Europäischen Union übermittelt wurden, sind die in Art. 33 Abs. 3 DSGVO genannten Informationen dem Verantwortlichen jenes Mitgliedstaates der Europäischen Union unverzüglich zu übermitteln.

Benachrichtigung der betroffenen Person von Verletzungen

§ 56. (1) Der Verantwortliche hat nach Maßgabe des Art. 34 DSGVO betroffene Personen von Verletzungen des Schutzes ihrer Daten zu benachrichtigen.

(2) Die Benachrichtigung gemäß Abs. 1 kann unter den in § 43 Abs. 4 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden.

Benennung, Stellung und Aufgaben des Datenschutzbeauftragten

§ 57. (1) Jeder Verantwortliche hat nach Maßgabe des Art. 37 Abs. 5 und 7 DSGVO einen Datenschutzbeauftragten zu benennen. Gerichte sind im Rahmen ihrer justiziellen Tätigkeit von der Verpflichtung zur Benennung eines Datenschutzbeauftragten ausgenommen. § 5 gilt im Hinblick auf die Bestimmungen dieses Hauptstücks sinngemäß.

(2) Für die Stellung des Datenschutzbeauftragten gilt Art. 38 DSGVO.

(3) Dem Datenschutzbeauftragten obliegen die in Art. 39 DSGVO genannten Aufgaben in Bezug auf die Einhaltung der Bestimmungen dieses Hauptstücks.

(4) Der Verantwortliche hat die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und der Datenschutzbehörde mitzuteilen.

4. Abschnitt

Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen

Allgemeine Grundsätze für die Übermittlung personenbezogener Daten

§ 58. (1) Eine Übermittlung von personenbezogenen Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, durch zuständige Behörden ist nur zulässig, wenn die Bestimmungen dieses Hauptstücks eingehalten werden und

1. die Übermittlung für die in § 36 Abs. 1 genannten Zwecke erforderlich ist,

2. die personenbezogenen Daten an einen Verantwortlichen in einem Drittland oder einer internationalen Organisation, die eine für die in § 36 Abs. 1 genannten Zwecke zuständige Behörde ist, übermittelt werden,

3. in Fällen, in denen personenbezogene Daten aus einem anderen Mitgliedstaat der EU übermittelt oder zur Verfügung gestellt werden, dieser Mitgliedstaat die Übermittlung zuvor genehmigt hat,

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. prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');

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

10. ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

Notification of a breach to the Data Protection Authority

§ 55. (1) In accordance with Article 33 of the General Data Protection Regulation, the controller shall notify personal data breaches to the Data Protection Authority.

(2) Where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State of the European Union, the information referred to in Article 33 para. 3 of the General Data Protection Regulation shall be communicated to the controller of that Member State of the European Union without undue delay.

Communication of personal data breaches to data subjects

§ 56. (1) In accordance with Article 34 of the General Data Protection Regulation, the controller shall communicate breaches concerning their personal data to data subjects. § 42 para. 4 shall apply to the communication.

(2) Communication pursuant to para. 1 can be delayed, restricted or omitted under the conditions laid out in § 43 para. 4.

Designation, position and tasks of the data protection officer

§ 57. (1) Every controller shall designate a data protection officer in accordance with Article 37 paras. 5 and 7 of the General Data Protection Regulation. Courts are exempted from the obligation to designate a data protection officer in the context of their judicial activities. § 5 shall apply accordingly with regard to the provisions of this Chapter.

(2) Article 38 of the General Data Protection Regulation shall apply to the position of the data protection officer.

(3) The data protection officer shall have the tasks referred to in Article 39 of the General Data Protection Regulation with regard to compliance with the provisions of this Chapter.

(4) The controller shall publish the contact details of the data protection officer and communicate them to the Data Protection Authority.

Part 4

Transfers of personal data to third countries or international organisations

General principles for transfers of personal data

§ 58. (1) Any transfer by competent authorities of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if the conditions laid down in this Chapter are complied with and

1. the transfer is necessary for the purposes set out in § 36 para. 1,

2. the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in § 36 para. 1,

3. where personal data are transmitted or made available from another EU Member State, that Member State has given its prior authorisation to the transfer,

4. die Europäische Kommission gemäß § 59 Abs. 1 und 2 einen Angemessenheitsbeschluss gefasst hat oder, wenn kein solcher Beschluss vorliegt, geeignete Garantien im Sinne des § 59 Abs. 3 bis 5 erbracht wurden oder bestehen oder, wenn kein Angemessenheitsbeschluss gemäß § 59 Abs. 1 und 2 vorliegt und keine geeigneten Garantien im Sinne des § 59 Abs. 3 bis 5 vorhanden sind, Ausnahmen für bestimmte Fälle gemäß § 59 Abs. 6 und 7 anwendbar sind und

5. sichergestellt ist, dass eine Weiterübermittlung an ein anderes Drittland oder eine andere internationale Organisation nur aufgrund einer vorherigen Genehmigung der zuständigen Behörde, die die ursprüngliche Übermittlung durchgeführt hat, und unter gebührender Berücksichtigung sämtlicher maßgeblicher Faktoren, einschließlich der Schwere der Straftat, des Zwecks der ursprünglichen Übermittlung personenbezogener Daten und des Schutzniveaus für personenbezogene Daten in dem Drittland oder der internationalen Organisation, an das bzw. die personenbezogene Daten weiterübermittelt werden, zulässig ist.

(2) Eine Übermittlung ohne vorherige Genehmigung gemäß Abs. 1 Z 3 ist nur zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Die für die Erteilung der vorherigen Genehmigung zuständige Behörde ist unverzüglich zu unterrichten.

(3) Ersucht eine zuständige Behörde eines anderen Mitgliedstaates der EU um Genehmigung zur Übermittlung von personenbezogenen Daten, die ursprünglich aus dem Inland übermittelt wurden, an ein Drittland oder eine internationale Organisation gemäß Abs 1 Z 3, so ist zur Erteilung dieser Genehmigung jene zuständige Behörde zuständig, die die personenbezogenen Daten ursprünglich übermittelt hat, soweit nicht gesetzlich anderes angeordnet ist.

Datenübermittlung an Drittländer oder internationale Organisationen

§ 59. (1) Die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation ist zulässig, wenn die Europäische Kommission gemäß Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 im Wege eines Durchführungsaktes beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung Die Genehmigungspflicht gemäß § 58 Abs. 1 Z 3 bleibt davon unberührt.

(2) Übermittlungen personenbezogener Daten an ein Drittland, an ein Gebiet oder einen oder mehrere spezifischen Sektoren in einem Drittland oder an eine internationale Organisation gemäß den Abs. 3 bis 8 werden durch einen gemäß Art. 36 Abs. 5 der Richtlinie (EU) 2016/680 gefassten Beschluss der Europäischen Kommission zum Widerruf, zur Änderung oder zur Aussetzung eines Beschlusses nach Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 nicht berührt

(3) Liegt kein Beschluss nach Abs. 1 vor, so ist die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder

2. der Verantwortliche auf Grund einer Beurteilung der für die Übermittlung personenbezogener Daten maßgeblichen Umstände zu der Auffassung gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen.

(4) Bestehen geeignete Garantien gemäß Abs. 3 Z 2 für Kategorien von Übermittlungen, so hat der Verantwortliche die Datenschutzbehörde über diese Kategorien zu unterrichten.

(5) Übermittlungen gemäß Abs. 3 Z 2 sind zu dokumentieren und die Dokumentation einschließlich Datum und Zeitpunkt der Übermittlung, Informationen über die empfangende zuständige Behörde, Begründung der Übermittlung und übermittelte personenbezogenen Daten, der Datenschutzbehörde auf Anforderung zur Verfügung zu stellen.

(6) Wenn weder ein Angemessenheitsbeschluss gemäß Abs. 1 bis 2 vorliegt noch geeignete Garantien gemäß Abs 3 bis 5 vorhanden sind, so ist nach Maßgabe des Abs. 5 eine Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur zulässig, wenn die Übermittlung erforderlich ist

4. the European Commission has adopted an adequacy decision pursuant to § 59 paras. 1 and 2 or, in the absence of such a decision, appropriate safeguards as referred to in § 59 paras. 3 to 5 have been provided or exist, or, in the absence of an adequacy decision pursuant to § 59 paras 1 and 2 and of appropriate safeguards in accordance with § 59 paras 3 to 5, derogations for specific situations apply pursuant to § 59 paras. 6 and 7, and

5 it is ensured that an onward transfer to another third country or international organisation is permitted only subject to prior authorisation by the competent authority that carried out the original transfer and after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

(2) Transfers without prior authorisation pursuant to para. 1 subpara. 3 shall be permitted only if the transfer is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

(3) If a competent authority of another EU Member State requests authorisation to transfer to a third country or an international organisation pursuant to para. 1 subpara 3 personal data that have originally been transferred from Austria, the authority that originally transferred the personal data shall be the authority competent for giving the authorisation, unless otherwise provided for by law.

Data transfers to third countries or international organisations

§ 59. (1) The transfer of personal data to a third country or an international organisation shall be permitted where the European Commission has decided pursuant to Article 36 para. 3 of Directive (EU) 2016/680 by way of an implementing act that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection Such a transfer shall not require any specific authorisation. The authorisation obligation pursuant to § 58 para 1 subpara 3 shall remain unaffected thereby.

(2) A decision by the European Commission taken pursuant to Article 36 para. 5 of Directive (EU) 2016/680 to revoke, amend or suspend a decision pursuant to Article 36 para 3 of Directive (EU) 2016/680 shall be without prejudice to transfers of personal data to the third country, the territory or one or more specified sectors within that third country, or the international organisation in question pursuant to paras. 3 to 8.

(3) In the absence of a decision pursuant to para. 1, a transfer of personal data to a third country or an international organisation may take place where

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

2 the controller, following an assessment of the circumstances relevant for the transfer of personal data, concludes that appropriate safeguards exist with regard to the protection of personal data.

(4) If appropriate safeguards pursuant to para. 3 subpara. 2 exist for categories of transfers, the controller shall inform the Data Protection Authority of these categories.

(5) Transfers pursuant to para. 3 subpara. 2 shall be documented, and the documentation shall be made available to the Data Protection Authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

(6) In the absence of an adequacy decision pursuant to paras. 1 to 2 or of appropriate safeguards pursuant to paras. 3 to 5, a transfer of personal data to a third country or an international organisation may take place in accordance with para. 5 only on the condition that the transfer is necessary:

1. zum Schutz lebenswichtiger Interessen einer Person,
2. wenn dies zur Wahrung berechtigter Interessen der betroffenen Person gesetzlich vorgesehen ist,
3. zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaates der EU oder eines Drittlandes,
4. im Einzelfall für die in § 36 Abs. 1 genannten Zwecke, oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 36 Abs. 1 genannten Zwecken.

(7) In den Fällen des Abs. 6 Z 4 und 5 ist die Übermittlung nur zulässig, wenn keine das öffentliche Interesse an der Übermittlung überwiegenden Grundrechte und Grundfreiheiten der betroffenen Person der Übermittlung entgegenstehen.

(Anm.: Abs 1 durch Art. 2 § 2 Abs 1 Z 24 und Abs 2 Z 71, BGBl. I Nr. 2/2008, als nicht mehr geltend festgestellt.)

(8) **(Verfassungsbestimmung)** § 2 Abs. 2 und § 35 Abs. 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013 treten mit 1. Jänner 2014 in Kraft.

Übergangsbestimmungen

§ 61. *(Anm : Abs 1 bis 3 aufgehoben durch Z 3, BGBl. I Nr 120/2017)*

1. to protect the vital interests of a person,
2. to safeguard legitimate interests of the data subject, where the law so provides,
3. for the prevention of an immediate and serious threat to the public security of an EU Member State or a third country,
4. in individual cases for the purposes set out in § 36 para. 1, or
5. in an individual case for the establishment, exercise or defence of legal claims relating to the purposes set out in § 36 para. 1.

(7) In the cases referred to in para. 6 subparas. 4 and 5, a transfer is permitted only if no fundamental rights and freedoms of the data subject overriding the public interests in the transfer are an obstacle to the transfer.

Entry into force

§ 60. *(Note: para. 1 was found to be no longer in force in Article 2 § 2 para. 1 subpara. 24 und para. 2 subpara. 71, Federal Law Gazette I No 2/2008.)*

(2) The other provisions of this federal law shall also enter into force on 1 January 2000.

(3) § 26 para. 6 and § 52 paras. 1 and 2 as amended by the federal law promulgated in Federal Law Gazette I No 136/2001 shall enter into force on 1 January 2002.

(4) § 48a para. 5 as amended by the federal law promulgated in Federal Law Gazette I No 135/2009 shall enter into force on 1 January 2010.

(5) The table of contents, § 4 para. 1 subparas. 4, 5, 7 to 9, 11 and 12, § 8 paras. 1, 2 and 4, § 12 para. 1, the re-numbering of the paragraphs in § 13, § 16 paras. 1 and 3, § 17 paras. 1, 1a and 4, § 19 para. 1 subpara. 3a and para. 2, the re-numbering of the paragraphs in § 19, § 20 to § 22a including captions, § 24 para. 2a, § 24 para. 4, § 26 paras. 1 to 8 and 10, § 28 para. 3, § 30 para. 2a, 5 to 6a, § 31 and § 31a including captions, § 32 paras. 1, 4, 6 and 7, § 34 paras. 1, 3 and 4, § 36 paras. 3, 3a and 9, § 39 para. 5, § 40 paras. 1 and 2, § 41 para. 2 subpara. 4a, § 42 para. 1 subpara. 1, § 42 para. 5, § 46 para. 1 subparas. 2 and 3, paras. 2 to 3a, § 47 para. 4, § 49 para. 3, § 50 paras. 1 to 2a, Part 9a, § 51, § 52 paras. 2 and 4, § 55, § 61 paras. 6 to 9 as well as § 64 as amended by the federal law promulgated in Federal Law Gazette I No 133/2009 shall enter into force on 1 January 2010. Simultaneously, § 4 para. 1 subpara. 10, § 13 para. 3 as well as § 51 para. 2 shall become ineffective.

(6) § 36 para. 6 as amended by the federal law promulgated in Federal Law Gazette I No 133/2009 shall enter into force on 1 July 2010.

(6a) § 37 para 2, § 38 para. 2 and § 61 para. 9 as amended by the federal law promulgated in Federal Law Gazette I No 57/2013 shall enter into force on 1 May 2013.

(7) The table of contents, § 5 para. 4, § 10 para. 2, § 12 para. 4, § 13 paras. 1 and 2 subpara. 2, paras. 3, 4 and 6, § 16 para. 1, § 17 para. 1, § 18 para. 2, § 19 para. 1 subpara. 6 and para. 2, § 20 paras. 2 and 5 subpara. 2, § 21 para. 1 subpara. 3, § 22 paras. 2 to 4, § 22a paras. 1, 3 to 5, § 23 para. 2, § 26 paras. 2, 5 and 7, § 27 paras. 5 and 7, the caption of § 30, § 30 paras. 1, 2, 2a, 4 to 6a, the caption of § 31, § 31 paras. 1, 2, 5, 6 and 8, § 31a, § 32 paras. 5 to 7, § 34 para. 3 and 4, the caption of § 35, § 35 para. 1, § 36 to § 40 including the captions, § 41 para. 2 subpara. 1, § 44 paras. 6 and 8, § 46 para. 2 subpara. 3 and para. 3, § 47 paras. 3 and 4, § 48a para. 2, § 50 paras. 1 and 2, § 50b para. 2, § 50c para. 1, § 52 para. 2 subparas. 2 and 3 as well as para. 5, § 54 para. 2 and § 61 paras. 8 to 10 as amended by the federal law promulgated in Federal Law Gazette I No 83/2013 shall enter into force on 1 January 2014. Simultaneously, § 41 para. 2 subpara. 4a and the Data Protection Commission Remuneration Regulation, Federal Law Gazette II No 145/2006, shall become ineffective. All organisational and human resource measures needed to appoint the head of the Data Protection Authority and the deputy may be implemented before the federal law promulgated in Federal Law Gazette I No 83/2013 enters into force.

(8) **(Constitutional provision)** § 2 para. 2 and § 35 para. 2 as amended by the federal law promulgated in Federal Law Gazette I No 83/2013 shall enter into force on 1 January 2014.

Transitional provisions

§ 61. *(Note. paras. 1 to 3 repealed by subpara. 3, Federal Law Gazette I*

(4) **(Verfassungsbestimmung)** Datenanwendungen, die für die in § 17 Abs. 3 genannten Zwecke notwendig sind, dürfen auch bei Fehlen einer im Sinne des § 1 Abs. 2 ausreichenden gesetzlichen Grundlage bis 31. Dezember 2007 vorgenommen werden, in den Fällen des § 17 Abs. 3 Z 1 bis 3 jedoch bis zur Erlassung von bundesgesetzlichen Regelungen über die Aufgaben und Befugnisse in diesen Bereichen.

(Anm.: Abs. 5 bis 10 aufgehoben durch Z 3, BGBl. I Nr. 120/2017)

4. Hauptstück
Besondere Strafbestimmungen

Verwaltungsstrafbestimmung

§ 62. (1) Sofern die Tat nicht einen Tatbestand nach Art. 83 DSGVO verwirklicht oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 50 000 Euro zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenverarbeitung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält,
2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 6) übermittelt, insbesondere Daten, die ihm gemäß §§ 7 oder 8 anvertraut wurden, vorsätzlich für andere unzulässige Zwecke verarbeitet,
3. sich unter Vortäuschung falscher Tatsachen vorsätzlich personenbezogene Daten gemäß § 10 verschafft,
4. eine Bildverarbeitung entgegen den Bestimmungen des 3. Abschnittes des 1. Hauptstücks betreibt oder
5. die Einschau gemäß § 22 Abs. 2 verweigert.

(2) Der Versuch ist strafbar.

(3) Gegen juristische Personen können bei Verwaltungsübertretung nach Abs. 1 und 2 Geldbußen nach Maßgabe des § 30 verhängt werden.

(4) Die Strafe des Verfalls von Datenträgern und Programmen sowie Bildübertragungs- und Bildaufzeichnungsgeräten kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 in Zusammenhang stehen.

(5) Die Datenschutzbehörde ist zuständig für Entscheidungen nach Abs. 1 bis 4.

Datenverarbeitung in Gewinn- oder Schädigungsabsicht

§ 63. Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

5. Hauptstück
Schlussbestimmungen

Durchführung und Umsetzung von Rechtsakten der EU

§ 64. (1) Dieses Bundesgesetz dient der Durchführung der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5 2016 S. 1.

(2) Bundesgesetz dient weiters der Umsetzung der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung,

No 120/2017)

(4) **(Constitutional provision)** Data applications that are required for the purposes laid down in § 17 para. 3 may be continued even without a sufficient legal basis in terms of § 1 para. 2 until 31 December 2007, in the cases of § 17 para. 3 subparas. 1 to 3, however, only until federal regulations covering the functions and powers in these fields are enacted.

(Note: paras. 5 to 10 repealed by subpara. 3, Federal Law Gazette I No 120/2017)

Chapter 4
Special penal provisions

Administrative penalties

§ 62. (1) Unless the offence meets the elements of Article 83 of the General Data Protection Regulation or is subject to a more severe punishment according to other administrative penal provisions, an administrative offence punishable by a fine of up to €50,000 is committed by anyone who

1. intentionally and illegally gains access to data processing or maintains an obviously illegal means of access,
2. transmits data intentionally in violation of the rules on confidentiality (§ 6), in particular intentionally uses data entrusted to him or her according to § 7 or § 8 for other prohibited purposes,
3. by giving incorrect information intentionally obtains personal data according to § 10,
4. processes images contrary to the provisions of Chapter 1, Part 3, or
5. refuses inspection pursuant to § 22 para. 2.

(2) Attempts shall be punishable.

(3) In the case of an administrative offence pursuant to paras. 1 and 2, administrative fines can be imposed on legal persons in accordance with § 30.

(4) Data media and programs as well as apparatus for the transmission and recording of images can be forfeited (§ 10, § 17 and § 18 of the Administrative Penal Act) if they are linked to an administrative offence according to para. 1.

(5) The Data Protection Authority shall be the competent authority for decisions pursuant to paras. 1 to 4.

Processing with the intention to make a profit or to cause harm

§ 63. Whoever, with the intention to enrich himself or a third person unlawfully or to harm someone regarding that person's entitlement guaranteed according to § 1 para. 1, deliberately uses personal data that have been entrusted to or have become accessible to him solely because of his professional occupation, or that he has acquired illegally, for himself or makes such data available to another person or publishes such data despite the data subject's interest in confidentiality which deserves protection, shall be punished by a court with imprisonment of up to one year or with a fine of up to €720, unless the offence is subject to a more severe punishment pursuant to another provision.

Chapter 5
Final provisions

Execution and implementation of EU legal acts

§ 64. (1) This federal law serves to implement Regulation (EU) 2016/679 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 No L 119 of 4 May 2016, p. 1.

(2) Furthermore, this federal law serves to implement Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention,

Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. Nr. L 119 vom 4 5.2016 S. 89.

Sprachliche Gleichbehandlung

§ 65. Soweit in diesem Bundesgesetz auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise. Bei der Anwendung der Bezeichnungen auf bestimmte natürliche Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

Erlassung von Verordnungen

§ 66. Verordnungen auf Grund dieses Bundesgesetzes in seiner jeweiligen Fassung dürfen bereits von dem Tag an erlassen werden, der der Kundmachung der durchzuführenden Gesetzesbestimmungen folgt; sie dürfen jedoch nicht vor den durchzuführenden Gesetzesbestimmungen in Kraft treten.

Verweisungen

§ 67. Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden

Vollziehung

§ 68. Mit der Vollziehung dieses Bundesgesetzes sind, soweit sie nicht der Bundesregierung obliegt, der Bundeskanzler und die anderen Bundesminister im Rahmen ihres Wirkungsbereichs betraut.

Übergangsbestimmungen

§ 69. (1) Die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes laufende Funktionsperiode des Leiters der Datenschutzbehörde wird bis zu deren Ablauf fortgesetzt. Dies gilt auch für dessen Stellvertreter.

(2) Das von der Datenschutzbehörde geführte Datenverarbeitungsregister ist von der Datenschutzbehörde bis zum 31. Dezember 2019 zu Archivzwecken fortzuführen. Es dürfen keine Eintragungen und inhaltliche Änderungen im Datenverarbeitungsregister vorgenommen werden. Registrierungen im Datenverarbeitungsregister werden gegenstandslos. Jedermann kann in das Register Einsicht nehmen. In den Registrierungsakt einschließlich darin allenfalls enthaltener Genehmigungsbescheide ist Einsicht zu gewähren, wenn der Einsichtswerber glaubhaft macht, dass er eine betroffene Person ist, und soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen des Verantwortlichen (Auftraggebers) oder anderer Personen entgegenstehen.

(3) Gemäß den §§ 17 und 18 Abs. 2 DSG 2000 im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes anhängige Registrierungsverfahren gelten als eingestellt. Im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes anhängige Verfahren nach den §§ 13, 46 und 47 DSG 2000 sind fortzuführen, sofern die Genehmigung nach diesem Bundesgesetz oder der DSGVO erforderlich ist. Anderenfalls gelten sie als eingestellt.

(4) Zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bei der Datenschutzbehörde oder bei den ordentlichen Gerichten zum Datenschutzgesetz 2000 anhängige Verfahren sind nach den Bestimmungen dieses Bundesgesetzes und der DSGVO fortzuführen, mit der Maßgabe, dass die Zuständigkeit der ordentlichen Gerichte aufrecht bleibt.

(5) Verletzungen des Datenschutzgesetzes 2000, die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes noch nicht anhängig gemacht wurden, sind nach der Rechtslage nach Inkrafttreten dieses Bundesgesetzes zu beurteilen.

(6) Die Eingaben der betroffenen Personen nach § 24 sind von den Verwaltungsabgaben des Bundes befreit.

(7) Die entsendenden Stellen haben eine dem § 15 Abs. 1 Z 1 bis 6 entsprechende Anzahl von Mitgliedern und Ersatzmitgliedern des Datenschutzrates dem innerhalb von zwei Wochen ab dem 25. Mai 2018 schriftlich bekannt zu geben. Die konstituierende Sitzung des Datenschutzrates hat innerhalb von sechs Wochen ab dem 25. Mai 2018 zu erfolgen. Bis zur Wahl des neuen Vorsitzenden und der beiden stellvertretenden Vorsitzenden bleiben der bisherige Vorsitzende sowie die beiden bisherigen stellvertretenden Vorsitzenden in ihrer Funktion.

(8) Besondere Bestimmungen über die Verarbeitung von personenbezogenen

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 No L 119 of 4 May 2016, p. 89.

Gender-neutral use of language

§ 65. Insofar as expressions relating to natural persons in this federal law are given only in the male form, they shall apply to males and females equally. When the expressions are applied to specific natural persons, the form specific to the gender shall be used.

Enactment of regulations

§ 66. Regulations based on this federal law as amended may already be enacted as of the day following the promulgation of the legal provision to be implemented; they shall, however, not enter into force before the statutory provisions which are to be implemented.

References

§ 67. Insofar as provisions of this federal law refer to provisions of other federal laws, these shall be applied as amended from time to time.

Execution

§ 68. The Federal Chancellor and the other federal ministers, within their sphere of responsibilities, shall execute this federal law insofar as the execution has not been entrusted to the Federal Government.

Transitional provisions

§ 69. (1) The current term of office of the head of the Data Protection Authority at the time of the entry into force of this federal law shall continue until the end of the term of office. This shall also apply to the deputy.

(2) The Data Protection Authority shall continue to have the Data Processing Register kept by the Data Protection Authority for archiving purposes until 31 December 2019. No entries and changes to the contents of the Data Processing Register may be made. Registrations in the Data Processing Register shall become void. Any person may inspect the Register. Inspection of the registration file including any authorisations contained therein shall be granted if the person applying for inspection can satisfactorily demonstrate that he or she is a data subject, and as far as no overriding interests in confidentiality which deserve protection on the part of the controller or another person are an obstacle to access.

(3) Any registration procedures pursuant to § 17 and § 18 para. 2 of the Data Protection Act 2000 pending at the time of entry into force of this federal law shall be deemed discontinued. Any registration procedures pursuant to § 13, § 46 and § 47 of the Data Protection Act 2000 pending at the time of entry into force of this federal law shall be continued if authorisation is required pursuant to this federal law or the General Data Protection Regulation. If no authorisation is required, they shall be deemed discontinued.

(4) Proceedings regarding the Data Protection Act 2000 pending before the Data Protection Authority or before courts of law at the time of entry into force of this federal law shall be continued in accordance with the provisions of this federal law and the General Data Protection Regulation with the reservation that courts of law continue to have jurisdiction.

(5) Infringements of the Data Protection Act 2000 that are not yet pending at the time of entry into force of this federal law shall be judged in accordance with the legal situation after entry into force of this federal law.

(6) Submissions by a data subject pursuant to § 24 shall be exempt from federal administrative fees.

(7) The entities or bodies delegating the members and substitute members shall notify the Federal Chancellery in writing within a period of two weeks from 25 May 2018 of the members and substitute members of the Data Protection Council, the number of whom must correspond to § 15 para. 1 subparas. 1 to 6. The constitutive meeting of the Data Protection Council shall take place within six weeks after 25 May 2018. The previous head and the two previous deputy heads shall continue to exercise their functions until the election of the new head and the two deputy heads.

(8) Special provisions on the processing of personal data in other federal or

Daten in anderen Bundes- oder Landesgesetzen bleiben unberührt.

(9) Vor Inkrafttreten dieses Bundesgesetzes nach §§ 13, 46 und 47 DSG 2000 rechtskräftig erteilte Genehmigungen der Datenschutzbehörde bleiben unberührt. Nach dem Datenschutzgesetz 2000 erteilte Zustimmungen bleiben aufrecht, sofern sie den Vorgaben der DSGVO entsprechen.

Inkrafttreten

§ 70.

) Der Titel, das Inhaltsverzeichnis, das 1. Hauptstück, die Bezeichnung und Überschrift des 2. Hauptstücks, der 1 , 2., 3. und 4. Abschnitt, die Überschrift und Bezeichnung des 5. Abschnittes, § 35 Abs 1, die Bezeichnung und Überschrift des 3. Hauptstücks, der 1., 2. und 3 Abschnitt, die Überschrift und Bezeichnung des 4. Abschnittes, die §§ 58 und 59 samt Überschriften sowie das 4. und 5. Hauptstück in der Fassung des Bundesgesetzes BGBl I Nr. 120/2017 treten mit 25 Mai 2018 in Kraft. Im Art. 2 treten der 1 , 2 , 3., 4 , 5 und 6 Abschnitt, die Bezeichnung und die Überschrift des 7 Abschnittes, die Überschrift zu § 35, die §§ 36 bis 44 samt Überschriften, der 8., 9., 9a und 10. Abschnitt, die Bezeichnung und die Überschrift des 11. Abschnittes, die §§ 53 bis 59 samt Überschriften, § 61 Abs 1 bis 3 und 5 bis 10 sowie die §§ 62 bis 64 samt Überschriften in der Fassung vor der Novelle BGBl. I Nr 120/2017 mit Ablauf des 24. Mai 2018 außer Kraft.

() Die Standard- und Muster-Verordnung 2004 – StMV 2004, BGBl II Nr. 312/2004, die Datenverarbeitungsregister-Verordnung 2012 – DVRV 2012, BGBl. II Nr. 257/2012, und die Datenschutzangemessenheits-Verordnung – DSAV, BGBl. II Nr. 521/1999, treten mit Ablauf des 24. Mai 2018 außer Kraft.

provincial laws shall remain unaffected.

(9) Authorisations pursuant to § 13, § 46 and § 47 of the Data Protection Act 2000 granted by the Data Protection Authority in a final manner shall remain unaffected. Consent given pursuant to the Data Protection Act 2000 shall continue to be valid if it meets the requirements of the General Data Protection Regulation.

Entry into force

§ 70. (1) The title, the table of contents, Chapter 1, the name and caption of Chapter 2, Parts 1, 2, 3, and 4, the caption and name of Part 5, § 35 para 1, the name and caption of Chapter 3, Parts 1, 2, and 3, the caption and name of Part 4, § 58 and § 59, including the captions, as well as Chapters 4 and 5 as amended by the federal law promulgated in Federal Law Gazette I No 120/2017 shall enter into force on 25 May 2018. In Article 2, Parts 1, 2, 3, 4, 5 and 6, the name and caption of Part 7, the caption of § 35, § 36 to § 44 including the captions, Parts 8, 9, 9a and 10, the name and the caption of Part 11, § 53 to § 59 including the captions, § 61 paras 1 to 3 and 5 to 10 as well as § 62 to § 64 including the captions in the version before the amendment by Federal Law Gazette I No 120/2017 shall become ineffective as of the end of 24 May 2018.

(2) The Standards and Models Regulation 2004, Federal Law Gazette II No 312/2004, the Data Processing Register Regulation 2012, Federal Law Gazette II No 257/2012, and the Data Protection Adequacy Regulation, Federal Law Gazette II No 521/1999, shall become ineffective as of the end of 24 May 2018.