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.)

← Original Version
as amended by:
(List of amendments published in the Federal Law Gazette (F. L. G. = BGBl.)

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

Disclaimer:

- This translation is an unofficial aid for our readers. It has been made with great care, but linguistic compromises were unavoidable. Only the original German version is valid in any legal dispute.
- The reader should bear in mind that this law does not exist alone, but is a part of the Austrian legal system. Some provisions of the DSG 2000 will remain unclear without a certain level of background knowledge.
- Please note that this law may be amended in the future, and check occasionally for updates.
- The German Title “Datenschutzgesetz 2000” and the abbreviation “DSG 2000” should be used in English texts to avoid confusion. .

Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000)

Inhaltsverzeichnis

Artikel 1 (Verfassungsbestimmung)

Federal Act concerning the Protection of Personal Data (DSG 2000)

Table of Contents

Article 1 (Constitutional Provision)

Artikel 2

1. Abschnitt: Allgemeines

2. Abschnitt: Verwendung von Daten

3. Abschnitt: Datensicherheit

4. Abschnitt: Publizität der Datenverarbeitungen

5. Abschnitt: Die Rechte des Betroffenen

Article 2

Part 1: General Provisions

Part 2: Use of Data

Part 3: Data Security

Part 4: Publicity of Data Applications

Part 5: Rights of the Data Subject

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

Article 1

(Constitutional Provision)

Fundamental Right to Data Protection

§ 1. (1) Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject [Betroffener].

(2) Insofar personal data is not used in the vital interest of the data subject or with his consent, restrictions to the right to secrecy are only permitted to safeguard overriding legitimate interests of another, namely in case of an intervention by a public authority the restriction shall only be permitted based on laws necessary for the reasons stated in Art. 8, para. 2 of the European Convention on Human Rights (Federal Law Gazette No. 210/1958). Such laws may provide for the use of data [Verwendung von Daten] that deserve special protection only in order to safeguard substantial public interests and shall provide suitable safeguards for the protection of the data subjects' interest in secrecy. Even in the case of permitted restrictions the intervention with the fundamental right shall be carried out using only the least intrusive of all effective methods.

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.

(5) Gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen. In allen übrigen Fällen ist die Datenschutzkommission zur Entscheidung zuständig, es sei denn, daß Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind.

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 Datenschutzkommission, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden.

Räumlicher Anwendungsbereich

§ 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

(3) Everybody shall have, insofar as personal data concerning him are destined for automated processing or manual processing, i.e. in filing systems [Dateien] without automated processing, as provided for by law,

1. the right to obtain information as to who processes what data concerning him, where the data originated, for which purpose they are used, as well as 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.

(5) The fundamental right to data protection, except the right to information [Auskunftsrecht], shall be asserted before the civil courts against organisations that are established according to private law, as long as they do not act in execution of laws. In all other cases the Data Protection Commission [Datenschutzkommission] shall be competent to render the decision, unless an act of Parliament or a judicial decision is concerned.

Legislative Power and Enforcement

§ 2 (1) The Federation [Bund] shall have power to pass laws concerning the protection of personal data that are automatically processed.

(2) The Federation shall have power to execute such federal laws. Insofar as such data are used by a State [Land], on behalf of a State, by or on behalf of legal persons established by law within the powers of the States [Länder] these Federal Acts [Bundesgesetze] shall be executed by the States unless the execution has been entrusted by federal law to the Data Protection Commission [Daten¬schutz¬kommission], the Data Protection Council [Daten¬schutz¬rat] or the courts.

Territorial Jurisdiction

§ 3 (1) The provisions of this Federal Act [Bundesgesetz] shall be applied to the use of personal data in Austria. This Federal Act shall also be applied to the use of data [Verwendung von Daten] outside of Austria, insofar as the data is used in other Member States of the European Union for purposes of a main establishment or branch establishment (§ 4 sub-para. 15) in Austria of the controller [Auftraggeber] (§ 4 sub-para. 4).

(2) Deviating from para. 1 the law of the state where the controller has its seat applies, when a controller of the private sector (§ 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.

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.

Artikel 2
1. Abschnitt

Allgemeines

Definitionen

§ 4. Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten die Begriffe:

1. „Daten“ („personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;
2. „sensible Daten“ („besonders schutzwürdige Daten“): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;
3. „Betroffener“: jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;
4. Auftraggeber: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister (Z 5) die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde ihm ausdrücklich untersagt oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden;
5. Dienstleister: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate

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

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

Article 2
Part 1

General Provisions

Definitions

§ 4. For the subsequent provisions of this Federal Act [Bundesgesetz] the terms listed below shall mean:

1. ”Data” (”Personal Data”) [Daten” (”personenbezogene Daten”)]: Information relating to data subjects (sub-para. 3) who are identified or identifiable; Data are ”only indirectly personal” for a controller (sub-para. 4), a processor (sub-para. 5) or recipient of a transmission (sub-para. 12) when the Data relate to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means;
2. ”Sensitive Data” (”Data deserving special protection”) [”sensible Daten” (”besonders schutzwürdige Daten”)]: Data relating to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and data concerning health or sex life;
3. ”Data Subject” [”Betroffener”]: any natural or legal person or group of natural persons not identical with the controller, whose data are processed (sub-para. 8);
4. ”Controller” [”Auftraggeber”]: natural or legal person, group of persons or organ of a territorial corporate body [Gebietskörperschaft] or the offices of these organs, if they decide alone or jointly with others to use data (sub-para.8), without regard whether they use the data themselves (sub-para. 8) or have it done by a service provider (sub-para. 5). They are also deemed to be controllers when the service provider instructed to carry out an order (sub-para. 5) decides to use data for this purpose (sub-para. 8) except if this was expressly prohibited or if the contractor has to decide under his own responsibility, on the basis of rules of law or codes of conduct.
5. ”Processor” [”Dienstleister”]: natural or legal person, group of persons or organ of a federal, state and local authority [Gebietskörperschaft] or the offices

solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden (Z 8);

6. „Datei“: strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;
7. „Datenanwendung“: die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);
8. Verwenden von Daten: jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten;
9. Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (Z 12) von Daten;
10. (Anm.: aufgehoben durch BGBl. I Nr. 133/2009)
11. Überlassen von Daten: die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses (Z 5);
12. Übermitteln von Daten: die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;
13. „Informationsverbundsystem“: die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, daß jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden;
14. „Zustimmung“: die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, daß er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;
15. „Niederlassung“: jede durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die am Ort ihrer Einrichtung auch tatsächlich Tätigkeiten ausübt.

Öffentlicher und privater Bereich

§ 5. (1) Datenanwendungen sind dem öffentlichen Bereich im Sinne dieses Bundesgesetzes zuzurechnen, wenn sie für Zwecke eines Auftraggebers des

of these organs, if they use data only for a commissioned work (sub-para. 8);

6. ”Filing System ” [”Datei”]: structured set of personal data which are accessible according to at least one specific criterion;
7. ”Data Application” [”Datenanwendung”]: the sum of logically linked stages of data use (sub-para. 8) which are organised in order to reach a defined result (the purpose of the Data Application) and which are as a whole or partially performed automatically, that is, performed by machines and controlled through programs (automated data processing);
8. ”Use of Data” [”Verwenden von Daten”]: all kinds of operations with Data, meaning both processing of data (sub-para. 9) and transmission of Data (sub-para. 12);
9. ”Processing of Data” [”Verarbeiten von Daten”]: the collection, recording, storing, sorting, comparing, modification, interlinkeage, reproduction, consultation, output, utilisation, committing (No. 11), blocking, erasure or destruction or any other kind of operation with data except the transmission of Data (sub-para. 12);
10. *(Note: Repealed by Federal Law Gazette I No. 133/2009)*
11. ”Committing of Data” [”Überlassen von Daten”]: the transfer of data from the controller to a processor in the context of a commissioned work (sub-para. 5);
12. ”Transmission of Data” [”Übermitteln von Daten”]: the transfer of data to recipients other than the data subject, the controller or a processor, in particular publishing of data as well as the use of data for another application purpose [Aufgabengebiet] of the controller;
13. ”Joint Information System” [”Informationsverbundsystem”]: joint processing of data in a data application by several controllers and the joint utilisation of the data so that every controller has access even to those data in the system that have been made available to the system by other controllers;
14. ”Consent” [”Zustimmung”]: the valid declaration of intention of the data subject, given without constraint, that he agrees to the use of data relating to him in a given case, after having been informed about the prevalent circumstances;
15. ”Establishment” [”Niederlassung”]: any organisational unit set apart in terms of layout and function by fixed facilities at a specific place, with or without the status of a legal person, which carries out activities at the place where it is set up.

Public and Private Sector

§ 5 (1) Data applications [Datenanwendungen] shall be imputed to the public sector according to this Federal Act [Bundes¬gesetz] if they are undertaken for

öffentlichen Bereichs (Abs. 2) durchgeführt werden.

(2) Auftraggeber des öffentlichen Bereichs sind alle Auftraggeber,

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.

(3) Die dem Abs. 2 nicht unterliegenden Auftraggeber gelten als Auftraggeber des privaten Bereichs im Sinne dieses Bundesgesetzes.

2. Abschnitt

Verwendung von Daten

Grundsätze

§ 6. (1) Daten dürfen nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werden;
2. für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden; die Weiterverwendung für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 zulässig;
3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;
4. so verwendet werden, daß sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
5. solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

(2) Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der in Abs. 1 genannten Grundsätze; dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.

(3) Der Auftraggeber einer diesem Bundesgesetz unterliegenden Datenanwendung hat, wenn er nicht im Gebiet der Europäischen Union niedergelassen ist, einen in Österreich ansässigen Vertreter zu benennen, der unbeschadet der Möglichkeit eines Vorgehens gegen den Auftraggeber selbst namens des Auftraggebers verantwortlich gemacht werden kann.

(4) Zur näheren Festlegung dessen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist, können für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare

purposes of a controller of the public sector (p. 2).

(2) Public sector controllers are all those controllers who

1. are established according to public law legal structures, in particular also as an organ of a territorial corporate body [Gebietskörperschaft], or
2. as far as they execute laws despite having been incorporated according to private law.

(3) Controllers not within the scope of para. 2 are considered controllers of the private sector according to this Federal Act [Bundesgesetz].

Part 2

Use of Data

Principles

§ 6. (1) Data shall only

1. be used fairly and lawfully;
2. be collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further uses for scientific and statistical purposes is permitted subject to § 46 and 47;
3. be used insofar as they are essential for the purpose of the data application [Datenanwendung] and are not excessive in relation to the purpose;
4. be used so that the results are factually correct with regard to the purpose of the application, and the data must be kept up to date when necessary;
5. be kept in a form which permits identification of data subjects [Betroffene] as long as this is necessary for the purpose for which the data were collected; a longer period of storage may be laid down in specific laws, particularly laws concerning archives.

(2) The controller [Auftraggeber] shall bear the responsibility that the principles of para. 1 are complied with in all his data applications; this also applies when he employs a processor [Dienstleister] to use the data.

(3) A controller responsible for a use of data [Datenverwendung] subject to this Federal Act [Bundesgesetz] who does not reside in the European Union has to name a representative residing in Austria who can be held responsible in place of the controller, without prejudice to the possibility of legal measures against the controller himself.

(4) To determine more closely what can be regarded as fair and lawful use of data [Datenverwendung] in a specific field, representations of interest established by law, other professional associations and comparable bodies may draw up codes of conduct

Einrichtungen Verhaltensregeln ausarbeiten. Solche Verhaltensregeln dürfen nur veröffentlicht werden, nachdem sie dem Bundeskanzler zur Begutachtung vorgelegt wurden und dieser ihre Übereinstimmung mit den Bestimmungen dieses Bundesgesetzes begutachtet und als gegeben erachtet hat.

Zulässigkeit der Verwendung von Daten

§ 7. (1) Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

(2) Daten dürfen nur übermittelt werden, wenn

1. sie aus einer gemäß Abs. 1 zulässigen Datenanwendung stammen und
2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis - soweit diese nicht außer Zweifel steht - im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und
3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

(3) Die Zulässigkeit einer Datenverwendung setzt voraus, daß die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und daß die Grundsätze des § 6 eingehalten werden.

Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten

§ 8. (1) Schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder
2. der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
3. lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder
4. überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.

(2) Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung zulässigerweise veröffentlichter Daten gemäß § 28 Widerspruch zu erheben, bleibt unberührt.

(3) Schutzwürdige Geheimhaltungsinteressen sind aus dem Grunde des Abs. 1 Z 4 insbesondere dann nicht verletzt, wenn die Verwendung der Daten

1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche

for the private sector. These codes of conduct shall only be published after they have been submitted to the Federal Chancellor [Bundeskanzler] for evaluation, have been evaluated and have been found to be in compliance with the present law.

Legitimate Use of Data

§ 7. (1) Data shall be processed only insofar as the purpose and content of the data application [Datenanwendung] are covered by the statutory competencies or the legitimate authority of the respective controller and the data subjects' [Betroffener] interest in secrecy deserving protection is not infringed.

(2) Data shall only be transmitted if

1. they originate from a legal data application according to para. 1 and
2. the recipient has satisfactorily demonstrated to the transmitting party his statutory competence or legitimate authority with regard to the purpose of the transmission [Übermittlung], insofar as it is not beyond doubt, and
3. the interests in secrecy of the data subject deserving protection are not infringed by the purpose and content of the transmission.

(3) The legitimacy of a use of data [Datenverwendung] requires that the intervention be carried out only to the extent required, and using the least intrusive of all effective methods and that the principles of § 6 be respected.

Interests in Secrecy Deserving Protection for the Use of Non-Sensitive Data

§ 8. (1) Interests in secrecy deserving protection are not infringed when using non-sensitive data if

1. an explicit legal authorisation or obligation to use the data exists; or
2. the data subject [Betroffener] has given his consent, which can be revoked at any time, the revocation making any further use of the data illegal; or
3. vital interests of the data subject require the use; or
4. overriding legitimate interests pursued by the controller [Auftraggeber] or by a third party require the use of data [Datenverwendung].

(2) The use of legitimately published data and only indirectly personal data shall not constitute an infringement of interests in secrecy deserving protection. The right to object to the use of data legitimately published pursuant to § 28 remains unaffected.

(3) Interests in secrecy deserving protection are not infringed according to para. 1 sub-para. 4, in particular if the use of data

1. is an essential requirement for a controller of the public sector to exercise a

Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder

2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder
3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder
4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem erforderlich ist oder
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat oder
7. im Katastrophenfall, 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; im letztgenannten Fall gilt § 48a Abs. 3.

(4) Die Verwendung von 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 verstößt - unbeschadet der Bestimmungen des Abs. 2 - nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht oder
2. die Verwendung derartiger Daten für Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist oder
3. sich sonst die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden berechtigten Interessen des Auftraggebers ergibt und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen nach diesem Bundesgesetz gewährleistet oder
4. die Datenweitergabe zum Zweck der Erstattung einer Anzeige an eine zur Verfolgung der angezeigten strafbaren Handlungen (Unterlassungen) zuständige Behörde erfolgt.

Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

§ 9. Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn

1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder

legally assigned function or

2. is performed by a controller of the public sector in fulfilment of his obligation to provide inter-authority assistance or
3. is required to protect the vital interests of a third party or
4. is necessary for the fulfilment of a contract between the controller and the data subject or
5. is necessary for establishment, exercise or defence of legal claims of the controller before a public authority and if the data were collected legitimately or
6. concerns solely the exercise of a public office by the data subject.
7. in case of catastrophy, to the extent required to assist the persons directly affected by the catastrophy, to locate and identify persons missing or dead and to inform next of kin; in the very last case § 48a para. 3 applies.

(4) The use of data concerning acts and omissions punishable by the courts or administrative authorities, and in particular concerning suspected criminal offences, as well as data concerning criminal convictions and preventive measures does not without prejudice to para. 2 infringe interests in secrecy deserving protection if

1. an explicit legal obligation or authorisation to use the data exists; or
2. the use of such data is an essential requirement for a controller of the public sector to exercise a legally assigned function;
3. the legitimacy of the data application [Daten¬anwendung] otherwise follows from statutory responsibilities or other legitimate interests of the controller that override the data subjects' interests in secrecy deserving protection and the manner of use safeguards the interests of the data subject according to this Federal Act [Bundesgesetz].or
4. the transmitting of data is made for a report to an institution in charge of prosecution of a reported criminal act (or criminal omission).

Interests in Secrecy Deserving Protection for the Use of Sensitive Data

§ 9. (1) The use of sensitive data does not infringe interests in secrecy deserving protection only and exclusively if

1. the data subject [Betroffener] has obviously made public the data himself or

2. die Daten in nur indirekt personenbezogener Form verwendet werden oder
3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen, oder
4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht oder
5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben, oder
6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder
8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist oder
9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
10. Daten für private Zwecke gemäß § 45 oder für wissenschaftliche Forschung oder Statistik gemäß § 46, zur Benachrichtigung oder Befragung des Betroffenen gemäß § 47 oder im Katastrophenfall gemäß § 48a verwendet werden oder
11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse im Hinblick auf die Datenverwendung unberührt bleiben, oder
12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder
13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten und es sich hiebei um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben; diese Daten dürfen, sofern sich aus gesetzlichen Vorschriften

2. the data are used only in indirectly personal form or
3. the obligation or authorisation to use the data is stipulated by laws, insofar as these serve an important public interest, or
4. the use is made by a controller of the public sector in fulfilment of his obligation to give inter-authority assistance or
5. data are used that concern solely the exercise of a public office by the data subject or
6. the data subject has unambiguously given his consent, which can be revoked at any time, the revocation making any further use of the data illegal, or
7. the processing or transmission [Über¬mittlung] is in the vital interest of the data subject and his consent cannot be obtained in time or
8. the use is in the vital interest of a third party or
9. the use is necessary for establishment, exercise or defence of legal claims of the controller before a public authority and the data were collected legitimately or
10. data are used for private purposes pursuant to § 45 or for scientific research or statistics pursuant to § 46 for information or interviewing of the data subject pursuant to § 47 or in case of a catastrophy according to § 48a or
11. the use is required according to the rights and duties of the controller in the field of employment law and civil service regulations and, and is legitimate according to specific legal provisions; the rights of the labour councils according to the Arbeitsverfassungsgesetz with regard to the use of data [Datenverwendung] remain unaffected, or
12. the data are required for the purposes of preventive medicine, medical diagnosis, the provision of health care or treatment or the management of health-care services, and the use of data is performed by medical personnel or other persons subject to an equivalent duty of secrecy, or
13. non profit-organisations with a political, philosophical, religious or trade-union aim process data revealing the political opinion or philosophical beliefs of natural persons in the course of their legitimate activities, as long as these are data of members, sponsors or other persons who display an interest in the aim of the organisation on a regular basis; these data shall not be disclosed to a third party without the consent of the data subjects unless otherwise provided for by law.

nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden.

Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen

§ 10. (1) Auftraggeber dürfen bei ihren Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Der Auftraggeber hat mit dem Dienstleister die hiefür notwendigen Vereinbarungen zu treffen und sich von ihrer Einhaltung durch Einholung der erforderlichen Informationen über die vom Dienstleister tatsächlich getroffenen Maßnahmen zu überzeugen.

(2) Die beabsichtigte Heranziehung eines Dienstleisters durch einen Auftraggeber des öffentlichen Bereichs im Rahmen einer Datenanwendung, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegt, ist der Datenschutzkommission mitzuteilen, es sei denn, daß die Inanspruchnahme des Dienstleisters auf Grund ausdrücklicher gesetzlicher Ermächtigung erfolgt oder als Dienstleister eine Organisationseinheit tätig wird, die mit dem Auftraggeber oder einem diesem übergeordneten Organ in einem Über- oder Unterordnungsverhältnis steht. Kommt die Datenschutzkommission zur Auffassung, daß die geplante Inanspruchnahme eines Dienstleisters geeignet ist, schutzwürdige Geheimhaltungsinteressen der Betroffenen zu gefährden, so hat sie dies dem Auftraggeber unverzüglich mitzuteilen. Im übrigen gilt § 30 Abs. 6 Z 4.

Pflichten des Dienstleisters

§ 11. (1) Unabhängig von allfälligen vertraglichen Vereinbarungen haben Dienstleister bei der Verwendung von Daten für den Auftraggeber jedenfalls folgende Pflichten:

1. die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden; insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten;
2. alle gemäß § 14 erforderlichen Datensicherheitsmaßnahmen zu treffen; insbesondere dürfen für die Dienstleistung nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen;
3. weitere Dienstleister nur mit Billigung des Auftraggebers heranzuziehen und deshalb den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, daß er dies allenfalls untersagen kann;
4. - sofern dies nach der Art der Dienstleistung in Frage kommt - im Einvernehmen mit dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen;
5. nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und

Legitimate Committing of Data for Service Processing

§ 10. (1) Controllers [Auftraggeber] may employ processors [Dienstleister] for their data applications [Datenanwendungen] insofar as the latter sufficiently warrant the legitimate and secure use of data [Datenverwendung]. The controller shall enter into agreements with the processor necessary therefor and satisfy himself that the agreements are complied with by acquiring the necessary information about the actual measures implemented by the processor.

(2) A planned enlistment of a processor by a controller of the public sector for a data application subject to prior checking [Vorabkontrolle] pursuant to § 18 para. 2 shall be notified to the Data Protection Commission [Datenschutzkommission] unless the enlistment of the processor is carried out on grounds of an explicit legal authorisation or the processor is an organisational unit that is superior or subordinate to the processor or one of his superior organs. The Data Protection Commission shall inform the controller without delay if it comes to the conclusion that the planned enlistment of a processor may endanger interest in secrecy of the data subject [Betroffener] deserving protection. § 30 para. 6 sub-para. 4 applies.

Obligations of the Processor

§ 11. (1) Irrespective of contractual obligations, all processors [Dienstleister] have the following obligations when using data for a controller [Auftraggeber]:

1. to use data only according to the instructions of the controller; in particular, the transmission [Übermittlung] of the data used is prohibited unless so instructed by the controller;
2. to take all required safety measures pursuant to § 14; in particular to employ only operatives who have committed themselves to confidentiality vis-á-vis the processor or are under a statutory obligation of confidentiality;
3. to enlist another processor only with the permission of the controller and therefore to inform the controller of this intended enlistment of another processor in such a timely fashion that the controller has the possibility to object;
4. insofar as this is possible given the nature of the service processing [Dienstleistung] to create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller’s obligation to grant the right of information, rectification and erasure;
5. to hand over to the controller after the end of the service processing all results

Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten;

6. dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der unter Z 1 bis 5 genannten Verpflichtungen notwendig sind.

(2) Vereinbarungen zwischen dem Auftraggeber und dem Dienstleister über die nähere Ausgestaltung der in Abs. 1 genannten Pflichten sind zum Zweck der Beweissicherung schriftlich festzuhalten.

Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland

§ 12. (1) Die Übermittlung und Überlassung von Daten an Empfänger in Vertragsstaaten des Europäischen Wirtschaftsraumes ist keinen Beschränkungen im Sinne des § 13 unterworfen. Dies gilt nicht für den Datenverkehr zwischen Auftraggebern des öffentlichen Bereichs in Angelegenheiten, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

(2) Keiner Genehmigung gemäß § 13 bedarf weiters der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutz. Welche Drittstaaten angemessenen Datenschutz gewährleisten, wird unter Beachtung des § 55 Z 1 durch Verordnung des Bundeskanzlers festgestellt. Maßgebend für die Angemessenheit des Schutzes ist die Ausgestaltung der Grundsätze des § 6 Abs. 1 in der ausländischen Rechtsordnung und das Vorhandensein wirksamer Garantien für ihre Durchsetzung.

(3) Darüberhinaus ist der Datenverkehr ins Ausland dann genehmigungsfrei, wenn

1. die Daten im Inland zulässigerweise veröffentlicht wurden oder
2. Daten, die für den Empfänger nur indirekt personenbezogen sind, übermittelt oder überlassen werden oder
3. die Übermittlung oder Überlassung von Daten ins Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind, oder
4. Daten aus Datenanwendungen für private Zwecke (§ 45) oder für publizistische Tätigkeit (§ 48) übermittelt werden oder
5. der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat oder
6. ein vom Auftraggeber mit dem Betroffenen oder mit einem Dritten eindeutig im Interesse des Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann oder
7. die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und die Daten rechtmäßig ermittelt wurden, oder
8. die Übermittlung oder Überlassung in einer Standardverordnung (§ 17 Abs. 2

of processing and documentation containing data or to keep or destroy them on his request;

6. to make available to the controller all information necessary to control the compliance with the obligations according to sub-paras. 1 to 5.

(2) Agreements between the controller and the processor concerning the details of the obligations according to para. 1 shall be laid down in writing to perpetuate the evidence.

Transborder Transmission and Committing of Data not Subject to Licensing

§ 12. (1) The transmission [Übermittlung] and committing [Überlassung] of data to recipients in signatory states of the European Economic Area is not subject to any restrictions in terms of § 13. This does not apply to data exchange between public sector controllers [Auftraggeber] in fields that are not subject to the law of the European Union.

(2) No authorisation pursuant to § 13 shall be required for data exchange with recipients in third countries with an adequate level of data protection. The countries that have an adequate level of data protection shall be enumerated in an ordinance [Verordnung] of the Federal Chancellor [Bundeskanzler] in accordance with § 55 sub-para. 1 . The decisive consideration as to the adequacy of the protection shall be the implementation of the principles of § 6 para. 1 in the foreign legal system as well as the existence of effective guarantees for their enforcement.

(3) Furthermore, transborder data exchange shall not require authorisation if

1. the data have been published legitimately in Austria or
2. data are transferred or committed that are only indirectly personal to the recipient or
3. the transborder transmission or committing is authorised by regulations that are equivalent to a statute in the Austrian legal system and are immediately applicable or
4. data from a data application [Daten¬anwendung] for private purposes (§ 45) or for journalistic purposes (§ 48) is transmitted or
5. the data subject [Betroffener] has without any doubt given his consent to the transborder transmission or committing or
6. a contract between the controller and the data subject or a third party that has been concluded clearly in the interest of the data subject cannot be fulfilled except by the transborder transmission of data or
7. the transmission is necessary for the establishment, exercise or defence of legal claims before a foreign authority and the data were collected legitimately or
8. the transmission or committing is expressly named in a standard ordinance

Z 6) oder Musterverordnung (§ 19 Abs. 2) ausdrücklich angeführt ist oder

9. es sich um Datenverkehr mit österreichischen Dienststellen im Ausland handelt oder
10. Übermittlungen oder Überlassungen aus Datenanwendungen erfolgen, die gemäß § 17 Abs. 3 von der Meldepflicht ausgenommen sind.

(4) Wenn eine Übermittlung oder Überlassung von Daten ins Ausland in Fällen, die von den vorstehenden Absätzen nicht erfaßt sind,

1. zur Wahrung eines wichtigen öffentlichen Interesses oder
2. zur Wahrung eines lebenswichtigen Interesses einer Person

notwendig und so dringlich ist, daß die gemäß § 13 erforderliche Genehmigung der Datenschutzkommission nicht eingeholt werden kann, ohne die genannten Interessen zu gefährden, darf sie ohne Genehmigung vorgenommen werden, muß aber der Datenschutzkommission umgehend mitgeteilt werden.

(5) Voraussetzung für die Zulässigkeit jeder Übermittlung oder Überlassung in das Ausland ist die Rechtmäßigkeit der Datenanwendung im Inland gemäß § 7. Bei Überlassungen ins Ausland muß darüber hinaus die schriftliche Zusage des ausländischen Dienstleisters an den inländischen Auftraggeber - oder in den Fällen des § 13 Abs. 5 an den inländischen Dienstleister - vorliegen, daß er die Dienstleisterpflichten gemäß § 11 Abs. 1 einhalten werde. Dies entfällt, wenn die Dienstleistung im Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind.

Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland

§ 13. (1) Soweit der Datenverkehr mit dem Ausland nicht gemäß § 12 genehmigungsfrei ist, hat der Auftraggeber vor der Übermittlung oder Überlassung von Daten in das Ausland eine Genehmigung der Datenschutzkommission (§§ 35 ff) einzuholen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen binden.

(2) Die Genehmigung ist unter Beachtung der gemäß § 55 Z 2 ergangenen Kundmachungen zu erteilen, wenn die Voraussetzungen des § 12 Abs. 5 vorliegen und wenn, ungeachtet des Fehlens eines im Empfängerstaat generell geltenden angemessenen Datenschutzniveaus,

1. für die im Genehmigungsantrag angeführte Übermittlung oder Überlassung im konkreten Einzelfall angemessener Datenschutz besteht; dies ist unter Berücksichtigung aller Umstände zu beurteilen, die bei der Datenverwendung eine Rolle spielen, wie insbesondere die Art der verwendeten Daten, die Zweckbestimmung sowie die Dauer der geplanten Verwendung, das Herkunfts- und das Endbestimmungsland und die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen,

[Standard¬verordnung] (§ 17 para. 2 sub-para. 6) or model ordinance [Musterverordnung] (§ 19 para. 2) or

9. the data exchange is with Austrian governmental missions and offices in foreign countries or
10. the transmissions or committings are made from a data application that is exempted from notification according to § 17 para. 3.

(4) If the transborder transmission or committing in cases not covered by the preceding paragraphs is necessary

1. to safeguard an important public interest or
2. to safeguard a vital interest of a person

and of such urgency that the authorisation of the Data Protection Commission [Datenschutzkommission] required according to § 13 cannot be obtained in time without risk to the above-mentioned interests, it may be performed without a permit, but must be notified to the Data Protection Commission immediately.

(5) The legality of a data application in Austria according to § 7 is a prerequisite for every transborder transmission or committing. Furthermore, transborder committings require the written promise of the processor [Dienstleister] abroad to the domestic controller - or in the case of § 13 para. 5 to the domestic processor - that he shall respect the obligations of a processor according to § 11 para 1. This is not applicable if the processing abroad is provided for in regulations that are equivalent to a law in the Austrian legal system and are immediately applicable.

Transborder Transmission and Committing of Data Subject to Licensing

§ 13. (1) Insofar as a case of transborder data exchange is not exempted from authorisation according to § 12, the controller has to apply for a permit by the Data Protection Commission [Datenschutzkommission] (§ 35) before the transmission [Übermittlung] or committing [Überlassung]. The Data Protection Commission can issue the permit subject to conditions and obligations.

(2) The permit shall be given, taking into consideration the promulgations [Kundmachungen] pursuant to § 55 sub-para. 2, if the requirements of § 12 para. 5 are met, and despite the lack of an adequate general level of data protection in the recipient state

1. an adequate level of data protection exists for the transmission or committing outlined in the application for the permit in this specific case; this is then to be judged considering all circumstances relevant to the use of data [Datenverwendung], such as the type of data used, the purpose and duration of use, the country of origin and final destination as well as the general and sectoral legal provisions, professional rules and security standards applying in the third country; or

Standesregeln und Sicherheitsstandards; oder

2. der Auftraggeber glaubhaft macht, daß die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Hiefür können insbesondere auch vertragliche Zusicherungen des Empfängers sowie einseitige Zusagen des Antragstellers (§ 19 Abs. 2) im Genehmigungsantrag über die näheren Umstände der Datenverwendung im Ausland von Bedeutung sein. Einseitige Zusagen des Antragstellers werden für diesen mit der Registrierung durch die Datenschutzkommission verbindlich.

(3) Bei meldepflichtigen Datenanwendungen hat die Datenschutzkommission eine Ausfertigung jedes Bescheides, mit dem eine Übermittlung oder Überlassung von Daten in das Ausland genehmigt wurde, zum Registrierungsakt zu nehmen und die Erteilung der Genehmigung im Datenverarbeitungsregister (§ 16) anzumerken.

(4) Abweichend von Abs. 1 kann auch ein inländischer Dienstleister die Genehmigung beantragen, wenn er zur Erfüllung seiner vertraglichen Verpflichtungen gegenüber mehreren Auftraggebern jeweils einen bestimmten weiteren Dienstleister im Ausland heranziehen will. Die tatsächliche Überlassung darf jeweils nur mit Zustimmung des Auftraggebers erfolgen. Der Auftraggeber hat der Datenschutzkommission mitzuteilen, aus welcher seiner meldepflichtigen Datenanwendungen die dem Dienstleister genehmigte Überlassung erfolgen soll; dies ist im Datenverarbeitungsregister anzumerken.

(5) Die Übermittlung von Daten an ausländische Vertretungsbehörden oder zwischenstaatliche Einrichtungen in Österreich gilt hinsichtlich der Pflicht zur Einholung von Genehmigungen nach Abs. 1 als Datenverkehr mit dem Ausland.

(6) Hat der Bundeskanzler trotz Fehlens eines im Empfängerstaat generell geltenden angemessenen Schutzniveaus durch Verordnung festgestellt, daß für bestimmte Kategorien des Datenverkehrs mit diesem Empfängerstaat die Voraussetzungen gemäß Abs. 2 Z 1 zutreffen, tritt an die Stelle der Verpflichtung zur Einholung einer Genehmigung die Pflicht zur Anzeige an die Datenschutzkommission. Die Datenschutzkommission hat binnen sechs Wochen ab Einlangen der Anzeige mit Bescheid den angezeigten Datenverkehr zu untersagen, wenn er keiner der in der Verordnung geregelten Kategorien zuzurechnen ist oder den Voraussetzungen gemäß § 12 Abs. 5 nicht entspricht; andernfalls ist die Übermittlung oder Überlassung der Daten in das Ausland zulässig.

2. the controller can satisfactorily demonstrate that the interests in secrecy deserving protection of the data subject [Betroffener] of the planned data exchange will be respected outside of Austria. In particular, contractual guarantees by the recipient as well as unilateral declarations by the applicant (§ 19 para 2) in the application for permit about the more detailed circumstances of the use of data abroad are significant for the decision. Unilateral declarations by the applicant become legally binding for him upon registration by the Data Protection Commission.

(3) In the case of data applications subject to notification, the Data Protection Commission shall put a copy of each ruling [Bescheid] authorising the transborder transmission or committing of data on the notification file and enter the fact that authorisation has been granted into the Data Processing Register [Datenverarbeitungsregister] (§ 16).

(4) Deviating from para. 1, a domestic processors [Dienstleister] can apply for a permit if, in order to fulfil his contractual duties vis-á-vis multiple controllers, he wishes to enlist the service of a specific processor outside of Austria. The actual committing shall only be performed with the consent of the controller. The controller shall report to the Data Protection Commission from which of his data applications subject to notification the authorised committing to the processor shall take place; this is to be entered into the Data Processing Register .

(5) The transmission of data to representations of foreign governments or intergovernmental institutions in Austria shall be treated as transborder data exchange with regard to the requirement for authorisation according to para. 1.

(6) If the Federal Chancellor [Bundeskanzler] has decreed by ordinance [Verordnung] that, despite the lack of an adequate general level of data protection in the recipient state, the requirements according to para. 2 sub-para. 1 are met for specific categories of data exchange with this recipient state, the obligation to obtain a permit is replaced by an obligation to notify the Data Protection Commission. The Data Protection Commission shall prohibit the notified data exchange within six weeks after receiving the notification if it is not attributed to one of the categories regulated in the ordinance [Verordnung] or if it does not fulfil the requirements according to sect. 12 para. 5; otherwise the transmission or committing is permitted.

3. Abschnitt

Datensicherheit

Datensicherheitsmaßnahmen

§ 14. (1) Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, daß die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, daß ihre Verwendung ordnungsgemäß erfolgt und daß die Daten Unbefugten nicht zugänglich sind.

(2) Insbesondere ist, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist,

1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,
2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
3. jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,
4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,
5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,
6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
7. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,
8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

Part 3

Data Security

Data Security Measures

§ 14. (1) Measures to ensure data security shall be taken by all organisational units of a controller [Auftraggeber] or processor [Dienstleister] that use data. Depending on the kind of data used as well as the extent and purpose of the use and considering the state of technical possibilities and economic justifiability it shall be ensured that the data are protected against accidental or intentional destruction or loss, that they are properly used and are not accessible to unauthorised persons.

(2) In particular, the following measures are to be taken insofar as this is necessary with regard to the last sentence of para. 1:

1. The distribution of functions between the organisational units as well as the operatives regarding the use of data [Datenverwendung] shall be laid down expressly,
2. The use of data must be tied to valid orders of the authorised organisational units or operatives,
3. every operative is to be instructed about his duties according to this Federal Act [Bundes¬gesetz] and the internal data protection regulations, including data security regulations,
4. The right of access to the premises of the data controller or processor is to be regulated,
5. The right of access to data and programs is to be regulated as well as the protection of storage media against access and use by unauthorised persons,
6. The right to operate the data processing equipment is to be laid down and every device is to be secured against unauthorised operation by taking precautions for the machines and programs used,
7. Logs shall be kept in order that the processing steps that were actually performed, in particular modifications, consultations and transmissions [Übermittlungen], can be traced to the extent necessary with regard to their permissibility,
8. A documentation shall be kept on the measures taken pursuant to sub-paras. 1 to 7 to facilitate control and conservation of evidence.

These measures must, taking into account the technological state of the art and the cost incurred in their execution, safeguard a level of data protection appropriate with regard to the risks arising from the use and the type of data to be protected.

(3) Nicht registrierte Übermittlungen aus Datenanwendungen, die einer Verpflichtung zur Auskunftserteilung gemäß § 26 unterliegen, sind so zu protokollieren, daß dem Betroffenen Auskunft gemäß § 26 gegeben werden kann. In der Standardverordnung (§ 17 Abs. 2 Z 6) oder in der Musterverordnung (§ 19 Abs. 2) vorgesehene Übermittlungen bedürfen keiner Protokollierung.

(4) Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck - das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes - unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, daß es sich um die Verwendung zum Zweck der Verhinderung oder Verfolgung eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, handelt.

(5) Sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, sind Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird.

(6) Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, daß sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können.

Datengeheimnis

§ 15. (1) Auftraggeber, Dienstleister und ihre Mitarbeiter - das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis - haben Daten aus Datenanwendungen, 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 Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Auftraggeber und Dienstleister haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, daß sie Daten aus Datenanwendungen nur auf Grund von Anordnungen übermitteln und das Datengeheimnis auch nach Beendigung des Arbeits(Dienst)verhältnisses zum Auftraggeber oder Dienstleister einhalten werden.

(3) Unregistered transmissions from data applications [Datenanwendungen] subject to an obligation to grant information pursuant to § 26 shall be logged in such a manner that the right of information [Auskunftsrecht] can be granted to the subject pursuant to § 26. Transmissions provided for in the standard ordinance [Standardverordnung] (§ 17 para. 2 lit. 6) and the model ordinance [Musterverordnung] (§ 19 para. 2) do not require logging.

(4) Logs and documentation data may not be used for purposes that are incompatible with the purpose of the collection [Ermittlung] - viz., monitoring the legitimacy of the use of the logged and documented data files [Datenbestand]. In particular, any further use for the purpose of supervising the data subjects [Betroffener] whose data is contained in the logged data files, as well as for the purpose of monitoring the persons who have accessed the logged data files, or for any purpose other than checking access rights shall be considered incompatible, unless the data is used is for the purpose of preventing or prosecuting a crime according to § 278a StGB (criminal organisation) or a crime punishable with a maximum sentence of more than five years imprisonment.

(5) Unless expressly provided for otherwise by law, logs and documentation data shall be kept for three years. Deviations from this rule shall be permitted to the same extent that the logged or documented data files [Datenbestand] may legitimately be erased earlier or kept longer.

(6) Data security regulations are to be issued and kept available in such a manner that the operatives can inform themselves about the regulations to which they are subject at any time.

Confidentiality of Data

§ 15. (1) Controllers [Auftraggeber], processors [Dienstleister] and their operatives these being the employees and persons comparable to employees shall keep data from uses of data [Datenanwendungen] confidential that have been entrusted or made accessible to them solely for professional reasons, without prejudice to other professional obligations of confidentiality, unless a legitimate reason exists for the transmission [Über¬mittlung] of the entrusted or accessed data (confidentiality of data [Datengeheimnis]).

(2) Operatives shall transmit data only if expressly ordered to do so by their employer. controllers and processors shall oblige their operatives by contract, insofar as they are not already obliged by law, to transmit data from uses of data only if so ordered and to adhere to the confidentiality of data even after the end of their professional relationship with the controller or processor.

(3) Auftraggeber und Dienstleister dürfen Anordnungen zur Übermittlung von Daten nur erteilen, wenn dies nach den Bestimmungen dieses Bundesgesetzes zulässig ist. Sie 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 Datenübermittlung wegen Verstoßes gegen die Bestimmungen dieses Bundesgesetzes kein Nachteil erwachsen.

4. Abschnitt

Publizität der Datenanwendungen

Datenverarbeitungsregister

§ 16. (1) Die Datenschutzkommission hat ein Register der Auftraggeber mit den von ihnen betriebenen Datenanwendungen zum Zweck der Information der Betroffenen zu führen.

(2) 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 Betroffener ist, und soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen des Auftraggebers oder anderer Personen entgegenstehen.

(3) Der Bundeskanzler hat die näheren Bestimmungen über die Führung des Registers durch Verordnung zu erlassen. Dabei ist auf die Richtigkeit und Vollständigkeit des Registers, die Übersichtlichkeit und Aussagekraft der Eintragungen und die Einfachheit der Einsichtnahme Bedacht zu nehmen.

Meldepflicht des Auftraggebers

§ 17. (1) Jeder Auftraggeber hat, soweit in den Abs. 2 und 3 nicht anderes bestimmt ist, vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission mit dem in § 19 festgelegten Inhalt zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten. Diese Meldepflicht gilt auch für Umstände, die nachträglich die Unrichtigkeit und Unvollständigkeit einer Meldung bewirken (Änderungsmeldung). Für manuelle Dateien besteht eine Meldepflicht nur, soweit die Inhalte zumindest einen der Tatbestände des § 18 Abs. 2 Z 1 bis 3 erfüllen.

(1a) Die Meldung ist in elektronischer Form im Wege der vom Bundeskanzler bereit zu stellenden Internetanwendung einzubringen. Die Identifizierung und Authentifizierung kann insbesondere durch die Bürgerkarte (§ 2 Z 10 des E Government-Gesetzes, BGBl. I Nr. 10/2004) erfolgen. Nähere Bestimmungen über die

(3) Controllers and processors may only issue orders for the transmission of data if this is permitted pursuant to the provisions of this Federal Act [Bundesgesetz]. They shall inform the operatives affected by these orders about the transmission orders in force and about the consequences of a violation of data confidentiality.

(4) Without prejudice to the constitutional right to issue instructions [Weisungen] , a refusal to follow an order to transmit data on the grounds that it violates the provisions of this Federal Act shall not be to the operatives detriment.

Part 4

Publicity of Data Applications

Data Processing Register

§ 16. (1 The Data Protection Commission [Datenschutzkommission] shall operate a register of controllers and their data applications [Datenanwendungen] for the purpose information of the data subjects [Betroffene].

(2) Any person may inspect the register. Access to the registration file including the licences contained therein shall be granted if the person applying for inspection can satisfactorily demonstrate that he is a data subject, and as far as no overriding interest in secrecy on part of the controller deserving protection is an obstacle to access.

(3) The Federal Chancellor [Bundeskanzler] shall lay down more specific regulations about the management of the register in an ordinance [Verordnung]. This is to be done with due regard to the correctness and completeness of the register, the clarity and expressiveness of the entries and the ease of access.

Duty of the Controller to Notify

§ 17. (1) Every controller [Auftraggeber] shall, unless provided for otherwise in paras. 2 and 3, before commencing a data application [Datenanwendung], file a notification whose contents are laid down in § 19 with the Data Protection Commission [Datenschutzkommission] for the purpose of registration in the Data Processing Register [Datenverarbeitungsregister]. The duty to notify also applies to all circumstances that subsequently lead to the incorrectness or incompleteness of the notification (notification of change). Such duty of notification applies to manual filing systems only to the extent its contents match at least one of the elements of § 18 para 2 sub-para. 1 to 3.

(1a) The notification is to be filed electronically through a web application to be provided by the Federal Chancellor. Identification and authentication can be performed by using the citizen´s card [Bürgerkarte] (§ 2 para 10 of the E Government Act, Federal Law Gazette I No. 10/2004). Detailed instructions on the identification

Identifizierung und Authentifizierung sind in die gemäß § 16 Abs. 3 zu erlassende Verordnung aufzunehmen. Eine Meldung in Form von E-Mail oder in nicht-elektronischer Form ist für manuelle Dateien sowie bei einem längeren technischen Ausfall der Internetanwendung zulässig.

(2) Nicht meldepflichtig sind Datenanwendungen, die

1. ausschließlich veröffentlichte Daten enthalten oder
2. die Führung von Registern oder Verzeichnissen zum Inhalt haben, die von Gesetzes wegen öffentlich einsehbar sind, sei es auch nur bei Nachweis eines berechtigten Interesses oder
3. nur indirekt personenbezogene Daten enthalten oder
4. von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden (§ 45) oder
5. für publizistische Tätigkeit gemäß § 48 vorgenommen werden oder
6. einer Standardanwendung entsprechen: Der Bundeskanzler kann durch Verordnung Typen von Datenanwendungen und Übermittlungen aus diesen zu Standardanwendungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszwecks und der verarbeiteten Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist. In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen.

(3) Weiters sind Datenanwendungen für Zwecke

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
3. der Sicherstellung der Interessen der umfassenden Landesverteidigung oder
4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten

von der Meldepflicht ausgenommen, soweit dies zur Verwirklichung des Zweckes der Datenanwendung notwendig ist.

Aufnahme der Verarbeitung

§ 18. (1) Der Vollbetrieb einer meldepflichtigen Datenanwendung darf - außer in den Fällen des Abs. 2 - unmittelbar nach Abgabe der Meldung aufgenommen werden.

(2) Meldepflichtige Datenanwendungen, die weder einer Musteranwendung nach

and authentication procedure shall be contained in the ordinance to be rendered according to § 16 para 3. Notification by e-mail or in non-electronic form is admissible for manual filing systems, or in case of a longer lasting technical blackout of the web application.

(2) Data applications are not subject to notification

1. which solely contain published data or
2. whose subject is the management of registers and catalogues that are by law open to inspection by the public, even if a legitimate interest for doing so must be demonstrated or
3. which contain only indirectly personal data or
4. which are carried out by natural persons for activities that are entirely personal or concern just the person's family life (§ 45) or
5. which are carried out for journalistic purposes according to § 48 or
6. correspond to a standard application [Standardanwendung]. The Federal Chancellor [Bundeskanzler] can lay down in an ordinance [Verordnung] that some types of data applications and transmissions [Übermittlung] are standard applications, if they are carried out by a large number of controllers in similar fashion and if a risk to the data subjects' [Betroffener] interest in secrecy deserving protection is unlikely considering the purpose of the use and the processed categories of data [Datenarten]. The ordinance shall list for every Standard Application the authorised categories of data, the categories of data subjects [Betroffenenkreise] and recipients [Empfängerkreise] as well as the maximum period of time during which the data may be stored .

(3) Furthermore, data applications for the purpose of

1. protecting the constitutional institutions of the Republic of Austria or
2. safeguarding the operational readiness of the federal army or
3. safeguarding the interests of comprehensive national defence or
4. protecting important foreign policy, economic or financial interests of the Republic of Austria or the European Union
5. preventing and prosecuting of crimes

shall be exempt from the duty to notify, insofar as this is necessary to achieve the purpose of the data application.

Commencement of Processing

§ 18. (1) A data application [Daten¬anwendung] subject to notification may - except as laid down in para. 2 - take up full operation immediately after the notification has been submitted.

(2) Data applications subject to notification which neither correspond to a Model

§ 19 Abs. 2 entsprechen, noch innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften noch die Verwendung von Daten im Katastrophenfall für die in § 48a Abs. 1 genannten Zwecke betreffen, dürfen, wenn sie

1. sensible Daten enthalten oder
2. strafrechtlich relevante Daten im Sinne des § 8 Abs. 4 enthalten oder
3. die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder
4. in Form eines Informationsverbundsystems durchgeführt werden sollen,

erst nach ihrer Prüfung (Vorabkontrolle) durch die Datenschutzkommission nach den näheren Bestimmungen des § 20 aufgenommen werden.

Notwendiger Inhalt der Meldung

§ 19. (1) Eine Meldung im Sinne des § 17 hat zu enthalten:

1. den Namen (die sonstige Bezeichnung) und die Anschrift des Auftraggebers sowie eines allfälligen Vertreters gemäß § 6 Abs. 3 oder eines Betreibers gemäß § 50 Abs. 1, weiters die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde, und
2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit des Auftraggebers, soweit dies erforderlich ist, und
3. den Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z 2 ergeben, und

3a. die Erklärung, ob die Datenanwendung einen oder mehrere der in § 18 Abs. 2 Z 1 bis 4 oder § 50c Abs. 1 zweiter Satz genannten Tatbestände für die Vorabkontrollpflicht erfüllt, und

4. die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten und
5. die Kreise der von beabsichtigten Übermittlungen Betroffenen, die zu übermittelnden Datenarten und die zugehörigen Empfängerkreise - einschließlich allfälliger ausländischer Empfängerstaaten - sowie die Rechtsgrundlagen der Übermittlung und
6. - soweit eine Genehmigung der Datenschutzkommission notwendig ist - die Geschäftszahl der Genehmigung durch die Datenschutzkommission sowie
7. allgemeine Angaben über die getroffenen Datensicherheitsmaßnahmen im Sinne des § 14, die eine vorläufige Beurteilung der Angemessenheit der Sicherheitsvorkehrungen erlauben.

Application [Musteranwendung] pursuant to § 19 para. 2 nor concern the internal affairs of the churches and religious communities recognised by the state or the processing of data in case of a catastrophy for the purposes named in § 48a al 1 and

1. which involve sensitive data or
2. which involve data about offences according to § 8 para. 4 or
3. whose purpose is to give information on the data subjects [Betroffener] creditworthiness or
4. which are carried out in the form of a joint information system [Informationsverbundsystem],

shall be initiated only after an examination (prior checking) [Vorabkontrolle] by the Data Protection Commission [Datenschutzkommission] in accordance with § 20.

Required Content of the Notification

§ 19. (1) A notification pursuant to § 17 must contain

1. the name (or other designation) and address of the controller [Auftraggeber] and of his representative according to § 6 para. 3 or of the operator pursuant to § 50 para. 1; furthermore the registration number of the controller, insofar as one has been already assigned to him, and
2. the proof of statutory competence or of the legitimate authority that the controller’s activities are permitted, if so required and
3. the purpose of the data application [Datenanwendung] to be registered and the legal basis, as long as this is not included in the information according to sub-para. 2 and

3a. a statement, whether the data application matches one or more of the cases for prior checking named in § 18 para 2 sub-para 1 to 4 or § 50c para 1 second sentence and

4. the categories of data subjects [Betroffenenkreise] and the categories of data [Datenarten] about them that are processed and
5. the categories of data subjects [Betroffenenkreise] affected by intended transmissions [Übermittlungen], the categories of data [Datenarten] to be transmitted and the matching categories of recipients [Empfängerkreise] - including possible recipient states abroad - as well as the legal basis for the transmission and
6. insofar as a permit by the Data Protection Commission [Datenschutzkommission] is required the file number of the permit of the Data Protection Commission as well as
7. a general description of data security measures taken pursuant to § 14, which enable a preliminary assessment of the appropriateness of the security measures.

(2) Der Auftraggeber kann bei Einbringung der Meldung oder danach bis zum Abschluss des Registrierungsverfahrens zusagen, dass er sich beim Betrieb der Datenanwendung bestimmten Auflagen oder Bedingungen unterwerfen oder die Datenanwendung nur befristet betreiben wird. Eine derartige Zusage wird für den Auftraggeber mit der Registrierung durch die Datenschutzkommission rechtsverbindlich. Eine Registrierung darf nur erfolgen, wenn die zugesagte Auflage, Bedingung oder Befristung derart bestimmt ist, dass sie auch von der Datenschutzkommission nach § 21 Abs. 2 ausgesprochen werden könnte.

(3) Wenn eine größere Anzahl von Auftraggebern gleichartige Datenanwendungen vorzunehmen hat und die Voraussetzungen für die Erklärung zur Standardanwendung nicht vorliegen, kann der Bundeskanzler durch Verordnung Musteranwendungen festlegen. Meldungen über Datenanwendungen, die inhaltlich einer Musteranwendung entsprechen, müssen nur folgendes enthalten:

1. die Bezeichnung der Datenanwendung gemäß der Musterverordnung und
2. die Bezeichnung und Anschrift des Auftraggebers sowie den Nachweis seiner gesetzlichen Zuständigkeit oder seiner rechtlichen Befugnis, soweit dies erforderlich ist, und
3. die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde.

(4) Eine Meldung ist mangelhaft, wenn Angaben fehlen, offenbar unrichtig, unstimmig oder so unzureichend sind, daß Einsichtnehmer im Hinblick auf die Wahrnehmung ihrer Rechte nach diesem Bundesgesetz keine hinreichende Information darüber gewinnen können, ob durch die Datenanwendung ihre schutzwürdigen Geheimhaltungsinteressen verletzt sein könnten. Unstimmigkeit liegt insbesondere auch dann vor, wenn der Inhalt einer gemeldeten Datenanwendung durch die gemeldeten Rechtsgrundlagen nicht gedeckt ist.

Prüfungs- und Verbesserungsverfahren

§ 20. (1) Meldungen von Datenanwendungen, die nach Angabe des Auftraggebers nicht einen der Tatbestände des § 18 Abs. 2 Z 1 bis 4 erfüllen, sind nur automationsunterstützt auf ihre Vollständigkeit und Plausibilität zu prüfen. Ist demnach die Meldung nicht fehlerhaft, so ist sie sofort zu registrieren.

(2) Wird bei der automationsunterstützten Prüfung ein Fehler der Meldung festgestellt, so ist dem Auftraggeber die Möglichkeit zur Verbesserung einzuräumen. Gleichzeitig ist er darauf hinzuweisen, dass die Meldung als nicht eingebracht gilt, wenn keine Verbesserung erfolgt oder er auf der Einbringung der unverbesserten Meldung besteht. Im letztgenannten Fall kann der Einbringer die Meldung schriftlich unter Anschluss der ausgedruckten Fehlermeldung der Datenschutzkommission übermitteln, welche die Meldung auf Mangelhaftigkeit im Sinn des § 19 Abs. 4 zu prüfen hat.

(2) The controller may at from time the notification is submitted until the end of the registration procedure promise to respect certain requirements or conditions when operating a data application or to operate the data application only for a limited period of time. A declaration of this type becomes legally binding for the controller upon registration by the Data Protection Commission. A registration may only be made if a promised requirement, the condition or time limit is equally specific to a requirement that could be imposed by the Data Protection Commission according to § 21 para 2.

(3) If a large number of controllers has to carry out data applications in similar fashion and the prerequisites for a Standard Application [Standardanwendung] do not apply, the Federal Chancellor can designate Model Applications [Musteranwendung] by ordinance [Verordnung]. Notifications of data applications whose content corresponds to a Model Application need to contain only the following:

1. the designation of the model application [Musteranwendung] according to the model ordinance [Musterverordnung] and
2. the designation and address of the controller as well as proof of statutory competencies or of legitimate authority, as far as this is required, and
3. the registration number of the controller, insofar as one has been already assigned to him.

(4) A notification is insufficient if information is missing, obviously incorrect, inconsistent or so insufficient that persons accessing the register to safeguard their rights according to this Federal Act [Bundesgesetz] cannot obtain sufficient information as to the issue whether their interests in secrecy deserving protection could be infringed by the data application. In particular, inconsistency is given in case of a deviation of the notified content from the notified legal basis.

Examination and Correction Procedure

§ 20. (1) Notifications of data applications, which according to the information provided by the controller, do not match one of the cases of § 18 para 2 No. 1 to 4, are to be examined only through automatic examination for completeness and plausibility. If, accordingly, the notification is not faulty, it is to be registered immediately.

(2) In case it is determined in the course of the automatic examination that the notification is faulty, the controller is to be granted the opportunity for correction. Simultaneously he is to be informed that the notification shall be regarded as not have been submitted if no correction is made or if he insists on the submitting the uncorrected notification. In the latter case the filing person may transmit the notification in writing, attaching the printed error report, to the data protection commission, which has to examine the notification for defectiveness in the sense of § 19 para 4.

(3) Meldungen, die der Auftraggeber als vorabkontrollpflichtig bezeichnet hat oder von diesem zulässigerweise nicht im Wege der Internetanwendung (§ 17 Abs. 1a) eingebracht wurden, sind auf Mangelhaftigkeit im Sinn des § 19 Abs. 4 zu prüfen.

(4) Ergibt die Prüfung nach § 19 Abs. 4 eine Mangelhaftigkeit der Meldung, so ist dem Auftraggeber innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung unter Setzung einer angemessenen Frist aufzutragen. Im Verbesserungsauftrag ist auf die Rechtsfolgen einer Nichtbefolgung nach Abs. 5 hinzuweisen.

(5) Wird dem Verbesserungsauftrag nicht entsprochen, ist die Registrierung der Meldung durch eine schriftliche Mitteilung abzulehnen. In die Mitteilung sind aufzunehmen:

1. die Punkte, in denen der Verbesserungsauftrag nicht erfüllt wurde und
2. der Hinweis, dass innerhalb von zwei Wochen ab Zustellung bei der Datenschutzkommission ein Antrag gestellt werden kann, über die Ablehnung mit Bescheid abzusprechen.

Nach Absendung der Mitteilung erstattete Verbesserungen sind nicht zu berücksichtigen.

Registrierung

§ 21. (1) Meldungen gemäß § 19 sind in das Datenverarbeitungsregister einzutragen, wenn

1. das Prüfungsverfahren nach § 20 Abs. 1 keinen Fehler ergeben hat oder
2. das Prüfungsverfahren nach § 20 Abs. 2 und 3 keine Mangelhaftigkeit der Meldung ergeben hat oder
3. nach Einlangen einer auf Mangelhaftigkeit zu prüfenden Meldung bei der Datenschutzkommission zwei Monate verstrichen sind, ohne dass ein Verbesserungsauftrag gemäß § 20 Abs. 4 erteilt wurde oder
4. der Auftraggeber die aufgetragenen Verbesserungen (§ 20 Abs. 2 und 4) vorgenommen hat.

Die in der Meldung enthaltenen Angaben über Datensicherheitsmaßnahmen sind im Register nicht ersichtlich zu machen.

(2) Bei Datenanwendungen, die gemäß § 18 der Vorabkontrolle unterliegen, können auf Grund der Ergebnisse des Prüfungsverfahrens dem Auftraggeber Auflagen, Bedingungen oder Befristungen für die Vornahme der Datenanwendung durch Bescheid erteilt werden, soweit dies zur Wahrung der durch dieses Bundesgesetz geschützten Interessen der Betroffenen notwendig ist.

(3) Der Auftraggeber ist von der Durchführung und vom Inhalt der Registrierung in geeigneter Weise zu verständigen.

(3) Notifications which the controller has marked as subject to prior checking or which have been filed not by web application in an admissible manner (§ 17 para 1a) are to be examined for defectiveness in the sense of § 19 para 4.

(4) If the examination according to § 19 para 4 shows the defectiveness of a notification, the controller is to it be instructed within two months after the notification has been received, to correct it within an adequate time period. The instruction for correction has to contain information on the legal consequences of non-compliance according to para 5.

(5) If the instruction for correction [Verbesserungsauftrag] is not fulfilled the registration of the notification is to be denied by written information. This information must contain:

1. the points in which the instruction for correction was not fulfilled and
2. the information, that within two weeks after delivery a motion can be filed with the Data Protection Commission to render a ruling on the refusal.

Corrections filed after sending of the information are not to be taken into consideration.

Registration

§ 21. (1) Notifications pursuant to § 19 are to be entered into the Data Processing Register [Datenverarbeitungsregister] if

1. the examination procedure according to § 20 para 1 has shown no defect or
2. the examination procedure according to § 20 paras 2 and 3 has shown no deficiency of the notification or
3. two months have passed since a notification meant to be examined for deficiency was submitted to the Data Protection Commission without a request for correction having been issued pursuant to § 20 para 4 or
4. the controller has made the corrections which were requested (§ 20 para 2 and 4).

The information on data security measures contained in the notification shall not be entered into the register.

(2) For data applications subject to prior checking [Vorabkontrolle] pursuant to § 18 the execution of the data application may be permitted subject to conditions, requirements and deadlines based on the findings of the checking procedure, insofar as this is necessary to safeguard interests of the data subject [Betroffener] that are protected by this Federal Act [Bundesgesetz].

(3) The controller is to be informed on the registration and its content in an appropriate manner.

(4) Jedem Auftraggeber ist bei der erstmaligen Registrierung eine Registernummer zuzuteilen.

(5) Hat die automationsunterstützte Prüfung nach § 20 Abs. 1 keine Fehlerhaftigkeit der Meldung ergeben, so ist in die Registrierung ein Vermerk aufzunehmen, dass der Meldungsinhalt nur automationsunterstützt geprüft wurde.

Richtigstellung des Registers und Rechtsnachfolge

§ 22. (1) Streichungen aus dem Register und sonstige Änderungen des Registers sind auf Grund einer Änderungsmeldung des registrierten Auftraggebers oder von Amts wegen in den Fällen des Abs. 2, des § 22a Abs. 2 und des § 30 Abs. 6a vorzunehmen. Derartige Änderungen sind für die Dauer von sieben Jahren ersichtlich zu machen.

(2) Gelangen der Datenschutzkommission aus amtlichen Verlautbarungen Änderungen in der Bezeichnung oder der Anschrift des Auftraggebers zur Kenntnis, so sind die Eintragungen von Amts wegen zu berichtigen. Ergibt sich aus einer amtlichen Verlautbarung der Wegfall der Rechtsgrundlage des Auftraggebers, ist dieser von Amts wegen aus dem Register zu streichen. Außerdem ist eine registrierte Datenanwendung zu streichen, wenn eine Befristung des Betriebes (§ 19 Abs. 2, § 21 Abs. 2) abgelaufen ist oder der Datenschutzkommission zur Kenntnis gelangt, dass die Datenanwendung dauerhaft nicht mehr betrieben wird.

(3) Berichtigungen oder Streichungen nach Abs. 2 sind ohne weiteres Ermittlungsverfahren durch Mandatsbescheid (§ 38) zu verfügen.

(4) Der Rechtsnachfolger eines registrierten Auftraggebers kann einzelne oder alle registrierten Meldungen des Rechtsvorgängers übernehmen, wenn er innerhalb von sechs Monaten nach Wirksamkeit der Rechtsnachfolge eine entsprechend glaubhaft gemachte Erklärung gegenüber der Datenschutzkommission abgibt. Dem Rechtsnachfolger kann auf Antrag auch die Registernummer des Rechtsvorgängers übertragen werden, wenn der Rechtsvorgänger jegliche Verarbeitung personenbezogener Daten in Auftraggebereigenschaft eingestellt hat.

Verfahren zur Überprüfung der Erfüllung der Meldepflicht

§ 22a. (1) Die Datenschutzkommission kann jederzeit die Erfüllung der Meldepflicht durch einen Auftraggeber prüfen. Dies gilt sowohl für die Mangelhaftigkeit einer registrierten Meldung im Sinn des § 19 Abs. 4 als auch für die rechtswidrige Unterlassung von Meldungen.

(2) Bei Vorliegen des Verdachtes der Nichterfüllung der Meldepflicht infolge Mangelhaftigkeit einer registrierten Meldung (Abs. 1) oder Unterlassung der Meldung, die über die Fälle des § 22 Abs. 2 hinausgeht, ist ein Verfahren zur Berichtigung des Datenverarbeitungsregisters durchzuführen. Das Verfahren wird durch begründete Verfahrensanordnung eingeleitet, die dem meldepflichtigen Auftraggeber mit einem Auftrag zur Verbesserung (§ 20 Abs. 4) oder einer Aufforderung zur Nachmeldung

(4) A registration number shall be assigned to each controller upon first registration.

(5) If the automatically processed examination according to § 20 para 1 has shown no deficiency of the notification a note is to be made in the registration that the content of the notification was only examined through automatic processing.

Rectification of the Register and Legal Succession

§ 22. (1) Deletions from the register and other amendments of the register are to be made on the basis of an amendment notification by the registered controller or ex officio in the cases of para 2, § 22a para 2 and of § 30 para 6a. Such amendments are to be made visible for the duration of seven years.

(2) If the Data Protection Commission [Daten¬schutz¬kommission] learns through official publications about changes in the designation or address of the controller [Auftraggeber], the entry shall be corrected ex officio. If an official publication states that the legal basis of the controller [Auftraggeber] is no longer valid, the he/she shall be deleted from the register shall ex officio. Also a registered data-application is to be deleted if a time limit for its operation has expired (§19 para 2, § 21 para 2) or the Data Protection Commission learns that the data application is no longer in operation.

(3) Corrections or deletions pursuant to para. 2 are to be ordered without further investigation by provisional rulings [Mandatsbescheid] (§ 38).

(4) The legal successor of a registered controller may take over individual or all registered notifications of the predecessor, if he/she, within six months after the effectiveness of the legal succession, makes a plausible statement to the Data Protection Commission. Upon request, the legal successor may also be granted the register number of the predecessor, if the predecessor has discontinued any processing of personal data in the function of a controller.

Procedure for the control of the fulfilment of the registration obligation

§ 22a. (1) The Data Protection Commission may at any time examine whether a controller has fulfilled the registration obligation. This applies to the deficiency of a registered notification and the sense of § 19 para 4 as well as to the unlawful omission of notifications.

(2) In case it is suspected that the registration obligation has not been fulfilled because of deficiency of a registered notification (para 1) or omission of the notification beyond the cases of § 22 para 2, a procedure to correct the data processing register is to be performed. The procedure is to be instituted by reasoned procedural order to be served to the controller obliged to the notification with the instruction for correction (§ 20 para 4) or with summons for subsequent notification (§ 17 para 1)

(§ 17 Abs. 1) innerhalb gesetzter Frist zuzustellen ist.

(3) Wird einem im Verfahren nach Abs. 2 erteilten Verbesserungsauftrag nicht entsprochen, so ist die Streichung der Meldung mit Bescheid der Datenschutzkommission zu verfügen. Die Streichung kann sich, wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Herstellung des rechtmäßigen Zustandes ausreichend ist, auch nur auf Teile der Meldung beschränken.

(4) Wird einer im Verfahren nach Abs. 2 erteilten Aufforderung zur Nachmeldung nicht entsprochen und die Unterlassung einer Meldung entgegen § 17 Abs. 1 erwiesen, so ist mit Bescheid der Datenschutzkommission der weitere Betrieb der Datenanwendung, soweit er vom Registerstand abweicht, zu untersagen und gleichzeitig Anzeige nach § 52 Abs. 2 Z 1 an die zuständige Behörde zu erstatten.

(5) Ergibt das Verfahren nach Abs. 2 alleine die Unangemessenheit oder die Nichteinhaltung von nach § 19 Abs. 1 Z 7 erklärten Datensicherheitsmaßnahmen, so ist dies mit Bescheid festzustellen und gleichzeitig eine angemessene Frist zur Herstellung ausreichender Datensicherheit zu setzen. Der Auftraggeber hat innerhalb dieser Frist der Datenschutzkommission die getroffenen Maßnahmen mitzuteilen. Sind diese nicht ausreichend, so ist die Streichung der Datenanwendung zu verfügen.

(6) Die Einleitung und der Stand eines Berichtigungsverfahrens nach Abs. 2 ist bei registrierten Meldungen im Datenverarbeitungsregister bis zur Einstellung oder bis zur Herstellung eines rechtmäßigen Zustandes durch Maßnahmen nach den Abs. 3 bis 6 geeignet anzumerken.

Pflicht zur Offenlegung nicht-meldepflichtiger Datenanwendungen

§ 23. (1) Auftraggeber einer Standardanwendung haben jedermann auf Anfrage mitzuteilen, welche Standardanwendungen sie tatsächlich vornehmen.

(2) Nicht-meldepflichtige Datenanwendungen sind der Datenschutzkommission bei Ausübung ihrer Kontrollaufgaben gemäß § 30 offenzulegen.

Informationspflicht des Auftraggebers

§ 24. (1) Der Auftraggeber einer Datenanwendung hat aus Anlaß der Ermittlung von Daten die Betroffenen in geeigneter Weise

1. über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und

2. über Namen und Adresse des Auftraggebers,

zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des

within a deadline set.

(3) If in a procedure an order for correction under para 2 is not complied with, the Data Protection Commission shall order the deletion of the notification by ruling. The deletion may be restricted only to parts of the notification, if this technically possible, gives a meaningful result with regard to the purpose of the data application and is sufficient to create the lawful situation.

(4) If in a procedure according to para 2 a request for subsequent notification is not complied with and the omission of a notification contrary to § 17 para 1 is proven, the Data Protection Commission shall prohibit any further operation of the data application, to the extent deviating from the situation in the register, by a ruling and simultaneously a report is to be made according to § 52 para 2 sub-para. 1 to the authority in charge.

(5) In case the procedure according to para 2 shows only that data safety measures declared in accordance with § 19 para 1 sub-para. 7 are unsuitable or not observed, this is to be stated in a ruling and simultaneously an adequate deadline to be set to provide sufficient data security. The controller shall within such deadline inform the data protection commission about the measures taken. If such are insufficient, the deletion of the data application shall be ordered.

(6) The beginning and the current status of the correction procedure according to para 2 for registered notifications in the data processing register is to be marked in adequate manner till the termination or till a lawful situation has been created by measures according para 3 to 6.

Obligation to Provide Information on Data Applications not Subject to Notification

§ 23. (1) Controllers [Auftraggeber] of a standard application [Standardanwendung] shall inform anyone on request which standard applications they actually carry out.

(2) Data applications not subject to notification shall be disclosed to the Data Protection Commission [Daten¬schutz¬kommission] in pursuit of its supervisory duties according to § 30.

The Controller's Duty to Provide Information

§ 24. (1) The controller [Auftraggeber] of a data application [Datenanwendung] shall inform the data subjects when collecting data in an appropriate manner about

1. the purpose of the data application for which for which the data are collected, and

2. the name and address of the controller,

insofar as this as this information is not already available to the data subject

Falles nicht bereits vorliegen.

(2) Über Abs. 1 hinausgehende Informationen sind in geeigneter Weise zu geben, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist; dies gilt insbesondere dann, wenn

1. gegen eine beabsichtigte Verarbeitung oder Übermittlung von Daten ein Widerspruchsrecht des Betroffenen gemäß § 28 besteht oder
2. es für den Betroffenen nach den Umständen des Falles nicht klar erkennbar ist, ob er zur Beantwortung der an ihn gestellten Fragen rechtlich verpflichtet ist, oder
3. Daten in einem Informationsverbundsystem verarbeitet werden sollen, ohne daß dies gesetzlich vorgesehen ist.

(2a) Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht, hat er darüber unverzüglich die Betroffenen in geeigneter Form zu informieren. Diese Verpflichtung besteht nicht, wenn die Information angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert.

(3) Werden Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Auftraggebers oder aus Anwendungen anderer Auftraggeber ermittelt, darf die Information gemäß Abs. 1 entfallen, wenn

1. die Datenverwendung durch Gesetz oder Verordnung vorgesehen ist oder
2. die Information im Hinblick auf die mangelnde Erreichbarkeit von Betroffenen unmöglich ist oder
3. wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert. Dies liegt insbesondere dann vor, wenn Daten für Zwecke der wissenschaftlichen Forschung oder Statistik gemäß § 46 oder Adreßdaten im Rahmen des § 47 ermittelt werden und die Information des Betroffenen in diesen Bestimmungen nicht ausdrücklich vorgeschrieben ist. Der Bundeskanzler kann durch Verordnung weitere Fälle festlegen, in welchen die Pflicht zur Information entfällt.

(4) Keine Informationspflicht nach Abs. 1 besteht bei jenen Datenanwendungen, die gemäß § 17 Abs. 2 und 3 nicht meldepflichtig sind.

Pflicht zur Offenlegung der Identität des Auftraggebers

§ 25. (1) Bei Übermittlungen und bei Mitteilungen an Betroffene hat der

[Betroffener], with regard to the particular circumstances of the case.

(2) Information beyond the scope of para. 1 shall be given if this is necessary for fair and lawful processing, in particular if

1. the data subject has a right to object to intended processing or transmission of data pursuant to § 28 or
2. it is not clear for the data subject under the circumstances whether he is required by law to reply to the questions posed, or
3. data are to be processed in a joint information system [Informationsverbundsystem] that is not authorised by law.

(2a) If the controller learns that data from his data application are systematically and seriously misused and the data subject may suffer damages, he shall immediately inform the data subject in appropriate manner. Such obligation does not exist if the information – taking into consideration that only minor damage to the data subject is likely and the cost of the information to all persons concerned - .would require an inappropriate effort

(3) Where data have not been collected by asking the data subject, but through transmission [Übermittlung] from another application purpose [Aufgabengebiet] of the same controller or from a data application of another controller, the information according to para. 1 may be omitted

1. if the use of data [Datenverwendung] is provided for by law or an ordinance [Verordnung] or
2. if it is impossible to provide the information because the data subjects cannot be reached or
3. if, considering the improbability of infringements of the data subjects' rights and the expense involved in reaching the data subjects, an unreasonable effort would be required. In particular, this applies if data are collected for purposes of scientific research or statistics pursuant to § 46 or address data pursuant to § 47 and the requirement to inform the data subject is not explicitly stipulated. The Federal Chancellor may determine further cases by ordinance [Verordnung] in which the duty to give information does not apply.

(4) There shall be no duty to provide information according to para 1 regarding such data applications that are not subject to notification pursuant to § 17 para. 2 and 3.

Obligation to Disclose the Identity of the Controller

§ 25. (1) In the case of transmissions [Übermittlungen] and communications to

Auftraggeber seine Identität in geeigneter Weise offenzulegen, sodaß den Betroffenen die Verfolgung ihrer Rechte möglich ist. Bei meldepflichtigen Datenanwendungen ist in Mitteilungen an Betroffene die Registernummer des Auftraggebers anzuführen.

(2) Werden Daten aus einer Datenanwendung für Zwecke einer vom Auftraggeber verschiedenen Person verwendet, ohne daß diese ihrerseits ein Verfügungsrecht über die verwendeten Daten und damit die Eigenschaft eines Auftraggebers in Bezug auf die Daten erlangt, dann ist bei Mitteilungen an den Betroffenen neben der Identität der Person, für deren Zwecke die Daten verwendet werden, auch die Identität des Auftraggebers anzugeben, aus dessen Datenanwendung die Daten stammen. Handelt es sich hiebei um eine meldepflichtige Datenanwendung, ist die Registernummer des Auftraggebers beizufügen. Diese Pflicht trifft sowohl den Auftraggeber als auch denjenigen, in dessen Namen die Mitteilung an den Betroffenen erfolgt.

5. Abschnitt

Die Rechte des Betroffenen

Auskunftsrecht

§ 26. (1) Ein Auftraggeber hat jeder Person oder Personengemeinschaft, die dies schriftlich verlangt und ihre Identität in geeigneter Form nachweist, Auskunft über die zu dieser Person oder Personengemeinschaft verarbeiteten Daten zu geben. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden. Die Auskunft hat die verarbeiteten Daten, die Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hiefür in allgemein verständlicher Form anzuführen. Auf Verlangen eines Betroffenen sind auch Namen und Adressen von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Wenn zur Person des Auskunftswerbers keine Daten vorhanden sind, genügt die Bekanntgabe dieses Umstandes (Negativauskunft). Mit Zustimmung des Auskunftswerbers kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.

(2) Die Auskunft ist nicht zu erteilen, soweit dies zum Schutz des Auskunftswerbers aus besonderen Gründen notwendig ist oder soweit überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen, der Auskunftserteilung entgegenstehen. Überwiegende öffentliche Interessen können sich hiebei aus der Notwendigkeit

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
3. der Sicherung der Interessen der umfassenden Landesverteidigung oder

data subjects [Betroffene], the controller [Auftraggeber] shall disclose his identity in an appropriate manner, so that the data subjects can pursue their rights. In the case of data application [Datenanwendung] subject to notification, communications to the data subject shall carry the controllers registration number.

(2) Where data from a data application are used for purposes of a person other than the controller, without said person receiving a right of disposal and thereby the status of a controller over the used data , the communication to the data subject shall give the identity of the person for whose purposes the data are used as well as the identity of the controller from whose data application the data originate. If this concerns a data application subject to notification, the controller's registration number shall be included in the correspondence. This obligation applies to both the controller and the person in whose name the correspondence to the data subject is communicated.

Part 5

Rights of the Data Subject

Right to Information

§ 26. (1) A controller [Auftraggeber] shall provide any person or group of persons with information about the data being processed about the person or the group of persons who so request in writing and prove his/her identity in an appropriate manner. Subject to the agreement of the controller, the request for information can be made orally. The information shall contain the processed data, the information about their origin, the recipients or categories of recipients [Empfängerkreise] of transmissions [Übermittlungen], the purpose of the use of data [Datenverwendung] as well as its legal basis in intelligible form. Upon request of a data subject, the names and addresses of processors [Dienstleister] shall be disclosed in case they are charged with processing data relating to him. If no data of the person requesting information exist it is sufficient to disclose this fact (negative information). With the consent of the person requesting information, the information may be provided orally alongside with the possibility to inspect and make duplicates or photocopies instead of being provided in writing.

(2) The information shall not be given insofar as this is essential for the protection of the person requesting information for special reasons or insofar as overriding legitimate interests pursued by the controller or by a third party, especially overriding public interests, are an obstacle to furnishing the information. Overriding public interests can arise out of the necessity

1. to protect of the constitutional institutions of the Republic of Austria or
2. to safeguard of the operational readiness of the federal army or
3. to safeguard the interests of comprehensive national defence or

4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten

ergeben. Die Zulässigkeit der Auskunftsverweigerung aus den Gründen der Z 1 bis 5 unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission gemäß § 31 Abs. 4.

(3) Der Auskunftswerber hat am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden.

(4) Innerhalb von acht Wochen nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Auskunftswerber am Verfahren nicht gemäß Abs. 3 mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Auskunftsverweigerung erfordert, folgendermaßen vorzugehen:

Es ist in allen Fällen, in welchen keine Auskunft erteilt wird - also auch weil tatsächlich keine Daten verwendet werden -, anstelle einer inhaltlichen Begründung der Hinweis zu geben, daß keine der Auskunftspflicht unterliegenden Daten über den Auskunftswerber verwendet werden. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.

(6) Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Auskunftswerber im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. In allen anderen Fällen kann ein pauschalierter Kostenersatz von 18,89 Euro verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.

(7) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Auskunftswerber innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die

4. to protect important foreign policy, economic or financial interests of the Republic of Austria or the European Union or
5. to prevent and prosecute crimes.

The right to refuse information for the reasons stated in sub-paras. 1 to 5 is subject to control by the Data Protection Commission [Datenschutzkommission] pursuant to § 30 para. 3 and the special complaint proceeding before the Data Protection Commission pursuant to § 31 para. 4.

(3) Upon inquiry, the person requesting information has to cooperate in the information procedure to a reasonable extent to prevent an unwarranted and disproportionate effort on the part of the controller.

(4) Within eight weeks of the receipt of the request, the information shall be provided or a reason given in writing why the information is not or not completely provided. The information may be refused if the person requesting information has failed to cooperate in the procedure according to para. 3 or has not reimbursed the cost.

(5) In the areas of the executive responsible for the fields described in para. 2 sub-para. 1 to 5, the procedure in a case where public interests require that no information be given shall be as follows:

In all cases where no information is given even when in fact no data on the person requesting information is used instead of giving a reason in substance, an indication shall be given that no data are being used which are subject to the right to information. The legality of such course of action is subject to review by the Data Protection Commission [Datenschutzkommission] pursuant to § 30 para. 3 and the special complaint proceeding before the Data Protection Commission pursuant to § 31 para. 4..

(6) The information shall be given free of charge if it concerns the current data files [Daten¬bestand] of a use of data and if the person requesting information has not yet made a request for information to the same controller regarding the same application purpose [Aufgabengebiet] in the current year. In all other cases a flat rate compensation of 18,89 Euro may be charged; deviations are permitted to cover actually incurred higher expenses. A compensation already paid shall be refunded, irrespective of any claims for damages, if data have been used illegally or if the information has otherwise led to a correction.

(7) As of the moment the controller has knowledge of a request for information, the controller shall not erase the data relating to the person requesting information until four months have passed or in case a complaint is lodged with the Data Protection

Datenschutzkommission bis zum rechtskräftigen Abschluß des Verfahrens nicht vernichten. Diese Frist gilt nicht, wenn einem Löschungsantrag des Auskunftswerbers nach § 27 Abs. 1 Z 2 oder § 28 zu entsprechen ist.

(8) In dem Umfang, in dem eine Datenanwendung für eine Person oder Personengemeinschaft 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.

(9) Für Auskünfte aus dem Strafregister gelten die besonderen Bestimmungen des Strafregistergesetzes 1968 über Strafregisterbescheinigungen.

(10) Ergibt sich eine Auftraggeberstellung auf Grund von Rechtsvorschriften, obwohl die Datenverarbeitung für Zwecke der Auftragserfüllung für einen Dritten erfolgt (§ 4 Abs. 1 Z 4 letzter Satz), kann der Auskunftswerber sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Auskunftswerber, soweit ihm dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des tatsächlichen Auftraggebers mitzuteilen, damit der Auskunftswerber sein Auskunftsrecht gemäß Abs. 1 gegen diesen geltend machen kann. Wird ein Auskunftsbegehren an einen Dienstleister gerichtet und lässt dieses erkennen, dass der Auskunftswerber ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Dienstleister das Auskunftsbegehren unverzüglich an den Auftraggeber weiterzuleiten und dem Auskunftswerber mitzuteilen, dass in seinem Auftrag keine Daten verwendet werden. Der Auftraggeber hat innerhalb von acht Wochen ab Einlangen des Auskunftsbegehrens beim Dienstleister dem Auskunftswerber Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, von einer Auskunftserteilung abzusehen. Wird jedoch in weiterer Folge das Ersuchen direkt an den Auftraggeber gestellt, so hat dieser nach Abs. 5 vorzugehen. Für Betreiber von Informationsverbundsystemen gilt jedoch ausschließlich § 50 Abs. 1.

Recht auf Richtigstellung oder Löschung

§ 27. (1) Jeder Auftraggeber hat unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete Daten richtigzustellen oder zu löschen, und zwar

1. aus eigenem, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder
2. auf begründeten Antrag des Betroffenen.

Commission pursuant to § 31, until the final conclusion of the proceedings. This deadline does not apply if a request for deletion by the person requesting information according to § 27 para 1 sub-para. 2 or § 28 is to be complied with.

(8) To the extent a data application [Daten¬anwendung] is by law open to inspection by a person or group of persons with regard to data processed on them they shall have the right to information in accordance with the provisions providing the right to inspect. To the procedure of inspection (and its refusal) the regulations of the law providing the right of inspection are to be applied. Parts of an information according ton para 1 that are not covered by the right of inspection may, however, be asserted according to this federal law.

(9) For information on Criminal Records [Strafregister], the special regulations of the Criminal Records Act 1968 [Strafregistergesetz 1968] shall apply.

(10) In case legal provisions lead to a qualification as controller, though the data are processed for a third party in order to carry out a job (§ 4 para 1 sub-para. 4 last sentence), the person requesting information may also first direct the request for information to the entity that ordered the job. This entity has to provide the person requesting information, to the extent the one does not know already, with the name and address of the effective controller within two weeks, free of costs, so that the person requesting information may assert his right of information according to para 1 against him. In case a request for information is directed to a service provider and is obvious that the person requesting information mistakes him for the controller of the data application operated by him, the service provider shall forward the request for information immediately to the controller and to inform the person requesting information, that no data are processed by him as controller. Within eight weeks after the request for information has been received by the service provider the controller has to grant information to the person requesting information or argue in writing, for which reason it is not granted or not completely. In those sectors of public administration what are charged to implement the functions named in para 2 sub-para. 1 to 5, information shall not be given to the extent necessary for the protection of public interests. If, subsequently, the request is directed to the controller, such has to act according to para 5. To operators of joint information systems § 50 para 1 is to be applied exclusively.

Right to Rectification and Erasure

§ 27. (1) Every controller shall rectify or erase data that are incorrect or have been processed contrary to the provisions of this Federal Act [Bundesgesetz]

1. on his own, as soon the incorrectness of the data or the inadmissibility of the processing becomes know to him, or
2. on a well founded application by the data subject [Betroffener].

Der Pflicht zur Richtigstellung nach Z 1 unterliegen nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist. Die Unvollständigkeit verwendeter Daten bewirkt nur dann einen Berichtigungsanspruch, wenn sich aus der Unvollständigkeit im Hinblick auf den Zweck der Datenanwendung die Unrichtigkeit der Gesamtinformation ergibt. Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, daß ihre Archivierung rechtlich zulässig ist und daß der Zugang zu diesen Daten besonders geschützt ist. Die Weiterverwendung von Daten für einen anderen Zweck ist nur zulässig, wenn eine Übermittlung der Daten für diesen Zweck zulässig ist; die Zulässigkeit der Weiterverwendung für wissenschaftliche oder statistische Zwecke ergibt sich aus den §§ 46 und 47.

(2) Der Beweis der Richtigkeit der Daten obliegt - sofern gesetzlich nicht ausdrücklich anderes angeordnet ist - dem Auftraggeber, soweit die Daten nicht ausschließlich auf Grund von Angaben des Betroffenen ermittelt wurden.

(3) Eine Richtigstellung oder Löschung von Daten ist ausgeschlossen, soweit der Dokumentationszweck einer Datenanwendung nachträgliche Änderungen nicht zuläßt. Die erforderlichen Richtigstellungen sind diesfalls durch entsprechende zusätzliche Anmerkungen zu bewirken.

(4) Innerhalb von acht Wochen nach Einlangen eines Antrags auf Richtigstellung oder Löschung ist dem Antrag zu entsprechen und dem Betroffenen davon Mitteilung zu machen oder schriftlich zu begründen, warum die verlangte Löschung oder Richtigstellung nicht vorgenommen wird.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in § 26 Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Geheimhaltung erfordern, mit einem Richtigstellungs- oder Löschungsantrag folgendermaßen zu verfahren: Die Richtigstellung oder Löschung ist vorzunehmen, wenn das Begehren des Betroffenen nach Auffassung des Auftraggebers berechtigt ist. Die gemäß Abs. 4 erforderliche Mitteilung an den Betroffenen hat in allen Fällen dahingehend zu lauten, daß die Überprüfung der Datenbestände des Auftraggebers im Hinblick auf das Richtigstellungs- oder Löschungsbegehren durchgeführt wurde. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.

(6) Wenn die Löschung oder Richtigstellung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind bis dahin die zu löschenden Daten für den Zugriff zu sperren und die zu berichtigenden Daten mit einer berichtigenden Anmerkung zu versehen.

(7) Werden Daten verwendet, deren Richtigkeit der Betroffene bestreitet, und läßt

The obligation to rectify data according to sub-para. 1 shall apply only to those data whose correctness is significant for the purpose of the data application [Datenanwendung]. The incompleteness of data shall only justify a claim to rectification if the incorrectness, with regard to the purpose of the data application, results in the entire information being incorrect. As soon as data are no longer needed for the purpose of the data application, they shall be regarded as illegally processed data and shall be erased unless their archiving is legally permitted and unless the access to these data is specially secured. Any further use for another purpose shall be legitimate only if a transmission [Übermittlung] of the data for this purpose is legitimate; the legitimacy of further uses for scientific or statistical purposes is laid down in sects. 46 and 47.

(2) It shall be the obligation of the controller to prove that the data are correct unless specifically provided otherwise by law insofar as the data have not been collected exclusively based on statements made by the data subject.

(3) No rectification or erasure of data is possible insofar as the documentation purpose of a data application does not permit later changes. In such case, the necessary rectifications shall be effected by means of additional comments.

(4) The application for rectification or erasure shall be complied with within eight weeks after receipt and the applicant shall be informed thereof, or a reason in writing shall be given why the requested erasure or rectification was not carried out.

(5) In the areas of the executive responsible for the fields described in § 26 para. 2 sub paras. 1 to 5, the following procedure shall be applied to applications for rectification or erasure, insofar as this is required to safeguard those public interests that require secrecy: The rectification or erasure shall be carried out if the demands of the data subject are justified in the opinion of the controller. The required information pursuant to para. 4 shall in all cases be that a check of the data files [Datenbestand] of the controller with regard to the application for rectification or erasure has been performed. The legality of this course of action is subject to review by the Data Protection Commission [Datenschutzkommission] according to § 30 para. 3 and the special complaint proceeding before the Data Protection Commission pursuant to § 31 para. 4.

(6) If the erasure or rectification of data kept solely on media readable by means of automatic processing systems can be carried out only at specific times for economic reasons, the data to be erased shall be kept inaccessible and a correcting remark shall be attached the data that are to be corrected.

(7) If data are used whose correctness is disputed by the data subject, and if

sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen, so ist auf Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. Der Bestreitungsvermerk darf nur mit Zustimmung des Betroffenen oder auf Grund einer Entscheidung des zuständigen Gerichtes oder der Datenschutzkommission gelöscht werden.

(8) Wurden im Sinne des Abs. 1 richtiggestellte oder gelöschte Daten vor der Richtigstellung oder Löschung übermittelt, so hat der Auftraggeber die Empfänger dieser Daten hievon in geeigneter Weise zu verständigen, sofern dies keinen unverhältnismäßigen Aufwand, insbesondere im Hinblick auf das Vorhandensein eines berechtigten Interesses an der Verständigung, bedeutet und die Empfänger noch feststellbar sind.

(9) Die Regelungen der Abs. 1 bis 8 gelten für das gemäß Strafregistergesetz 1968 geführte Strafregister sowie für öffentliche Bücher und Register, die von Auftraggebern des öffentlichen Bereichs geführt werden, nur insoweit als für

1. die Verpflichtung zur Richtigstellung und Löschung von Amts wegen oder
2. das Verfahren der Durchsetzung und die Zuständigkeit zur Entscheidung über Berichtigungs- und Löschungsanträge von Betroffenen

durch Bundesgesetz nicht anderes bestimmt ist.

Widerspruchsrecht

§ 28. (1) Sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder Betroffene das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber der Datenanwendung Widerspruch zu erheben. Der Auftraggeber hat bei Vorliegen dieser Voraussetzungen die Daten des Betroffenen binnen acht Wochen aus seiner Datenanwendung zu löschen und allfällige Übermittlungen zu unterlassen.

(2) Gegen eine nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datenanwendung kann der Betroffene jederzeit auch ohne Begründung seines Begehrens Widerspruch erheben. Die Daten sind binnen acht Wochen zu löschen.

(3) § 27 Abs. 4 bis 6 gelten auch in den Fällen der Abs. 1 und 2.

Die Rechte des Betroffenen bei der Verwendung nur indirekt personenbezogener Daten

§ 29. Die durch die §§ 26 bis 28 gewährten Rechte können nicht geltend gemacht werden, soweit nur indirekt personenbezogene Daten verwendet werden.

neither their correctness or incorrectness can be established, an entry about the dispute [Bestreitungsvermerk] shall be attached upon request by the data subject. The entry about the dispute shall be erased only with the consent of the data subject or on grounds of a decision of the competent court of law or of the Data Protection Commission.

(8) If data that were rectified or erased in terms of para. 1 were transmitted before having been rectified or erased, the controller shall inform the recipient of the data by appropriate means, insofar as this does not constitute an unreasonable effort, in particular with regard to a legitimate interest in the information, and that the recipient can still be determined.

(9) The provisions of para. 1 to 8 shall be applied to the criminal records [Strafregister], kept according to the Criminal Records Act 1968 [Strafregistergesetz 1968] as well as to public books and registers kept by public sector controllers only insofar as

1. the obligation to rectification and erasure ex officio or
2. the procedure to assert and the competence to decide applications to rectification and erasure of data subjects

is not regulated otherwise by federal law.

Right to Object

§ 28. (1) Insofar as a use of data [Datenverwendung] is not authorised by law, every data subject [Betroffener] shall have the right to raise an objection with the controller [Auftraggeber] of the data application [Datenanwendung] against the use of data because of an infringement of an overriding interest in secrecy deserving protection arising from his special situation. If the requirements are met, the controller shall erase the data relating to the data subject within eight weeks from his data application and shall refrain from transmitting the data.

(2) If the inclusion of data in a data application open to inspection by the public is not mandated by law, the data subject can object at any time and without any need to give reasons for his desire. The data shall be erased within eight weeks.

(3) § 27 para 4 to 6 shall also be applied in the cases of paras 1 and 2.

Rights of the Data Subject concerning the Use of only Indirectly Personal Data

§ 29. The rights granted in sects. 26 to 28 cannot be exercised insofar as only indirectly personal data are used.

6. Abschnitt

Rechtsschutz

Kontrollbefugnisse der Datenschutzkommission

§ 30. (1) Jedermann kann sich wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten eines Auftraggebers oder Dienstleisters nach diesem Bundesgesetz mit einer Eingabe an die Datenschutzkommission wenden.

(2) Die Datenschutzkommission kann im Fall eines begründeten Verdachtes auf Verletzung der im Abs. 1 genannten Rechte und Pflichten Datenanwendungen überprüfen. Hiebei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenanwendungen und diesbezügliche Unterlagen begehren.

(2a) Sofern sich eine zulässige Eingabe nach Abs. 1 oder ein begründeter Verdacht nach Abs. 2 auf eine meldepflichtige Datenanwendung (Datei) bezieht, kann die Datenschutzkommission die Erfüllung der Meldepflicht überprüfen und erforderlichenfalls nach den §§ 22 und 22a vorgehen.

(3) Datenanwendungen, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegen, dürfen auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden. Dies gilt auch für jene Bereiche der Vollziehung, in welchen ein Auftraggeber des öffentlichen Bereichs die grundsätzliche Anwendbarkeit der §§ 26 Abs. 5 und 27 Abs. 5 in Anspruch nimmt.

(4) Zum Zweck der Einschau ist die Datenschutzkommission nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) berechtigt, Räume, in welchen Datenanwendungen 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. Der Auftraggeber (Dienstleister) hat die für die Einschau notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Auftraggebers (Dienstleisters) und Dritter auszuüben.

(5) Informationen, die der Datenschutzkommission oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Dazu zählt auch die Verwendung für Zwecke der gerichtlichen Rechtsverfolgung durch den Einschreiter oder die Datenschutzkommission nach § 32. Im Übrigen besteht die Pflicht zur Verschwiegenheit auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, dass dann, wenn die

Part 6

Legal Remedies

Duties of Supervision of the Data Protection Commission

§ 30. (1) Anyone shall have the right to lodge an application with the Data Protection Commission [Daten¬schutz¬kommission] because of an alleged infringement of his rights or obligations concerning him pursuant to this Federal Act [Bundesgesetz] by a controller [Auftraggeber] or processor [Dienstleister].

(2) The Data Protection Commission shall have the right to examine data applications [Daten¬anwendungen] in case of reasonable suspicion of an infringement of the rights and obligations mentioned in para. 1. It can order the controller or processor of the examined data application to give all necessary clarifications and to grant access to data applications and relevant documents.

(2a) In case an application admissible according to para 1 or a reasonable suspicion according to para 2 refers to a data application (filing system) subject to the obligation of notification, the data protection commission may examine whether the notification obligation has been fulfilled and eventually proceed according to §§ 22 and 22a.

(3) Data applications subject to prior checking [Vorabkontrolle] pursuant to § 18 para. 2 may be examined without a suspicion of illegal data use. The same applies to those fields of the government where a public sector controller claims that sects. 26 para. 5 and 27 para. 5 are to be applied.

(4) For purposes of the inspection, the Data Protection Commission shall have the right, after having informed the owner of said rooms and the controller (processor), to enter rooms where data applications are carried out, operate data processing equipment, run the processing to be examined and to make copies of the storage media to the extent absolutely required for the exercise of the right to examination. The controller (processor) shall render the assistance necessary for the examination. The supervisory rights are to be exercised in a way that least interferes with the rights of the controller (processor) and third parties.

(5) Information acquired by the Data Protection Commission or its representatives during any examination shall be used only for supervisory purposes in the context of the execution of data protection regulations. This includes the use for purposes of litigation at courts by the person involved or the Data Protection Commission according to § 22. Incidentally, the obligation to confidentiality also exists before courts and administrative authorities, in particular fiscal authorities, with the reservation that, if the examination leads to probable cause to believe that a crime

Einschau den Verdacht einer strafbaren Handlung nach den §§ 51 oder 52 dieses Bundesgesetzes, einer strafbaren Handlung nach den §§ 118a, 119, 119a, 126a bis 126c, 148a oder § 278a des Strafgesetzbuches, 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, BGBl. Nr. 631/1975, zu entsprechen ist.

(6) Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzkommission, sofern nicht Maßnahmen nach den §§ 22 und 22a oder nach Abs. 6a zu treffen sind, Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzkommission je nach der Art des Verstoßes von Amts wegen insbesondere

1. Strafanzeige nach §§ 51 oder 52 erstatten, oder
2. bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 5 erheben, oder
3. bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, dass der Empfehlung der Datenschutzkommission entsprochen wird, oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzkommission der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.

(6a) Liegt durch den Betrieb einer Datenanwendung eine wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen (Gefahr im Verzug) vor, so kann die Datenschutzkommission die Weiterführung der Datenanwendung mit Bescheid gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG, BGBl. Nr. 51, untersagen. Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Wird einer Untersagung nicht sogleich Folge geleistet, ist Strafanzeige nach § 52 Abs. 1 Z 3 zu erstatten. Nach Rechtskraft einer Untersagung nach diesem Absatz ist ein Berichtigungsverfahren nach § 22a Abs. 2 formlos einzustellen. Die Datenanwendung ist im Umfang der Untersagung aus dem Register zu streichen.

(7) Der Einschreiter ist darüber zu informieren, wie mit seiner Eingabe verfahren wurde.

Beschwerde an die Datenschutzkommission

§ 31. (1) Die Datenschutzkommission erkennt über Beschwerden von Personen oder Personengemeinschaften, die behaupten, in ihrem Recht auf Auskunft nach § 26

according to sects. 51 and 52 of this Federal Act [Bundesgesetz] or a criminal act according 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, a report shall be made and requests for assistance according to § 76 Code of Criminal Procedure, Federal Law Gazette No. 631/1974 regarding such crimes and offences shall be complied with.

(6) To establish the rightful state, the Data Protection Commission can issue recommendations, unless measures according to §§ 22 and 22a or para 6a are to be taken an appropriate period for compliance shall be set if required. If a recommendation is not obeyed within the set period, the Data Protection Commission shall, depending on the kind of transgression and ex officio,

1. bring a criminal charge pursuant to sects. 51 or 52, or
2. in case of severe transgressions by a private sector controller file a lawsuit before the competent court of law pursuant to § 32 para. 5, or
3. in case of a transgression by an organ of a territorial corporate body [Gebietskörperschaft], involve the competent highest authority. This authority shall within an appropriate period, not exceeding twelve weeks, take measures to ensure that the recommendation of the Data Protection Commission is complied with or inform the Data Protection Commission why the recommendation is not complied with. The reason may be publicised by the Data Protection Commission in an appropriate manner as far as not contrary to official secrecy.

(6a) In case the operation of a data application causes an serious and immediate danger to interests of secrecy of the data subject deserving protection (imminent danger) the Data Protection Commission may prohibit the continuation of the data application by ruling in accordance with § 57 para 1 of the General Administrative Act 1991, Federal Law Gazette No. 51. The continuation may also be prohibited only partially if this technically possible, gives a meaningful result with regard to the purpose of the data application and is sufficient to eliminate the risk. If the ban is not complied with the offence is to be reported according to § 52 para 1 sub-para 3. If a ban under this para has become final, any running procedure for correction according to § 22a para 2 is to be discontinued informally. According to the extent of the ban the data application is to be deleted from the register.

(7) The intervening party shall be informed as to how his intervention was dealt with.

Complaint before the Data Protection Commission

§ 31. (1) The Data Protection Commission [Datenschutzkommission] shall decide on complaints of persons or group of persons who allege to have been infringed in their

oder nach § 50 Abs. 1 dritter Satz oder in ihrem Recht auf Darlegung einer automatisierten Einzelentscheidung nach § 49 Abs. 3 verletzt zu sein, soweit sich das Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) nicht auf die Verwendung von Daten für Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit bezieht.

(2) Die Datenschutzkommission erkennt weiters über Beschwerden von Personen oder Personengemeinschaften, die behaupten, in ihrem Recht auf Geheimhaltung (§ 1 Abs. 1) oder in ihrem Recht auf Richtigstellung oder auf Löschung (§§ 27 und 28) verletzt zu sein, sofern der Anspruch nicht nach § 32 Abs. 1 vor einem Gericht geltend zu machen ist oder sich gegen ein Organ im Dienste der Gesetzgebung oder der Gerichtsbarkeit richtet.

(3) Die Beschwerde hat zu enthalten:

1. die Bezeichnung des als verletzt erachteten Rechts,
2. soweit dies zumutbar ist, die Bezeichnung des Rechtsträgers 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 stützt,
5. das Begehren, die behauptete Rechtsverletzung festzustellen und
6. die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist.

(4) Einer Beschwerde nach Abs. 1 sind außerdem das zu Grunde liegende Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) und eine allfällige Antwort des Beschwerdegegners anzuschließen. Einer Beschwerde nach Abs. 2 sind außerdem der zu Grunde liegende Antrag auf Richtigstellung oder Löschung und eine allfällige Antwort des Beschwerdegegners anzuschließen.

(5) Die der Datenschutzkommission durch § 30 Abs. 2 bis 4 eingeräumten Kontrollbefugnisse kommen ihr auch in Beschwerdeverfahren nach Abs. 1 und 2 gegenüber dem Beschwerdegegner zu. Ebenso besteht auch hinsichtlich dieser Verfahren die Verschwiegenheitspflicht nach § 30 Abs. 5.

(6) Im Fall der Einbringung einer zulässigen Beschwerde nach Abs. 1 oder 2 ist ein auf Grund einer Eingabe nach § 30 Abs. 1 über denselben Gegenstand eingeleitetes Kontrollverfahren durch eine entsprechende Information (§ 30 Abs. 7) zu beenden. Die Datenschutzkommission kann aber dennoch auch während der Anhängigkeit des Beschwerdeverfahrens von Amts wegen nach § 30 Abs. 2 vorgehen, wenn ein begründeter Verdacht einer über den Beschwerdefall hinausgehenden Verletzung datenschutzrechtlicher Verpflichtungen besteht. § 30 Abs. 3 bleibt unberührt.

(7) Soweit sich eine Beschwerde nach Abs. 1 oder 2 als berechtigt erweist, ist ihr Folge zu geben und die Rechtsverletzung festzustellen. Ist eine festgestellte Verletzung

right for information according to § 26 or § 50 para 1 third phrase or in their right to be informed about an automatically processed individual decision according to § 49 para 3 insofar as the request for information (the application for information or disclosure) does not concern the use of data [Datenverwendung] for acts in the service of legislation or jurisdiction.

(2) Furthermore, the Data Protection Commission shall decide on complaints of persons or groups of persons who allege to have been infringed in their right to secrecy (§ 1 para 1) or in their right to correction or deletion (§§ 27 and 28), to the extent the right is not to be asserted under § 32 para 1 before a court or is not directed against an organ in the service of legislation or jurisdiction.

(3) The complaint must contain:

1. the description of the right considered to be infringed,
2. to the extent reasonable, the description of the legal entity or the organ, which is deemed to be responsible for the alleged infringement (opponent of the complaint),
3. the facts from which the infringement is derived,
4. the reasons for which the unlawfulness is alleged,
5. the request to determine the alleged infringement and
6. the details which are necessary in order to decide whether the complaint has been filed in due time.

(4) A complaint according to para 1 must be accompanied by the pertinent request for information (the application for information or presentation) and an reply by the opponent to the complaint, if any. A complaint according to para 2 must be accompanied by the pertinent request for correction or deletion and an answer of the opponent to the complaint, if any.

(5) The control rights granted to the Data Protection Commission according to § 30 paras 2 to 4 also apply to the complaint procedure according to para 1 and 2 vis-a-vis the opponent to the complaint. Also, the duty of confidentiality according to § 30 para 5 applies to this procedure.

(6) In case of filing of an admissible complaint according to paras 1 or 2 a control procedure instituted on an application based on § 30 para 1 on the same issue is to be discontinued merely by giving information (§ 30 para 7). Nevertheless, the Data Protection Commission may proceed even when the complaint procedure is pending ex officio according to § 30 para 2, if reasonable suspicion exists on an infringement of obligations under the data protection provisions beyond the case of complaint. § 30 para 3 remains unaffected.

(7) To the extent a complaint according to paras 1 or 2 is shown to be justified, it is to be granted and the infringement to be stated. If a stated infringement of the right of

im Recht auf Auskunft (Abs. 1) einem Auftraggeber des privaten Bereichs zuzurechnen, so ist diesem auf Antrag zusätzlich die – allenfalls erneute – Reaktion auf das Auskunftsbegehren nach § 26 Abs. 4, 5 oder 10 in jenem Umfang aufzutragen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen. Soweit sich die Beschwerde als nicht berechtigt erweist, ist sie abzuweisen.

(8) Ein Beschwerdegegner, gegen den wegen Verletzung in Rechten nach den §§ 26 bis 28 Beschwerde erhoben wurde, kann bis zum Abschluss des Verfahrens vor der Datenschutzkommission durch Reaktionen gegenüber dem Beschwerdeführer gemäß § 26 Abs. 4 oder § 27 Abs. 4 die behauptete Rechtsverletzung nachträglich beseitigen. Erscheint der Datenschutzkommission durch derartige Reaktionen des Beschwerdegegners die Beschwerde als gegenstandslos, so hat sie den Beschwerdeführer dazu zu hören. Gleichzeitig ist er darauf aufmerksam zu machen, dass die Datenschutzkommission das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begründet, warum er die ursprünglich behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet. Wird durch eine derartige Äußerung des Beschwerdeführers die Sache ihrem Wesen nach geändert (§ 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 Beschwerdeverfahren formlos einzustellen und der Beschwerdeführer davon zu verständigen. Verspätete Äußerungen sind nicht zu berücksichtigen.

Begleitende Maßnahmen im Beschwerdeverfahren

§ 31a. (1) Sofern sich eine zulässige Beschwerde nach § 31 Abs. 2 auf eine meldepflichtige Datenanwendung (Datei) bezieht, kann die Datenschutzkommission die Erfüllung der Meldepflicht überprüfen und erforderlichenfalls nach den §§ 22 und 22a vorgehen.

(2) Macht der Beschwerdeführer im Rahmen einer Beschwerde nach § 31 Abs. 2 eine wesentliche Beeinträchtigung seiner schutzwürdigen Geheimhaltungsinteressen durch die Verwendung seiner Daten glaubhaft, so kann die Datenschutzkommission nach § 30 Abs. 6a vorgehen.

(3) Ist in einem Verfahren nach § 31 Abs. 2 die Richtigkeit von Daten strittig, so ist vom Beschwerdegegner bis zum Abschluss des Verfahrens ein Bestreitungsvermerk anzubringen. Erforderlichenfalls hat dies die Datenschutzkommission auf Antrag des Beschwerdeführers mit Mandatsbescheid anzuordnen.

(4) Beruft sich ein Auftraggeber des öffentlichen Bereichs bei einer Beschwerde wegen Verletzung des Auskunfts-, Richtigstellungs- oder Löschungsrechts gegenüber der Datenschutzkommission auf die §§ 26 Abs. 5 oder 27 Abs. 5, so hat diese nach Überprüfung der Notwendigkeit der Geheimhaltung die geschützten öffentlichen Interessen in ihrem Verfahren zu wahren. Kommt sie zur Auffassung, dass die

information (para 1) falls under the responsibility of a controller in the private sector, he/she, upon request, in addition, is to be instructed to give - again - an answer to the request for information according to § 26 para 4, 5 or 10, in the extent required, to eliminate the infringement having been stated. To the extent the complaint is not found to be justified, it is to be rejected.

(8) An opponent against whom a complaint has been filed for infringement of rights according to §§ 26 to 28, may, till the end of the proceedings before the data protection commission, by communicating with the complaining person according to § 26 para 4 or § 27 para 5, subsequently eliminate the alleged infringement. If the data protection commission deems the complaint to be settled by such reactions of the opponent to the complaint, it shall hear the person complaining on this. Simultaneously he/she is to be informed, that the Data Protection Commission will informally end the procedure, if he/she does not establish within an adequate period, for which reason he/she still does not consider the originally alleged infringement to be eliminated at least partially. If such answer of the person complaining modifies the merits of the case (§ 13 para 8 General Administrative Act) the original complaint is to be deemed withdrawn and simultaneously a new complaint to be deemed filed. In this case the original complaint procedure is also to be ended informally and the person complaining to be informed correspondingly. Belated answers are to be ignored.

Accompanying measures in the complaint procedure

§ 31a. (1) In so far an admissible complaint according to § 31 para 2 refers to a data application subject to the obligation of notification, the data protection commission may examine whether the obligation for notification has been fulfilled and eventually proceed according to §§ 22 and 22a.

(2) If the person complaining establishes a prima facie case of serious infringement to his/her interests for confidentiality deserving protection within the frame of a complaint according ot § 31 para 2 by use of his/her data, the data protection commission may proceed according to § 30 para 6a.

(3) If in a proceeding according to § 31 para 2 the correctness of data is controversial, the opponent to the complaint shall place a note of the dispute [Bestreitungsvermerk] till the proceedings are terminated. If necessary, upon request of the person complaining, the Data Protection Commission shall order this done by provisional rulings.

(4) If a public sector controller invokes sects. 26 para. 5 or 27 para. 5 vis-á-vis the Data Protection Commission concerning a complaint because of an infringement of the rights to information, rectification and erasure, the Data Protection Commission shall, after having examined the necessity of confidentiality, safeguard the protected public interests during the proceedings. If the Data Protection Commission comes to the

Geheimhaltung von verarbeiteten Daten gegenüber dem Betroffenen nicht gerechtfertigt war, ist die Offenlegung der Daten mit Bescheid aufzutragen. Gegen diese Entscheidung der Datenschutzkommission kann die belangte Behörde Beschwerde an den Verwaltungsgerichtshof erheben. Wurde keine derartige Beschwerde eingebracht und wird dem Bescheid der Datenschutzkommission binnen acht Wochen nicht entsprochen, so hat die Datenschutzkommission die Offenlegung der Daten gegenüber dem Betroffenen selbst vorzunehmen und ihm die verlangte Auskunft zu erteilen oder ihm mitzuteilen, welche Daten bereits berichtigt oder gelöscht wurden. Die ersten beiden Sätze gelten in Verfahren nach § 30 sinngemäß.

conclusion that it was not justified to keep the processed data secret from the data subject, the disclosure of the data shall be ordered by a ruling [Bescheid]. The authority against whom action was taken may lodge an appeal against this decision with the administrative court [Verwaltungsgerichtshof]. If no such appeal is made and the ruling [Bescheid] of the Data Protection Commission is not complied within eight weeks, the Data Protection Commission itself shall carry out the disclosure to the data subject and shall communicate to him the desired information or inform him which data have been rectified or erased. In proceedings according to § 30 the first two sentences are to be applied accordingly.

Anrufung der Gerichte

§ 32. (1) Ansprüche wegen Verletzung der Rechte einer Person oder Personengemeinschaft auf Geheimhaltung, auf Richtigstellung oder auf Löschung gegen natürliche Personen, Personengemeinschaften oder Rechtsträger, die in Formen des Privatrechts eingerichtet sind, sind, soweit diese Rechtsträger bei der behaupteten Verletzung nicht in Vollziehung der Gesetze tätig geworden sind, auf dem Zivilrechtsweg geltend zu machen.

(2) Sind Daten entgegen den Bestimmungen dieses Bundesgesetzes verwendet worden, so hat der Betroffene Anspruch auf Unterlassung und Beseitigung des diesem Bundesgesetz widerstreitenden Zustandes.

(3) Zur Sicherung der auf dieses Bundesgesetz gestützten Ansprüche auf Unterlassung können einstweilige Verfügungen erlassen werden, auch wenn die in § 381 EO bezeichneten Voraussetzungen nicht zutreffen. Dies gilt auch für Verfügungen über die Verpflichtung zur Anbringung eines Bestreitungsvermerks.

(4) Für Klagen und Anträge auf Erlassung einer einstweiligen Verfügung nach diesem Bundesgesetz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Kläger (Antragsteller) seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen (Anträge) können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder eine Niederlassung hat.

(5) Die Datenschutzkommission hat in Fällen, in welchen der begründete Verdacht einer schwerwiegenden Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs besteht, gegen diesen eine Feststellungsklage (§ 228 ZPO) bei dem gemäß Abs. 4 zweiter Satz zuständigen Gericht zu erheben.

(6) Die Datenschutzkommission hat, wenn ein Einschreiter (§ 30 Abs. 1) es verlangt und es zur Wahrung der nach diesem Bundesgesetz geschützten Interessen einer größeren Zahl von natürlichen Personen geboten ist, einem Rechtsstreit auf Seiten des Einschreiters als Nebenintervenient (§§ 17 ff ZPO) beizutreten.

Court Action

§ 32. (1) Claims for infringement of the rights of a person or a group of persons to secrecy, rectification and erasure against natural persons, groups of persons or legal entities established in forms of private law, are, as long as such legal entities were not acing to enforce laws when their rights were infringed, shall be brought before the civil courts.

(2) If data have been used contrary to the provisions of this Federal Act [Bundesgesetz], the data subject shall have the right to sue for an end to such unlawful condition.

(3) In order to safeguard the legal right to put an end to an unlawful state an injunction may be issued even if the requirements mentioned in § 381 Foreclosure Act are not fulfilled. This also applies to orders to make a note about the dispute [Bestreitungsvermerk].

(4) Complaints and applications for injunctions pursuant to this Federal Act shall in the first instance be lodged with the regional civil court [Landesgericht] in whose district the plaintiff (applicant) has his domicile or seat. Actions (applications) may, however, also be brought before the regional civil court in whose district the defendant has his domicile or seat or branch office.

(5) The Data Protection Commission [Datenschutzkommission] shall, in a case where there is probable cause to believe that a serious data protection infringement has been committed by a private sector controller, file an action for a declaratory judgement (§ 228 Code of Civil Procedure) [Feststellungsklage] in the court that is competent pursuant to para. 4 second sentence.

(6) On request of an intervening party (§ 30 para 1) the Data Protection Commission shall, if such action appears necessary to safeguard the protected interests of a large number of natural persons pursuant to this Federal Act, intervene in the proceedings in support of the intervening party as an intervening third party [Nebenintervenient] (§§ 17 et seq. of the Code of Civil Procedure).

(7) Anlässlich einer zulässigen Klage nach Abs. 1, die sich auf eine nach Ansicht des Gerichts meldepflichtige Datenanwendung bezieht, kann das Gericht die Datenschutzkommission um Überprüfung nach den §§ 22 und 22a ersuchen. Die Datenschutzkommission hat das Gericht vom Ergebnis der Überprüfung zu verständigen. Dieses ist sodann vom Gericht auch den Parteien bekannt zu geben, sofern das Verfahren noch nicht rechtskräftig beendet ist.

Schadenersatz

§ 33. (1) Ein Auftraggeber oder Dienstleister, der Daten schuldhaft entgegen den Bestimmungen dieses Bundesgesetzes verwendet, hat dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. Werden durch die öffentlich zugängliche Verwendung der in § 18 Abs. 2 Z 1 bis 3 genannten Datenarten schutzwürdige Geheimhaltungsinteressen eines Betroffenen in einer Weise verletzt, die einer Eignung zur Bloßstellung gemäß § 7 Abs. 1 des Mediengesetzes, BGBl. Nr. 314/1981, gleichkommt, so gilt diese Bestimmung auch in Fällen, in welchen die öffentlich zugängliche Verwendung nicht in Form der Veröffentlichung in einem Medium geschieht. Der Anspruch auf angemessene Entschädigung für die erlittene Kränkung ist gegen den Auftraggeber der Datenverwendung geltend zu machen.

(2) Der Auftraggeber und der Dienstleister haften auch für das Verschulden ihrer Leute, soweit deren Tätigkeit für den Schaden ursächlich war.

(3) Der Auftraggeber kann sich von seiner Haftung befreien, wenn er nachweist, daß der Umstand, durch den der Schaden eingetreten ist, ihm und seinen Leuten (Abs. 2) nicht zur Last gelegt werden kann. Dasselbe gilt für die Haftungsbefreiung des Dienstleisters. Für den Fall eines Mitverschuldens des Geschädigten oder einer Person, deren Verhalten er zu vertreten hat, gilt § 1304 ABGB.

(4) Die Zuständigkeit für Klagen nach Abs. 1 richtet sich nach § 32 Abs. 4.

Gemeinsame Bestimmungen

§ 34. (1) Der Anspruch auf Behandlung einer Eingabe nach § 30, einer Beschwerde nach § 31 oder einer Klage nach § 32 erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, einbringt. Dies ist dem Einschreiter im Falle einer verspäteten Eingabe gemäß § 30 mitzuteilen; verspätete Beschwerden nach § 31 und Klagen nach § 32 sind zurückzuweisen.

(2) Eingaben nach § 30, Beschwerden nach § 31, Klagen nach § 32 sowie Schadenersatzansprüche nach § 33 können nicht nur auf die Verletzung der Vorschriften dieses Bundesgesetzes, sondern auch auf die Verletzung von datenschutzrechtlichen Vorschriften eines anderen Mitgliedstaates der Europäischen

(7) At the occasion of an admissible claim according to para 1 referring to a data application subject to the obligation of notification according to the view of the court, the court may request the data protection commission for a review according to §§ 22 and 22a. The Data Protection Commission shall inform the court about the result of the review. The result is then to be notified by the court also to the parties, insofar as the proceedings have not been decided finally.

Damages

§ 33. (1) A controller [Auftraggeber] or processor [Dienstleister] who has culpably used data contrary to the provisions of this Federal Act [Bundesgesetz], shall indemnify the data subject [Betroffener] pursuant to the general provisions of civil law. If data falling under the categories listed in § 18 para. 2 no. 1 to 3 are publicly used in a manner that violates a data subjects' interests in secrecy deserving protection that is suitable to expose that person in a like manner to § 7 para. 1 of the Media Act, Federal Law Gazette No. 314/1981, that provision shall be applied even if the public use of data [Datenverwendung] is not committed by publication in the media. The claim for appropriate compensation for the defamation suffered shall be brought against the controller of the data used.

(2) The controller or processor shall also be liable for damage caused by their staff, insofar as their actions was casual for the damage.

(3) The controller shall be free from liability if he can prove that the circumstances which caused the damage cannot be attributed to him or his staff (para. 2). This also applies to the exclusion of the processors' liability. In the case of contributory negligence on the part of the injured party or a person for whose conduct the injured party is responsible, § 1304 ABGB shall apply.

(4) Lawsuits according to para. 1 shall be brought before the court that is competent according to § 32 para. 4.

Common Provisions

§ 34. (1) The right to lodge an application according to § 30, a complaint according to § 31 or legal action according to § 32 and claims for damages according to § 33 shall apply only if the charge is filed by the intervening party within a year after having gained knowledge of the incident that gave rise to the complaint and no later than three years after the alleged incident. This is to be communicated to the intervening party in the case of a late application according to § 30; late complaints according to § 31 or legal actions according to § 32 shall be rejected.

(2) Applications according to § 30, complaints according to § 31 or legal action according to § 32 and claims for damages according to § 33 can be filed not only because of an alleged infringement of this Federal Act [Bundesgesetz], but also based on an infringement of data protection provisions of another member state of the

Union gegründet werden, soweit solche Vorschriften gemäß § 3 im Inland anzuwenden sind.

(3) Ist ein von der Datenschutzkommission zu prüfender Sachverhalt gemäß § 3 nach der Rechtsordnung eines anderen Vertragsstaates des Europäischen Wirtschaftsraumes zu beurteilen, so kann die Datenschutzkommission die zuständige ausländische Datenschutzkontrollstelle um Unterstützung ersuchen.

(4) Die Datenschutzkommission hat den Unabhängigen Datenschutzkontrollstellen der anderen Vertragsstaaten des Europäischen Wirtschaftsraumes über Ersuchen Amtshilfe zu leisten.

7. Abschnitt

Kontrollorgane

Datenschutzkommission und Datenschutzrat

§ 35. (1) Zur Wahrung des Datenschutzes sind nach den näheren Bestimmungen dieses Bundesgesetzes - unbeschadet der Zuständigkeit des Bundeskanzlers und der ordentlichen Gerichte - die Datenschutzkommission und der Datenschutzrat berufen.

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

Zusammensetzung der Datenschutzkommission

§ 36. (1) Die Datenschutzkommission besteht aus sechs Mitgliedern, die auf Vorschlag der Bundesregierung vom Bundespräsidenten für die Dauer von fünf Jahren bestellt werden. Wiederbestellungen sind zulässig. Die Mitglieder müssen rechtskundig sein. Ein Mitglied muß dem Richterstand angehören.

(2) Die Vorbereitung des Vorschlages der Bundesregierung für die Bestellung der Mitglieder der Datenschutzkommission obliegt dem Bundeskanzler. Er hat dabei Bedacht zu nehmen auf:

1. einen Dreiervorschlag des Präsidenten des Obersten Gerichtshofs für das richterliche Mitglied,
2. einen Vorschlag der Länder für zwei Mitglieder,
3. einen Dreiervorschlag der Bundeskammer für Arbeiter und Angestellte für ein Mitglied,
4. einen Dreiervorschlag der Wirtschaftskammer Österreich für ein Mitglied.

Alle vorgeschlagenen Personen sollen Erfahrung auf dem Gebiet des Datenschutzes besitzen.

European Union, insofar as these provisions are applicable in Austria according to § 3.

(3) If a case to be adjudicated by the Data Protection Commission by applying the national provisions of another member state of the European Economic Area pursuant to § 3, the Data Protection Commission [Datenschutzkommission] shall ask the competent foreign supervisory authority for assistance.

(4) The Data Protection Commission shall render inter-authority assistance [Amtshilfe] to the independent supervisory authorities of the signatory states of the European Economic Area upon request.

Part 7

Control Bodies

Data Protection Commission and Data Protection Council

§ 35. (1) The Data Protection Commission [Datenschutzkommission] and the Data Protection Council [Datenschutzrat] shall safeguard data protection in accordance with the regulations of this Federal Act [Bundesgesetz] without prejudice to the competence of the Federal Chancellor [Bundeskanzler] and the courts of law.

(2) The Data Protection Commission shall exercise its functions vis-á-vis the highest executive authorities enumerated in art. 19 B VG .

Composition of the Data Protection Commission

§ 36. (1) The Data Protection Commission [Daten¬schutz¬kommission] shall consist of six members appointed by the Federal President [Bundespräsident] on a proposal of the Federal Government [Bundesregierung] for a term of five years. Reappointments shall be permitted. All members shall have legal expertise. One member shall be a judge.

(2) The proposal of the Federal Government for the nomination of the members of the Data Protection Commission shall be prepared by the Federal Chancellor. The Federal Chancellor shall choose from

1. a proposal of three candidates by the President of the Supreme Court [Oberster Gerichtshof] for the judge,
2. a proposal of the states [Bundesländer] for two members,
3. a proposal of three candidates by the Federal Chamber of Labour [Bundeskammer für Arbeiter und Angestellte] for one member,
4. a proposal of three candidates by the Austrian Federal Economic Chamber [Wirtschafts¬kammer Österreich] for one member.

All proposed persons should have experience in the field of data protection.

(3) Ein Mitglied ist aus dem Kreise der rechtskundigen Bundesbediensteten vorzuschlagen.

(3a) Die Mitglieder der Datenschutzkommission üben diese Funktion neben ihnen sonst obliegenden beruflichen Tätigkeiten aus.

(4) Für jedes Mitglied ist ein Ersatzmitglied zu bestellen. Das Ersatzmitglied tritt bei Verhinderung des Mitglieds an dessen Stelle. Die Funktionsperiode des Ersatzmitglieds endet mit der Funktionsperiode des Mitglieds; für den Fall der vorzeitigen Beendigung der Funktionsperiode des Mitglieds gilt Abs. 8.

(5) Der Datenschutzkommission können nicht angehören:

1. Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre;
2. Personen, die zum Nationalrat nicht wählbar sind.

(6) Hat ein Mitglied der Datenschutzkommission Einladungen zu drei aufeinanderfolgenden Sitzungen ohne genügende Entschuldigung keine Folge geleistet oder tritt bei einem Mitglied ein Ausschließungsgrund des Abs. 5 nachträglich ein, so hat dies nach seiner Anhörung die Datenschutzkommission festzustellen. Diese Feststellung hat den Verlust der Mitgliedschaft zur Folge. Im übrigen kann ein Mitglied der Datenschutzkommission nur aus einem schwerwiegenden Grund durch Beschluß der Datenschutzkommission, dem mindestens drei ihrer Mitglieder zustimmen müssen, seines Amtes für verlustig erklärt werden. Die Mitgliedschaft endet auch, wenn das Mitglied seine Funktion durch schriftliche Erklärung an den Bundeskanzler zurücklegt.

(7) Auf die Ersatzmitglieder sind die Abs. 2, 3, 5 und 6 wie auf Mitglieder anzuwenden.

(8) Scheidet ein Mitglied wegen Todes, freiwillig oder gemäß Abs. 6 vorzeitig aus, so wird das betreffende Ersatzmitglied (Abs. 4) Mitglied der Datenschutzkommission bis zum Ablauf der Funktionsperiode des ausgeschiedenen Mitglieds. Unter Anwendung der Abs. 2 und 3 ist für diese Zeit ein neues Ersatzmitglied zu bestellen. Scheidet ein Ersatzmitglied vorzeitig aus, ist unverzüglich ein neues Ersatzmitglied zu bestellen.

(9) Die Mitglieder und Ersatzmitglieder der Datenschutzkommission haben für die Anreise zu den Sitzungen der Datenschutzkommission sowie für in Ausübung ihrer Funktion erforderliche sonstige Dienstreisen Anspruch auf Ersatz der Reisekosten (Gebührenstufe 3) durch den Bundeskanzler nach Maßgabe der für Bundesbedienstete geltenden Rechtsvorschriften. Sie haben ferner Anspruch auf eine der Zeit und dem Arbeitsaufwand entsprechende Vergütung, die auf Antrag des Bundeskanzlers von der Bundesregierung durch Verordnung festzusetzen ist.

Weisungsfreiheit der Datenschutzkommission

§ 37. (1) Die Mitglieder der Datenschutzkommission sind in Ausübung ihres

(3) One member shall be proposed from the circle of federal servant with legal expertise.

(3a) The members of the Data Protection Commission exercise this function in addition to their other professional duties.

(4) For every regular member an alternate member shall be appointed. The alternate member shall act in case the member is unable to fulfil his duties. The term of the alternate member shall expire with the end of the members term of office; if the term of the member ends prematurely para. 8 shall be applied.

(5) The following persons cannot be members of the Data Protection Commission:

1. members of the Federal Government [Bundesregierung] or of a State Government [Landes¬regierung] or Secretaries of State [Staatssekretäre];
2. persons who may not be elected for the National Council [Nationalrat].

(6) Where a member of the Data Protection Commission fails, without adequate excuse, to take part in three consecutive meetings or if one of the causes for exclusion specified in para. 5 arises after the appointment, the Data Protection Commission shall, after hearing the member concerned, decide on the matter. Such decision shall result in the loss of membership. In all other cases a member of the Data Protection Commission may only be deprived of his office on serious grounds and by a decision of the Data Protection Commission approved by at least three members. The term of office shall end when the member resigns from his function in a written statement to the Federal Chancellor.

(7) Para. 2, 3, 5 and 6 shall be applied to the alternate members the same way as to members.

(8) If membership ends because of death, voluntary resignation or in accordance with para. 6, the respective alternate member (para. 4) shall become a full member of the Data Protection Commission until the expiry of the term of the member he replaced. A new alternate member shall be appointed for that time according to para. 2 and 3. If an alternate member leaves prematurely, a new alternate member shall be appointed without delay.

(9) The members and alternate members of the Data Protection Commission shall be entitled to receive compensation for travel expenses (category 3) by the Federal Chancellor according to the regulations for federal employees for the travelling to the meetings of the Data Protection Commission and other duty travels in exerting their function. They shall furthermore be entitled to a compensation according to the amount of time and effort involved, the amount of which shall be determined in an ordinance of the Federal Government upon request of the Federal Chancellor.

Independence of the Data Protection Commission

§ 37. (1) The members of the Data Protection Commission

Amtes unabhängig und an keine Weisungen gebunden.

(2) Die in der Geschäftsstelle der Datenschutzkommission tätigen Bediensteten unterstehen fachlich nur den Weisungen des Vorsitzenden oder des geschäftsführenden Mitglieds der Datenschutzkommission.

Organisation und Geschäftsführung der Datenschutzkommission

§ 38. (1) (Verfassungsbestimmung) Die Datenschutzkommission hat sich eine Geschäftsordnung zu geben, in der eines ihrer Mitglieder mit der Führung der laufenden Geschäfte zu betrauen ist (geschäftsführendes Mitglied). Diese Betrauung umfaßt auch die Erlassung von verfahrensrechtlichen Bescheiden und von Mandatsbescheiden im Registrierungsverfahren gemäß § 20 Abs. 2 oder § 22 Abs. 3. Inwieweit einzelne fachlich geeignete Bedienstete der Geschäftsstelle der Datenschutzkommission zum Handeln für die Datenschutzkommission oder das geschäftsführende Mitglied ermächtigt werden, bestimmt die Geschäftsordnung.

(2) Für die Unterstützung in der Geschäftsführung der Datenschutzkommission hat der Bundeskanzler eine Geschäftsstelle einzurichten und die notwendige Sach- und Personalausstattung bereitzustellen. Er hat das Recht, sich jederzeit über alle Gegenstände der Geschäftsführung der Datenschutzkommission beim Vorsitzenden und dem geschäftsführenden Mitglied zu unterrichten.

(3) Die Datenschutzkommission ist vor Erlassung von Verordnungen anzuhören, die auf der Grundlage dieses Bundesgesetzes ergehen oder sonst wesentliche Fragen des Datenschutzes unmittelbar betreffen.

(4) Die Datenschutzkommission hat spätestens alle zwei Jahre einen Bericht über ihre Tätigkeit zu erstellen und in geeigneter Weise zu veröffentlichen. Der Bericht ist dem Bundeskanzler zur Kenntnis zu übermitteln.

Beschlüsse der Datenschutzkommission

§ 39. (1) Die Datenschutzkommission ist bei Anwesenheit aller sechs Mitglieder beschlußfähig. Für den Fall der Verhinderung eines Mitglieds gilt § 36 Abs. 4.

(2) Das richterliche Mitglied führt den Vorsitz.

(3) Für einen gültigen Beschluß der Datenschutzkommission ist die Zustimmung der Mehrheit der abgegebenen Stimmen notwendig. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig.

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

[Datenschutzkommission] shall be independent and not bound by instructions [Weisungen] in the exercise of their duties.

(2) The officials working in the office of the Data Protection Commission shall be bound only by instructions [Weisungen] of the chairman and the executive member [geschäftsführendes Mitglied] of the Data Protection Commission with regard to their professional work.

Organisation and Operation of the Data Protection Commission

§ 38. (1) (Constitutional Provision) The Data Protection Commission [Daten¬schutz¬kommission] shall adopt its own rules of procedure, in which one of its members shall be charged with directing the current business (executive member) [geschäftsführendes Mitglied]. This shall include rulings [Bescheide] on procedure and provisional rulings [Mandatsbescheide] in the course of the registration proceedings according to § 20 para. 2 and § 22 para. 3. Whether competent members of the office of the Data Protection Commission shall be authorised to act on behalf of the Data Protection Commission or the executive member [geschäftsführendes Mitglied], shall be laid down in the rules of procedure.

(2) The Federal Chancellor [Bundeskanzler] shall install an office and supply the necessary personnel and equipment to support the operation of the Data Protection Commission. He is entitled to request information anytime in all matters regarding the conduct of the management of the Data Protection Commission from the Chairman and the executive member.

(3) The Data Protection Commission shall be heard before an ordinance based on this Federal Act [Bundesgesetz] is enacted or which otherwise directly concerns important issues of data protection.

(4) The Data Protection Commission shall compile a report about its activities at least every other year and publish it in an appropriate manner. The report shall be forwarded to the Federal Chancellor.

Decisions of the Data Protection Commission

§ 39. (1) The Data Protection Commission [Daten¬schutz¬kommission] shall be able to make decisions when all six members are present. § 36 para. 4 shall apply when a member is unable to fulfil his duties.

(2) The judge shall preside.

(3) A valid decision of the Data Protection Commission shall require a majority of votes cast. In the case of a parity of votes the vote of the chairman shall decide the issue. An abstention from the vote is not permitted.

(4) Decisions of the Data Protection Commission that are of fundamental importance for the general public shall be published in an appropriate manner by the Data Protection Commission taking into account the requirements of official secrecy.

(5) Beschlüsse der Datenschutzkommission werden vom Vorsitzenden ausgefertigt.

Wirkung von Bescheiden der Datenschutzkommission und des geschäftsführenden Mitglieds

§ 40. (1) Gegen Bescheide, die das geschäftsführende Mitglied der Datenschutzkommission gemäß § 22 Abs. 3, § 30 Abs. 6a oder § 31a Abs. 3 in Verbindung mit § 38 Abs. 1 erlassen hat, ist die Vorstellung an die Datenschutzkommission gemäß § 57 Abs. 2 AVG zulässig. Eine Vorstellung gegen einen gemäß § 22 Abs. 3 ergangenen Bescheid hat aufschiebende Wirkung.

(2) Gegen Bescheide der Datenschutzkommission ist kein Rechtsmittel zulässig. Sie unterliegen nicht der Aufhebung oder Abänderung im Verwaltungsweg. Auftraggeber des öffentlichen Bereichs haben in Verfahren vor der Datenschutzkommission stets Parteistellung. Die Anrufung des Verwaltungsgerichtshofes durch die Parteien des Verfahrens ist zulässig. Dies gilt jedoch nicht für Auftraggeber des öffentlichen Bereichs als Beschwerdegegner im Verfahren nach § 31, es sei denn es ist durch besondere gesetzliche Regelung die Möglichkeit einer Amtsbeschwerde (Art. 131 Abs. 2 B VG) vorgesehen.

(3) Bescheide, mit welchen gemäß § 13 Übermittlungen oder Überlassungen von Daten ins Ausland genehmigt wurden, sind zu widerrufen, wenn die rechtlichen und tatsächlichen Voraussetzungen für die Erteilung der Genehmigung, insbesondere auch infolge einer gemäß § 55 ergangenen Kundmachung des Bundeskanzlers, nicht mehr bestehen.

(4) Wenn die Datenschutzkommission eine Verletzung von Bestimmungen dieses Bundesgesetzes durch einen Auftraggeber des öffentlichen Bereichs festgestellt hat, so hat dieser mit den ihm zu Gebote stehenden rechtlichen Mitteln unverzüglich den der Rechtsanschauung der Datenschutzkommission entsprechenden Zustand herzustellen.

Einrichtung und Aufgaben des Datenschutzrates

§ 41. (1) Beim Bundeskanzleramt ist ein Datenschutzrat eingerichtet.

(2) Der Datenschutzrat berät die Bundesregierung und die Landesregierungen auf deren Ersuchen in rechtspolitischen Fragen des Datenschutzes. Zur Erfüllung dieser Aufgabe

1. kann der Datenschutzrat Fragen von grundsätzlicher Bedeutung für den Datenschutz in Beratung ziehen;
2. ist dem Datenschutzrat Gelegenheit zur Stellungnahme zu Gesetzesentwürfen der Bundesministerien zu geben, soweit diese datenschutzrechtlich von Bedeutung sind;
3. haben Auftraggeber des öffentlichen Bereichs ihre Vorhaben dem

(5) Decisions of the Data Protection Commission are signed by the chairman.

Effect of Rulings of the Data Protection Commission and the Executive Member

§ 40. (1) Rulings [Bescheide] of the executive member [geschäftsführendes Mitglied] of the Data Protection Commission [Datenschutzkommission] pursuant to § 22 para. 3, § 30 para 6a or § 31 para. 3 in conjunction with § 38 para. 1 are subject to appeal [Vorstellung] pursuant to § 57 para. 2 AVG. An appeal against a ruling [Bescheid] pursuant to § 22 para. 3. shall have suspensive effect.

(2) No regular remedy at law shall be permitted against rulings [Bescheide] of the Data Protection Commission. They are not subject to repeal or modification by administrative procedure. Controllers in the public sector always have a position as party in proceedings before the Data Protection Commission. The parties shall have the right to bring the case before the Administrative Court [Verwaltungsgerichtshof]. This however, does not apply to public sector controllers as opponents to complaints in proceedings according to § 31, except if the possibility of a complaint ex officio (Art. 131 para 2 B Federal Constitutional Act) is provided by express legal regulation .

(3) Rulings permitting the transborder transmission [Über¬mittlung] or committing of data [Überlassung] pursuant to § 13 shall be cancelled whenever the legal or factual prerequisites for granting a permit no longer apply, in particular as the result of a promulgation [Kundmachung] of the Federal Chancellor pursuant to § 55.

(4) If the Data Protection Commission has established that an infringement of provisions of this Federal Act [Bundesgesetz] by a public sector controller has taken place, said controller shall without delay and with all means at his disposal create the state expressed in the legal opinion of the Data Protection Commission.

Establishment and Duties of the Data Protection Council

§ 41. (1) A Data Protection Council [Datenschutzrat] is established at the Federal Chancellery [Bundes¬kanzler¬amt].

(2) The Data Protection Council shall advise the Federal Government [Bundesregierung] and the State Governments [Landesregierungen] on requests in political matters of data protection. For this purpose,

1. the Data Protection Council can deliberate on questions of fundamental importance for data protection;
2. the Data Protection Council shall be given opportunity to give its opinion on draft bills of Federal Ministries [Bundesministerien], insofar as these are significant for data protection;
3. public sector controllers shall present their projects to the Data Protection

Datenschutzrat zur Stellungnahme zuzuleiten, soweit diese datenschutzrechtlich von Bedeutung sind;

4. hat der Datenschutzrat das Recht, von Auftraggebern des öffentlichen Bereichs Auskünfte und Berichte sowie die Einsicht in Unterlagen zu verlangen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist;

4a. hat der Datenschutzrat das Recht, von der Datenschutzkommission Auskünfte und Berichte sowie Einsicht in Unterlagen zu verlangen;

5. kann der Datenschutzrat Auftraggeber des privaten Bereichs oder auch ihre gesetzliche Interessenvertretung zur Stellungnahme zu Entwicklungen von allgemeiner Bedeutung auffordern, die aus datenschutzrechtlicher Sicht Anlaß zu Bedenken, zumindest aber Anlaß zur Beobachtung geben;

6. kann der Datenschutzrat seine Beobachtungen, Bedenken und allfälligen Anregungen zur Verbesserung des Datenschutzes in Österreich der Bundesregierung und den Landesregierungen mitteilen, sowie über Vermittlung dieser Organe den gesetzgebenden Körperschaften zur Kenntnis bringen.

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

Zusammensetzung des Datenschutzrates

§ 42. (1) Dem Datenschutzrat gehören an:

1. Vertreter der politischen Parteien: Von der im Hauptausschuss des Nationalrates am stärksten vertretenen Partei sind vier Vertreter, von der am zweitstärksten vertretenen Partei sind drei Vertreter und von jeder anderen im Hauptausschuss des Nationalrates vertretenen Partei ist ein Vertreter in den Datenschutzrat zu entsenden, wobei es allein auf die Stärke im Zeitpunkt der Entsendung ankommt. Bei Mandatsgleichheit zweier Parteien im Hauptausschuss ist die Stimmenstärke bei der letzten Wahl zum Nationalrat ausschlaggebend;
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 Bundeskanzler zu ernennender Vertreter des Bundes.

Council for evaluation, insofar as these are significant for data protection;

4. the Data Protection Council shall have the right to request information and documents from public sector controllers insofar as this is necessary to evaluate projects of significant impact on data protection in Austria;

4a. the Data Protection Council shall have the right to request information and reports as well as inspection of documents from the Data Protection Commission.

5. the Data Protection Council may ask private sector controllers or their representations of interest established by law to give their opinion on developments of general importance that give cause for concern or at least call for attention from a data protection perspective;

6. the Data Protection Council may transmit its observations, concerns and suggestions for improvements of data protection in Austria to the Federal Government and the State Governments, as well as to the legislative bodies by way of these organs.

(3) Para. 2 sub-paras. 3 and 4 shall not apply insofar as the internal affairs of the churches and religious communities recognised by law are concerned.

Composition of the Data Protection Council

§ 42. (1) The Data Protection Council [Datenschutzrat] shall have the following members:

1. representatives of the political parties: The party that is most strongly represented in the Main Committee of the National Council [Hauptausschuß des Nationalrates] shall delegate four representatives, the second strongest shall delegate three members and all other parties represented in the Main Committee of the National Council shall delegate one member each, to be determined by the strength of representation at the time of delegation. In case of equal number of deputies of two parties in the Main Committee the number of votes cast in the most recent election to the Federal Parliament is decisive;
2. one representative each from Federal Chamber of Labour [Bundeskammer für Arbeiter und Angestellte] and the Austrian Federal Economic Chamber [Wirtschaftskammer Österreich];
3. two representatives of the States [Länder];
4. one representative each of the Association of Austrian Municipalities [Gemeindebund] and the Austrian Association of Towns [Städtebund];
5. a member of the Federation [Bund] appointed by the Federal Chancellor [Bundeskanzler].

(2) Die in Abs. 1 Z 3, 4 und 5 genannten Vertreter sollen berufliche Erfahrung auf dem Gebiet der Informatik und des Datenschutzes haben.

(3) Für jedes Mitglied ist ein Ersatzmitglied namhaft zu machen.

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

(5) Die Mitglieder gehören dem Datenschutzrat solange an, bis sie dem Bundeskanzler schriftlich ihr Ausscheiden mitteilen oder, mangels einer solchen Mitteilung, von der entsendenden Stelle (Abs. 1) dem Bundeskanzler ein anderer Vertreter namhaft gemacht wird. Mitglieder nach Abs. 1 Z 1 scheiden außerdem aus, sobald der Hauptausschuss nach den §§ 29 und 30 des Geschäftsordnungsgesetzes 1975, BGBl. Nr. 410, neu gewählt wurde, und sie nicht neuerlich entsendet werden.

(6) Die Tätigkeit der Mitglieder des Datenschutzrates ist ehrenamtlich. Mitglieder des Datenschutzrates, die außerhalb von Wien wohnen, haben im Fall der Teilnahme an Sitzungen des Datenschutzrates Anspruch auf Ersatz der Reisekosten (Gebührenstufe 3) nach Maßgabe der für Bundesbeamte geltenden Rechtsvorschriften.

Vorsitz und Geschäftsführung des Datenschutzrates

§ 43. (1) Der Datenschutzrat gibt sich mit Beschluß eine Geschäftsordnung.

(2) Der Datenschutzrat hat aus seiner Mitte einen Vorsitzenden und zwei stellvertretende Vorsitzende zu wählen. Die Funktionsperiode des Vorsitzenden und der stellvertretenden Vorsitzenden dauert - unbeschadet des § 42 Abs. 5 - fünf Jahre. Wiederbestellungen sind zulässig.

(3) Die Geschäftsführung des Datenschutzrates obliegt dem Bundeskanzleramt. Der Bundeskanzler hat das hiefür notwendige Personal zur Verfügung zu stellen. Bei ihrer Tätigkeit für den Datenschutzrat sind die Bediensteten des Bundeskanzleramtes fachlich an die Weisungen des Vorsitzenden des Datenschutzrates gebunden.

Sitzungen und Beschlußfassung des Datenschutzrates

§ 44. (1) Die Sitzungen des Datenschutzrates werden vom Vorsitzenden nach Bedarf einberufen. Begehrt ein Mitglied die Einberufung einer Sitzung, so hat der Vorsitzende die Sitzung so einzuberufen, daß sie binnen vier Wochen stattfinden kann.

(2) Zu den Sitzungen kann der Vorsitzende nach Bedarf Sachverständige zuziehen.

(3) Für Beratungen und Beschlußfassungen im Datenschutzrat ist die Anwesenheit

(2) The representatives mentioned in para. 1 sub-para. 3, 4 and 5 should have professional experience in the field of computer science and data protection.

(3) An alternate representative shall be nominated for every representative.

(4) Members of the Federal Government [Bundesregierung] or of a State Government [Landesregierung] or Secretaries of State [Staatssekretäre] as well as persons who may not be elected for the National Council [Nationalrat] shall not be members of the Data Protection Council [Datenschutzrat].

(5) The representatives shall be members of the Data Protection Council until they announce their resignation in writing to the Federal Chancellor [Bundeskanzler], or, if no resignation is announced, until the nominating body (para. 1) has named another representative to the Federal Chancellor. Members according to para 1 sub-para 1 retire also, as soon as the Main Committee has been newly elected according to § 29 and 30 of the Parlamentary Rules of Procedure 1975, Federal Law Gazette No. 410, and they have not been delegated again.

(6) The members of the Data Protection Council shall serve in an honorary capacity. Members of the Data Protection Council living outside of Vienna shall be entitled to receive compensation for travel expenses (category 3) according to the regulations for federal officials, if they attend meetings of the Data Protection Council.

Chairmanship and Operation of the Data Protection Council

§ 43. (1) The Data Protection Council shall decide on its rules of procedure.

(2) The Data Protection Council [Datenschutzrat] shall elect a chairman and two vice chairmen. The term of office of the chairman and the vice chairmen shall be five years, without prejudice to § 42 para. 5. Reappointments shall be permitted.

(3) The Federal Chancellery [Bundeskanzleramt] shall be responsible for the operation of the Data Protection Council. The Federal Chancellor [Bundeskanzler] shall supply the necessary personnel. While working for the Data Protection Council, the officials of the Federal Chancellery shall be bound only by instructions [Weisungen] of the chairman of the Data Protection Council with regard to their professional work.

Meetings and Decisions of the Data Protection Council

§ 44. (1) The meeting of the Data Protection Council [Datenschutzrat] shall be convened by the chairman whenever the need arises. If a member requests that a meeting be convened, the chairman shall convene the meeting so that it can take place within four weeks.

(2) The chairman can bring experts into the meeting whenever the need arises.

(3) Deliberations and decisions of the Data Protection Council shall require the

von mehr als der Hälfte seiner Mitglieder erforderlich. Zur Beschlußfassung genügt die einfache Mehrheit der abgegebenen Stimmen. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig. Die Beifügung von Minderheitenvoten ist zulässig.

(4) Der Datenschutzrat kann aus seiner Mitte ständige oder nichtständige Arbeitsausschüsse bilden, denen er die Vorbereitung, Begutachtung und Bearbeitung einzelner Angelegenheiten übertragen kann. Er ist auch berechtigt, die Geschäftsführung, Vorbegutachtung und die Bearbeitung einzelner Angelegenheiten einem einzelnen Mitglied (Berichterstatter) zu übertragen.

(5) Jedes Mitglied des Datenschutzrates ist verpflichtet, an den Sitzungen - außer im Fall der gerechtfertigten Verhinderung - teilzunehmen. Ist ein Mitglied an der Teilnahme verhindert, hat es hievon unverzüglich das Ersatzmitglied zu verständigen.

(6) Mitglieder der Datenschutzkommission, die dem Datenschutzrat nicht angehören, sind berechtigt, an den Sitzungen des Datenschutzrates oder seiner Arbeitsausschüsse teilzunehmen. Ein Stimmrecht steht ihnen nicht zu.

(7) Die Beratungen in der Sitzung des Datenschutzrates sind, soweit er nicht selbst anderes beschließt, vertraulich.

(8) Die Mitglieder des Datenschutzrates, die anwesenden Mitglieder der Datenschutzkommission und die zur Sitzung gemäß Abs. 2 zugezogenen Sachverständigen sind zur Verschwiegenheit über alle ihnen ausschließlich aus ihrer Tätigkeit im Datenschutzrat bekanntgewordenen Tatsachen verpflichtet, sofern die Geheimhaltung im öffentlichen Interesse oder im Interesse einer Partei geboten ist.

8. Abschnitt

Besondere Verwendungszwecke von Daten

Private Zwecke

§ 45. (1) Für ausschließlich persönliche oder familiäre Tätigkeiten dürfen natürliche Personen Daten verarbeiten, wenn sie ihnen vom Betroffenen selbst mitgeteilt wurden oder ihnen sonst rechtmäßigerweise, insbesondere in Übereinstimmung mit § 7 Abs. 2, zugekommen sind.

(2) Daten, die eine natürliche Person für ausschließlich persönliche oder familiäre Tätigkeiten verarbeitet, dürfen, soweit gesetzlich nicht ausdrücklich anderes vorgesehen ist, für andere Zwecke nur mit Zustimmung des Betroffenen übermittelt werden.

Wissenschaftliche Forschung und Statistik

§ 46. (1) Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Auftraggeber der Untersuchung alle Daten verwenden, die

presence of at least half of its members. Decisions shall be passed by a simple majority of votes cast. In the case of a parity of votes, the vote of the chairman shall decide the issue. An abstention from the vote is not permitted. A dissenting opinion may be given.

(4) The Data Protection Council may create permanent or ad hoc working groups which it may entrust with the preparation, appraisal and handling of specific issues. An individual member (rapporteur) may be entrusted with executive work, the first appraisal and handling of specific issues.

(5) Every member of the Data Protection Council must except in case of justifiably being prevented attend the meetings of the Council. A member who is unable to attend shall inform his alternate member without delay.

(6) Members of the Data Protection Commission [Datenschutzkommission] who are not members of the Data Protection Council shall have the right to attend meetings of the Council or its working groups. They shall have no right to vote.

(7) The deliberations of the Data Protection Council shall be confidential as long as the Council itself does not decide otherwise.

(8) The members of the Data Protection Council, the members of the Data Protection Commission and experts brought into the meeting according to para. 2 shall be obliged to keep all information confidential of which they have learned solely due to their activities for the Data Protection Council, insofar as secrecy is required in the public interest or in the interest of a party.

Part 8

Special Purposes of Data Use

Private Purposes

§ 45.(1) Natural persons shall be permitted to process data for purely personal or family matters that have been disclosed to them by the data subject [Betroffener] himself or that they have received in a lawful manner, in particular in accordance with § 7 para. 2.

(2) Data that are processed by a natural person for purely personal or family matters shall be transmitted for another purpose only with the consent of the data subject, unless expressly provided for otherwise by law.

Scientific Research and Statistics

§ 46. (1) For the purpose of scientific or statistical research projects whose goal is not to obtain results in a form relating to specific data subjects [Betroffene], the controller [Auftraggeber] shall have the right to use all data that

1. öffentlich zugänglich sind oder
2. er für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für ihn nur indirekt personenbezogen sind.

Andere Daten dürfen nur unter den Voraussetzungen des Abs. 2 Z 1 bis 3 verwendet werden.

(2) Bei Datenanwendungen für Zwecke wissenschaftlicher Forschung und Statistik, die nicht unter Abs. 1 fallen, dürfen Daten nur

1. gemäß besonderen gesetzlichen Vorschriften oder
2. mit Zustimmung des Betroffenen oder
3. mit Genehmigung der Datenschutzkommission gemäß Abs. 3 verwendet werden.

(3) Eine Genehmigung der Datenschutzkommission für die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik ist auf Antrag des Auftraggebers der Untersuchung zu erteilen, wenn

1. die Einholung der Zustimmung der Betroffenen mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet und
2. ein öffentliches Interesse an der beantragten Verwendung besteht und
3. die fachliche Eignung des Antragstellers glaubhaft gemacht wird.

Sollen sensible Daten ermittelt werden, muß ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muß gewährleistet sein, daß die Daten beim Auftraggeber der Untersuchung nur von Personen verwendet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verläßlichkeit sonst glaubhaft ist. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten, notwendig ist.

(3a) Einem Antrag nach Abs. 3 ist jedenfalls eine vom Verfügungsbefugten über die Datenbestände, aus denen die Daten ermittelt werden sollen, oder einem sonst darüber Verfügungsbefugten unterfertigte Erklärung anzuschließen, dass er dem Auftraggeber 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.

(4) Rechtliche Beschränkungen der Zulässigkeit der Benützung von Daten aus anderen, insbesondere urheberrechtlichen Gründen bleiben unberührt.

(5) Auch in jenen Fällen, in welchen gemäß den vorstehenden Bestimmungen die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der direkte Personsbezug unverzüglich zu

1. are publicly accessible or
2. he has lawfully collected for other research projects or other purposes or
3. are only indirectly personal for him/her.

Other data shall only be used under the conditions specified in para. 2 sub-paras. 1 to 3.

(2) In case of the use of data [Datenverwendung] for purposes of scientific research or statistics that do not fall under para. 1 shall be used only

1. pursuant to specific legal provisions or
2. with the consent of the data subject [Betroffener] or
3. with a permit of the Data Protection Commission [Datenschutzkommission] pursuant to para. 3.

(3) A permit of the Data Protection Commission for the use of data for purposes of scientific research or statistics shall be granted upon request of the controller ordering the research project, if

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

If sensitive data are to be collected an important public interest in the research must exist; furthermore, it must be ensured that the data at the controller ordering the research project the data shall only be used by persons who are subject to a statutory duty to confidentiality or whose reliability in this respect is otherwise credible. The Data Protection Commission may issue its permit subject to terms and conditions insofar as this is necessary to safeguard the data subjects' interests deserving protection, in particular, with regard to the use of sensitive data.

(3a) An application according to para 3 must, however, be accompanied by a statement signed by the person authorized to dispose of the collection of information from which the data shall be collected or by another authorized person that he/she makes available the collection of information for the research. Such statement may be replaced by a writ of execution (§ 367 para 1 Foreclosure Act, RGBl No. 79/1896) replacing such statement.

(4) Legal restrictions on the right to make use of data [Datenverwendung] for other reasons, in particular copyright, shall not be affected.

(5) Even in those cases where the use of data in a form which permits identification of data subjects is legal for purposes of scientific research or statistics, the data shall be coded without delay so that the data subjects are no longer identifiable

verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit nur indirekt personenbezogenen Daten das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, ist der Personsbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen

§ 47. (1) Soweit gesetzlich nicht ausdrücklich anderes bestimmt ist, bedarf die Übermittlung von Adreßdaten eines bestimmten Kreises von Betroffenen zum Zweck ihrer Benachrichtigung oder Befragung der Zustimmung der Betroffenen.

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

1. Daten desselben Auftraggebers verwendet werden oder
2. bei einer beabsichtigten Übermittlung der Adreßdaten an Dritte
   a) an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht oder
   b) der Betroffene nach entsprechender Information über Anlaß und Inhalt der Übermittlung innerhalb angemessener Frist keinen Widerspruch gegen die Übermittlung erhoben hat.

(3) Liegen die Voraussetzungen des Abs. 2 nicht vor und würde die Einholung der Zustimmung der Betroffenen gemäß Abs. 1 einen unverhältnismäßigen Aufwand erfordern, ist die Übermittlung der Adreßdaten mit Genehmigung der Datenschutzkommission gemäß Abs. 4 zulässig, falls die Übermittlung an Dritte

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

erfolgen soll.

(4) Die Datenschutzkommission hat auf Antrag eines Auftraggebers, 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 der Übermittlung nicht entgegenstehen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies

if specific phases of scientific or statistic work can be performed with indirectly personal data only. Unless expressly laid down otherwise, data in a form which permits identification of data subjects shall be rendered unidentifiable as soon as it is no longer necessary for scientific or statistic work to keep them identifiable.

Transmission of Addresses to Inform or Interview Data Subjects

§ 47. (1) Unless provided for otherwise by law, the transmission [Übermittlung] of address data of a certain group of data subjects [Betroffene] in order to inform or interview them shall require the consent of the data subjects.

(2) If an infringement of the data subject's interests in secrecy is unlikely, considering the selection criteria for the category of data subjects [Betroffenenkreis] and the subject of the information or interviews, no consent shall be required if

1. data from the same controller are used or
2. in case of an intended transmission of address data to third parties
   a. there is an additional public interest in the information or interviewing or
   b. the data subject, having received an adequate information about the cause for and content of the transmission, has not objected to the transmission within a reasonable period of time.

(3) If the prerequisites of para. 2 are not met and if obtaining the consent of the data subjects' pursuant to para. 1 would require an unreasonable effort, the transmission of the address data shall be permissible with a permit of the Data Protection Commission [Datenschutzkommission] pursuant to para. 4, in case the transmission to third parties shall be performed for

1. the purpose of information or an interview due to an important interest of the data subject himself
2. an important public interest in the information or interviews or
3. an interview of the data subjects for reasons of scientific research and statistics.

(4) Upon request of a controller processing address data the Data Protection Commission shall grant the permit for the transmission if the controller has satisfactorily demonstrated that one of the requirements in para. 3 applies and no overriding interests in secrecy deserving protection on the part of the data subject are an obstacle to the transmission. The Data Protection Commission may issue the permit subject to terms and conditions, insofar s this is necessary to safeguard the data

zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten als Auswahlkriterium, notwendig ist.

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

(6) In jenen Fällen, in welchen 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.

Publizistische Tätigkeit

§ 48. (1) Soweit Medienunternehmen, Mediendienste oder ihre Mitarbeiter Daten unmittelbar für ihre publizistische Tätigkeit im Sinne des Mediengesetzes verwenden, sind von den einfachgesetzlichen Bestimmungen des vorliegenden Bundesgesetzes nur die §§ 4 bis 6, 10, 11, 14 und 15 anzuwenden.

(2) Die Verwendung von Daten für Tätigkeiten nach Abs. 1 ist insoweit zulässig, als dies zur Erfüllung der Informationsaufgabe der Medienunternehmer, Mediendienste und ihrer Mitarbeiter in Ausübung des Grundrechtes auf freie Meinungsäußerung gemäß Art. 10 Abs. 1 EMRK erforderlich ist.

(3) Im übrigen gelten die Bestimmungen des Mediengesetzes, insbesondere seines dritten Abschnitts über den Persönlichkeitsschutz.

Verwendung von Daten im Katastrophenfall

§ 48a. (1) Auftraggeber des öffentlichen Bereiches sind im Katastrophenfall ermächtigt, Daten zu verwenden, 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. Zu diesem Zweck sind auch Hilfsorganisationen (Abs. 6) nach Maßgabe der ihnen zukommenden Aufgaben und rechtlichen Befugnis ermächtigt, Daten zu verwenden. Wenn dies zur raschen Bewältigung der Katastrophe notwendig ist, darf eine Datenverwendung in Form der Teilnahme an einem Informationsverbundsystem erfolgen. Wer rechtmäßig über Daten verfügt, darf diese an Auftraggeber des öffentlichen Bereiches und Hilfsorganisationen übermitteln, sofern diese die Daten zur Bewältigung der Katastrophe für die genannten Zwecke benötigen. Die Daten sind unverzüglich zu löschen, wenn sie für die Erfüllung des konkreten Zwecks nicht mehr benötigt werden.

(2) Eine Überlassung oder Übermittlung von Daten in das Ausland ist zulässig, soweit dies für die Erfüllung der in Abs. 1 genannten Zwecke notwendig ist. Wenn dies zur raschen Bewältigung der Katastrophe notwendig ist, darf eine Datenverwendung durch Auftraggeber des öffentlichen Bereichs und Hilfsorganisationen in Form der Teilnahme an einem Informationsverbundsystem, an dem auch ausländische

subjects' interests deserving protection, in particular, with regard to the use of sensitive data as selection criterion.

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

(6) In those cases where it is lawful to transmit the names and addresses of persons belonging to a certain category of data subjects pursuant to the aforementioned provisions, the processing required for selecting the address data to be transmitted shall also be permitted.

Journalistic Purposes

§ 48. (1) Insofar as media companies, media services and their operatives use data directly for journalistic purposes according to the Media Act [Mediengesetz], only sects. 4 to 6, 10, 11, 14 and 15 of the non-constitutional provisions of this Federal Act [Bundesgesetz] shall apply.

(2) The use of data [Datenverwendung] for activities pursuant to para. 1 shall be legal insofar as this is required to fulfil the information requirements of the media companies, media services and their operatives in exercise of the right to free speech pursuant to art. 10 para. 1 of the European Convention on Human Rights.

(3) In all other respects the Media Act [Mediengesetz] shall apply, especially the third part about the protection of personality rights.

Use of data in case of a catastrophe

§ 48a. (1) Controllers of the public sector shall be authorised to use data in case of a catastrophe to assist persons affected directly by the catastrophe, to locate and identify missing or deceased persons and to provide information to the relatives. Relief organisations (para. 6) shall be authorised to use data for this purpose in accordance with their duties and legitimate authority. If this is necessary to cope with the catastrophe swiftly, the use of data may be carried out by participating in a joint information system. Anybody who lawfully possesses data shall be permitted to transmit these data to controllers of the public sector and relief organisations, if these organisations need this data to manage the catastrophe for the purposes specified. The data are to be deleted immediately if they are not any longer required for the fulfilment of the specific purpose.

(2) The data shall be committed or transmitted to recipients in third countries insofar as this is necessary to fulfil the purposes mentioned in para. 1. If this is necessary to rapidly cope with the catastrophe, data may be used by public sector controllers and relief organisations in the form of a joint information system with the participation of foreign controllers. A transfer of police records and sensitive data for

Auftraggeber beteiligt sind, erfolgen. Die Übermittlung erkennungsdienstlicher und sensibler Daten zu Identifizierungszwecken an ein derartiges System darf erst stattfinden, wenn auf Grund von Erhebungen konkrete Anhaltspunkte dafür vorliegen, dass die vermisste Person verstorben sein dürfte. Daten, die für sich allein den Betroffenen strafrechtlich belasten, dürfen nicht übermittelt werden, es sei denn, dass diese zur Identifizierung im Einzelfall unbedingt notwendig sind. Die Übermittlung von Daten Angehöriger darf nur in pseudonymisierter Form erfolgen. Daten dürfen in Staaten ohne angemessenes Datenschutzniveau nur übermittelt oder überlassen werden, wenn der Auftraggeber auf Grund schriftlicher Vereinbarungen mit dem Empfänger oder auf Grund schriftlicher Zusagen des Empfängers oder, wenn dies nach den Umständen nicht oder nicht in angemessener Zeit möglich ist, durch Erteilung von Auflagen an den Empfänger davon ausgehen kann, dass die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Eine Übermittlung oder Überlassung hat dann zu unterbleiben, wenn Grund zur Annahme besteht, dass der Empfänger nicht für den gebotenen Schutz der Geheimhaltungsinteressen der Betroffenen Sorge tragen oder ausdrückliche datenschutzrechtliche Auflagen des Auftraggebers missachten werde. Während der Dauer der Katastrophensituation entfällt im Hinblick auf § 12 Abs. 3 Z 3 die Genehmigungspflicht. Die Datenschutzkommission ist von den veranlassten Übermittlungen und Überlassungen und den näheren Umständen des Anlass gebenden Sachverhaltes jedoch unverzüglich zu verständigen. Die Datenschutzkommission kann zum Schutz der Betroffenenrechte Datenübermittlungen oder -überlassungen untersagen, wenn der durch die Datenweitergabe bewirkte Eingriff in das Grundrecht auf Datenschutz durch die besonderen Umstände der Katastrophensituation nicht gerechtfertigt ist.

the purpose of identification to a system of this kind shall only take place if investigations have yielded tangible evidence that the missing person is presumably deceased. Data that by itself would implicate the data subject in a crime shall not be transferred unless it is absolutely necessary for identification in a particular case. The data of relatives shall only be transferred in pseudonymous form. Data shall be transmitted or committed to states lacking an adequate general level of data protection only if the controller can assume, based on a written agreement with the recipient or, if such cannot be obtained under the circumstances in due time, by specifying conditions for the recipient, that the interests in secrecy deserving protection of the data subjects of the intended transfer shall be sufficiently respected in the recipient country. A transmission or committing shall not take place if there is cause for concern that the recipient will not devote attention to the interests in secrecy deserving protection of the data subjects or that he will ignore data protection conditions imposed by the controller. While the catastrophic event continues, the requirement to obtain a permit shall not apply pursuant to § 12 para. 3 sub-para. 3. The data protection commission shall be informed immediately about the data transfers and committings performed and about the circumstances of the motivating incident. The data protection commission is authorized to prohibit data transfers and committings if the intervention into the civil right to data protection is not justified by special circumstances caused by the catastrophe.

(3) Auf Grund einer konkreten Anfrage eines nahen Angehörigen einer tatsächlich oder vermutlich von der Katastrophe unmittelbar betroffenen Person sind Auftraggeber ermächtigt, dem Anfragenden Daten über die Reise in das und aus dem Katastrophengebiet, Aufenthaltsdaten im Katastrophengebiet sowie Daten über den Stand der Ausforschung von betroffenen Personen zu übermitteln, wenn der Angehörige folgende Daten bekannt gibt:

1. Vor- und Zuname, Geburtsdatum sowie Wohnadresse der tatsächlich oder vermutlich von der Katastrophe betroffenen Person und
2. seinen Vor- und Zunamen, sein Geburtsdatum, seine Wohnadresse und sonstige Erreichbarkeit sowie seine Angehörigeneigenschaft zur betroffenen Person.

Bestehen Zweifel an der Angehörigeneigenschaft und können diese durch Überprüfungen nicht ausgeräumt werden, ist ein Nachweis der Identität und Angehörigeneigenschaft notwendig.

(3) Based on a specific inquiry of a close relative of a person who is actually or presumably affected by a catastrophe, controllers of the public sector shall be authorised to transmit data to the inquiring person regarding the journey to an from the disaster area, data on the data subjects whereabouts in the disaster area as well as data on the search for the involved persons, if the relative can name the following data:

1. First name and surname, date of birth as well as the place of residence of a person who is actually or presumably affected by the catastrophe person and
2. then relatives own first name and surname, his date of birth, place of residence, contact details as well as his relation to the person involved.

If doubts remain about the relation to the person involved which cannot be eliminated by examination, a proof of identity and relation shall be required.

(4) Über Abs. 3 hinaus dürfen nahen Angehörigen von Auftraggebern des öffentlichen Bereiches und Hilfsorganisationen Daten einschließlich sensibler Daten

(4) Data, including sensitive data, on persons actually or presumably affected by the catastrophe may be transmitted beyond the scope of para. 3 to close relatives by

über tatsächlich oder vermutlich unmittelbar von der Katastrophe betroffene Personen nur übermittelt werden, wenn sie ihre Identität und ihre Angehörigeneigenschaft nachweisen und die Auskunft zur Wahrung ihrer Rechte oder jener der betroffenen Person erforderlich ist. Die Sozialversicherungsträger sind verpflichtet, die Auftraggeber des öffentlichen Bereiches und Hilfsorganisationen bei der Überprüfung der Daten gemäß Abs. 3 und der Angehörigenbeziehung zu unterstützen. Behörden sind ermächtigt, die zur Überprüfung dieser Angaben notwendigen Daten im Wege der Amtshilfe zu ermitteln und für diesen Zweck zu verwenden.

(5) Als nahe Angehörige im Sinne dieser Bestimmung sind Eltern, Kinder, Ehegatten, eingetragene Partner und Lebensgefährten der Betroffenen 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) Eine Hilfsorganisation im Sinne dieser Bestimmung ist eine allgemein anerkannte gemeinnützige Organisation, die statuten- oder satzungsgemäß das Ziel hat, Menschen in Notsituationen zu unterstützen und von der angenommen werden kann, dass sie in wesentlichem Ausmaß eine Hilfeleistung im Katastrophenfall erbringen kann.

(7) Alle Datenverwendungen sind im Sinne des § 14 Abs. 2 Z 7 zu protokollieren.

(8) Die Zulässigkeit von Datenverwendungen auf der Grundlage anderer in den §§ 8 und 9 genannter Tatbestände bleibt unberührt.

9. Abschnitt

Besondere Verwendungsarten von Daten

Automatisierte Einzelentscheidungen

§ 49. (1) Niemand darf einer für ihn rechtliche Folgen nach sich ziehenden oder einer ihn erheblich beeinträchtigenden Entscheidung unterworfen werden, die ausschließlich auf Grund einer automationsunterstützten Verarbeitung von Daten zum Zweck der Bewertung einzelner Aspekte seiner Person ergeht, wie beispielsweise seiner beruflichen Leistungsfähigkeit, seiner Kreditwürdigkeit, seiner Zuverlässigkeit oder seines Verhaltens.

(2) Abweichend von Abs. 1 darf eine Person einer ausschließlich automationsunterstützt erzeugten Entscheidung unterworfen werden, wenn

1. dies gesetzlich ausdrücklich vorgesehen ist oder
2. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages ergeht und dem Ersuchen des Betroffenen auf Abschluß oder Erfüllung des Vertrages stattgegeben wurde oder
3. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete

public sector controllers and relief organisations if they prove their identity and relation and the information is necessary to safeguard their rights or those of the affected person. The social insurance agencies shall be obliged to assist the public sector controllers and relief organisations with the verification of the data pursuant to para. 3 and the family relation. The authorities are authorized to collect the necessary data by administrative assistance and to use them for this purpose.

(5) Close relatives pursuant to this regulation are parents, children, spouses and companions in life of the data subjects. Other relatives shall receive the mentioned information under the same conditions as close relatives if they can satisfactorily demonstrate a special relationship to the person actually or presumably affected by the catastrophe.

(6) A relief organization in terms of this regulation is a generally recognized non-profit organisation with designated to assist people in emergencies as laid down in its charter or articles of association and which can be expected to deliver substantial aid in case of a catastrophe.

(7) all uses of data shall be logged pursuant to § 14 para. 2 sub-para 7.

(8) The legitimacy of any use of data based on any other case -outlined in § 8 and 9 shall not be affected.

Part 9

Special Uses of Data

Automated Individual Decisions

§ 49. (1) Nobody shall be subjected to a decision that produces legal effects concerning him or adversely affects him in a significant manner which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, for example his performance at work, creditworthiness, reliability and conduct.

(2) Deviating from para. 1, a person may be subjected to a decision based solely on auto¬mated processing if

1. this is expressly authorised by law or
2. the decision is taken in the course of the entering into or performance of a contract, and the request of the data subject [Betroffener] for the entering into or the performance of the contract has been satisfied or
3. the legitimate interests of the data subject are safeguarded by appropriate

Maßnahmen - beispielsweise die Möglichkeit, seinen Standpunkt geltend zu machen - garantiert wird.

(3) Dem Betroffenen ist bei automatisierten Einzelentscheidungen auf Antrag der logische Ablauf der automatisierten Entscheidungsfindung in allgemein verständlicher Form darzulegen. § 26 Abs. 2 bis 10 gilt sinngemäß.

Informationsverbundsysteme

§ 50. (1) Die Auftraggeber eines Informationsverbundsystems haben, soweit dies nicht bereits durch Gesetz geregelt ist, einen geeigneten Betreiber für das System zu bestellen. Name (Bezeichnung) und Anschrift des Betreibers sind in der Meldung zwecks Eintragung in das Datenverarbeitungsregister bekannt zu geben. Unbeschadet des Rechtes des Betroffenen auf Auskunft nach § 26 hat der Betreiber jedem Betroffenen auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen; in Fällen, in welchen der Auftraggeber gemäß § 26 Abs. 5 vorzugehen hätte, hat der Betreiber mitzuteilen, daß kein der Pflicht zur Auskunftserteilung unterliegender Auftraggeber benannt werden kann. Abgesehen von der abweichenden Frist gilt § 26 Abs. 3 bis 10 sinngemäß. Die Unterstützungspflicht des Betreibers gilt auch bei Anfragen von Behörden. Den Betreiber trifft überdies die Verantwortung für die notwendigen Maßnahmen der Datensicherheit (§ 14) im Informationsverbundsystem. Von der Haftung für diese Verantwortung kann sich der Betreiber unter den gleichen Voraussetzungen, wie sie in § 33 Abs. 3 vorgesehen sind, befreien. Wird ein Informationsverbundsystem geführt, ohne daß eine entsprechende Meldung an die Datenschutzkommission unter Angabe eines Betreibers erfolgt ist, treffen jeden einzelnen Auftraggeber die Pflichten des Betreibers.

(2) Durch entsprechenden Rechtsakt können auch weitere Auftraggeberpflichten, insbesondere auch die Vornahme der Meldung des Informationsverbundsystems, auf den Betreiber übertragen werden. Allein für die Übertragung der Meldepflicht ist die Vorlage von Vollmachten nach § 10 AVG nicht erforderlich. Soweit der Pflichtenübergang nicht durch Gesetz angeordnet ist, ist er gegenüber Dritten nur wirksam, wenn er – auf Grund einer entsprechenden Meldung an die Datenschutzkommission – aus der Registrierung im Datenverarbeitungsregister ersichtlich ist.

(2a) Wird ein Informationsverbundsystem auf Grund einer Meldung von zumindest zwei Auftraggebern registriert, so können Auftraggeber, die in der Folge die Teilnahme an dem Informationsverbundsystem anstreben, die Meldung im Umfang des § 19 Abs. 1 Z 3 bis 7 auf einen Verweis auf den Inhalt der Meldung eines bereits registrierten Auftraggebers beschränken, wenn sie eine Teilnahme im genau gleichen Umfang anstreben.

(3) Die Bestimmungen der Abs. 1 und 2 gelten nicht, soweit infolge der besonderen, insbesondere internationalen Struktur eines bestimmten

means such as arrangements allowing him to assert his point of view.

(3) Upon request, the data subject shall in case of automated decisions be informed of the logical procedure of the automated decision in an intelligible form. § 26 paras 2 to 10 are to be applied accordingly.

Joint Information Systems

§ 50. (1) The controllers [Auftraggeber] of a joint information system [Informationsverbundsystem] shall, unless already regulated by law, appoint a suitable operator [Betreiber] for the system. The name (designation) and address of the operator shall be included in the notification for registration in the Data Processing Register [Datenverarbeitungsregister]. Without prejudice to the data subject's rights pursuant to § 26, the operator shall give to the data subject [Betroffener] upon request within twelve weeks all information necessary to identify the controller who is responsible for the data processed in the system concerning him; in cases where the controller would have to apply § 26 para. 5, the operator shall inform the data subject that no controller obligated to give the information can be named. Notwithstanding the different deadline § 26 paras 3 to 10 applies accordingly. The operator's obligation to assist shall also apply in case of requests by public authorities. The operator shall also be responsible for the necessary data security measures (§ 14) in the joint information system. The operator can free himself of liability under the conditions laid down in § 33 para. 3. If a joint information system is operated and no appropriate notification with an appointed operator is filed with the Data Processing Register, each controller shall have to bear the obligations of the Operator.

(2) Further controller duties may be assigned to the operator by an appropriate legal instrument especially the duty of notification of the joint information system. Merely for the assignment of the notification obligation the presentation of powers according to § 10 General Administrative Act shall not be required. To the extent such assignment of duties is not provided by law it is only valid vis-á-vis third parties if the assignment is recorded in the Data Processing Register [Datenverarbeitungsregister] following an appropriate communication to the Data Protection Commission [Datenschutzkommission].

(2a) If a joint information system is registered based on the notification of at least two controllers, other controllers who subsequently wish to join the joint information system, may limit the registration in the extent of § 19 para 1 sub-para 3 to 7 to a reference to the content of the notification of an already registred controller, provided they intend to participate in exactly the same manner.

(3) The provisions of para. 1 and 2 shall not apply if provided for otherwise by law due to the special, in particular, international structure of a specific joint information

Informationsverbundsystems gesetzlich ausdrücklich anderes vorgesehen ist.

9a. Abschnitt

Videoüberwachung

Allgemeines

§ 50a. (1) Videoüberwachung im Sinne dieses Abschnittes bezeichnet die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt (überwachtes Objekt) oder eine bestimmte Person (überwachte Person) betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte. Für derartige Überwachungen gelten die folgenden Absätze, sofern nicht durch andere Gesetze Besonderes bestimmt ist.

(2) Für Videoüberwachung gelten die §§ 6 und 7, insbesondere der Verhältnismäßigkeitsgrundsatz (§ 7 Abs. 3). Rechtmäßige Zwecke einer Videoüberwachung, insbesondere der Auswertung und Übermittlung der dabei ermittelten Daten, sind jedoch vorbehaltlich des Abs. 5 nur der Schutz des überwachten Objekts oder der überwachten Person oder die Erfüllung rechtlicher Sorgfaltspflichten, jeweils einschließlich der Beweissicherung, im Hinblick auf Ereignisse nach Abs. 1. Persönlichkeitsrechte nach § 16 ABGB bleiben unberührt.

(3) Ein Betroffener ist durch eine Videoüberwachung dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen (§ 7 Abs. 2 Z 3) verletzt, wenn

1. diese im lebenswichtigen Interesse einer Person erfolgt, oder
2. Daten über ein Verhalten verarbeitet werden, das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden, oder
3. er der Verwendung seiner Daten im Rahmen der Überwachung ausdrücklich zugestimmt hat.

(4) Ein Betroffener ist darüber hinaus durch eine Videoüberwachung ausschließlich dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen (§ 7 Abs. 2 Z 3) verletzt, wenn sie nicht im Rahmen der Vollziehung hoheitlicher Aufgaben erfolgt und

1. bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt oder die überwachte Person könnte das Ziel oder der Ort eines gefährlichen Angriffs werden, oder
2. unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Gemeinschaftsrechts, Gesetze, Verordnungen, Bescheide oder gerichtliche Entscheidungen dem Auftraggeber spezielle Sorgfaltspflichten zum Schutz des überwachten Objekts oder der überwachten Person auferlegen, oder
3. sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte

system.

Part 9a.

Video surveillance

General

§ 50a. (1) Video surveillance in the sense of this part means the systematic, most of all continuous observation of occurrences concerning a certain object (observed object) or a certain person (observed person) by technical –devices designed to make or transmit images. The following paragraphs apply to such surveillance unless provided differently by other laws.

(2) §§ 6 and 7 apply to video surveillance, especially the principle of proportionality (§ 7 para 3). Lawful purposes for video surveillance, especially analysis and transmission of the data obtained such way, under reservation of para 5 only are the protection of the object or the person observed or the fulfilment of legal duties of diligence, including securing of evidence, with regard to occurrences according to para 1. Personal rights according to § 16 General Civil Code remain unaffected.

(3) A data subject concerned by video surveillance is not infringed in his/her interests for secrecy deserving protection (§ 7 para 2 sub-para 3) if,

1. it is made in the vital interest of a person, or
2. data on behaviour are processed which, without any doubt, has been intended to be publicly noticed, or
3. he/she has expressly consented to the use of his/her data in the context of the surveillance operation.

(4) A data subject concerned is exclusively not infringed in his/her interests for secrecy deserving protection (§ 7 para 2 sub-para 3), if the video-surveillance is not made in the performance of official executive tasks and

1. certain facts justify the presumption, that the object or person surveyed could become the target or the location of a dangerous attack, or
2. directly applicable legal rules of the international or EU-Law, laws, ordinances, orders or judicial decisions oblige the controller to special duties of diligence the for protection of the object or the person surveyed or
3. the surveillance is restricted to a mere real time reproduction of occurrences

Objekt/die überwachte Person betreffenden Ereignisse erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet werden (Echtzeitüberwachung), und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt.

(5) Mit einer Videoüberwachung nach Abs. 4 dürfen nicht Ereignisse an Orten festgestellt werden, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen. Weiters ist die Videoüberwachung zum Zweck der Mitarbeiterkontrolle an Arbeitsstätten untersagt.

(6) Schutzwürdige Geheimhaltungsinteressen Betroffener sind auch dann nicht verletzt, wenn durch Videoüberwachung aufgezeichnete Daten über eine Verwendung entsprechend den Abs. 2 bis 4 hinaus in folgenden Fällen übermittelt werden:

1. an die zuständige Behörde oder das zuständige Gericht, weil beim Auftraggeber der begründete Verdacht entstanden ist, die Daten könnten eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder
2. an Sicherheitsbehörden zur Ausübung der diesen durch § 53 Abs. 5 des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991, eingeräumten Befugnisse,

auch wenn sich die Handlung oder der Angriff nicht gegen das überwachte Objekt oder die überwachte Person richtet. Die Befugnisse von Behörden und Gerichten zur Durchsetzung der Herausgabe von Beweismaterial und zur Beweismittelsicherung sowie damit korrespondierende Verpflichtungen des Auftraggebers bleiben unberührt.

(7) Mit einer Videoüberwachung gewonnene Daten von Betroffenen dürfen nicht automationsunterstützt mit anderen Bilddaten abgeglichen und nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden.

Besondere Protokollierungs- und Löschungspflicht

§ 50b. (1) Jeder Verwendungsvorgang einer Videoüberwachung ist zu protokollieren. Dies gilt nicht für Fälle der Echtzeitüberwachung.

(2) Aufgezeichnete Daten sind, sofern sie nicht aus konkretem Anlass für die Verwirklichung der zu Grunde liegenden Schutz- oder Beweissicherungszwecke oder für Zwecke nach § 50a Abs. 6 benötigt werden, spätestens nach 72 Stunden zu löschen. § 33 Abs. 2 AVG gilt. Eine beabsichtigte längere Aufbewahrungsdauer ist in der Meldung anzuführen und zu begründen. In diesem Fall darf die Datenschutzkommission die Videoüberwachung nur registrieren, wenn dies aus besonderen Gründen zur Zweckerreichung regelmäßig erforderlich ist.

Meldepflicht und Registrierungsverfahren

§ 50c. (1) Videoüberwachungen unterliegen der Meldepflicht gemäß den §§ 17 ff. Sofern der Auftraggeber nicht in der Meldung zusagt, die Videoüberwachungsdaten zu verschlüsseln und unter Hinterlegung des einzigen Schlüssels bei der

concerning the surveyed object/the surveyed person which, therefore, are neither recorded nor processed in any other way (real time surveillance) and is performed for the purpose of the protection of health, life or property of the controller.

(5) Video surveillance according to para 4 must not observe occurrences at locations that are part of the most personal area of life of a data subject. Furthermore, video surveillance for staff-control at places of work is prohibited.

(6) Interests for secrecy of data subjects concerned deserving protection are also not infringed if data recorded by video surveillance, in cases exceeding a use in accordance with paras 2 to 4, are transmitted:

1. to the competent authority or the court, because the controller has reasonable ground for suspicion that the data could document a criminal act punishable by the courts to be prosecuted ex officio or
2. to police authorities in order to carry out their function granted under the Police Act (SPG) Federal Law Gazette No. 566/1991,

even if the action or attack is not directed against the object or the person surveyed. The rights of authorities and courts to enforce the submission of documented evidence and to secure means of evidence and the corresponding obligations of the controller remain unaffected.

(7) Data collected of data subjects concerned by video surveillance may not be analyzed by comparison with other picture data and not be searched using sensitive data as selection criteria.

Special duty of documentation and deletion

§ 50b. (1) Any use of video surveillance is to be documented. This does not apply to real time observation.

(2) Data recorded are to be deleted the latest after 72 hours, unless needed on a specific occasion for the intended purposes of protection or securing evidence or for purposes according to § 50a para 6. § 33 para 2 General Administrative Act is to be applied. An intended longer duration of storage is to be indicated in the notification and must be explained. In such case the Data Protection Commission may register the video surveillance only if this is regularly necessary for specific reasons to serve the purposes.

Obligation of notification and procedure of registration

§ 50c. (1) Video surveillances are subject to the obligation of notification according to §§ 17 et seq. If the controller does not specify in the notification that the video surveillance data are to be encrypted and does not ensure that an analysis of the

Datenschutzkommission sicherzustellen, dass eine Auswertung der Videoaufzeichnungen nur im begründeten Anlassfall durch eine bestimmte Stelle stattfindet, unterliegen sie der Vorabkontrolle (§ 18 Abs. 2). Bestimmte Tatsachen im Sinn von § 50a Abs. 4 Z 1 müssen bei Erstattung der Meldung glaubhaft gemacht werden. Soweit gemäß § 96a des Arbeitsverfassungsgesetzes 1974 – ArbVG, BGBl. Nr. 22, Betriebsvereinbarungen abzuschließen sind, sind diese im Registrierungsverfahren vorzulegen.

(2) Eine Videoüberwachung ist über § 17 Abs. 2 und 3 hinaus von der Meldepflicht ausgenommen

1. in Fällen der Echtzeitüberwachung oder
2. wenn eine Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium erfolgt.

(3) Mehrere überwachte Objekte oder überwachte Personen, für deren Videoüberwachung derselbe Auftraggeber eine gesetzliche Zuständigkeit oder rechtliche Befugnis (§ 7 Abs. 1) hat, können auf Grund ihrer gleichartigen Beschaffenheit oder ihrer räumlichen Verbundenheit in einer Meldung zusammengefasst werden, wenn sich diese auf die gleiche Rechtsgrundlage stützt.

Information durch Kennzeichnung

§ 50d. (1) Der Auftraggeber einer Videoüberwachung hat diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Auftraggeber eindeutig hervorzugehen, es sei denn, dieser ist den Betroffenen nach den Umständen des Falles bereits bekannt. Die Kennzeichnung hat örtlich derart zu erfolgen, dass jeder potentiell Betroffene, der sich einem überwachten Objekt oder einer überwachten Person nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen.

(2) Keine Kennzeichnungsverpflichtung besteht bei Videoüberwachungen im Rahmen der Vollziehung hoheitlicher Aufgaben, die nach § 17 Abs. 3 von der Meldepflicht ausgenommen sind.

Auskunftsrecht

§ 50e. (1) Abweichend von § 26 Abs. 1 ist dem Auskunftswerber, nachdem dieser den Zeitraum, in dem er möglicherweise von der Überwachung betroffen war, und den Ort möglichst genau benannt und seine Identität in geeigneter Form nachgewiesen hat, Auskunft über die zu seiner Person verarbeiteten Daten durch Übersendung einer Kopie der zu seiner Person verarbeiteten Daten in einem üblichen technischen Format zu gewähren. Alternativ kann der Auskunftswerber eine Einsichtnahme auf Lesegeräten des Auftraggebers verlangen, wobei ihm auch in diesem Fall die Ausfolgung einer Kopie zusteht. Die übrigen Bestandteile der Auskunft (verfügbare Informationen über die Herkunft, Empfänger oder Empfängerkreise von Übermittlungen, Zweck, Rechtsgrundlagen sowie allenfalls Dienstleister) sind auch im Fall der Überwachung schriftlich zu erteilen, wenn nicht der Auskunftswerber einer

video surveillance data may only take place through a certain institution in a specific case by depositing the sole code key with the Data Protection Commission, they are subject to prior checking (§ 18 para 2). When filing the notification prima facie evidence must be given for facts in the sense of § 50a para 4 sub-para 1. To the extent agreements between the works committee and the management are to be concluded according to § 96a of the Labour Constitution Act 1974 - ArbVG, Federal Law Gazette No. 22, such are to be submitted in the registration procedure.

(2) Beyond § 17 para 2 and 3, video surveillance is exempted from the notification obligation

1. in cases of real-time observation or
2. if the recording is only made on a analog video recording system.

(3) If the same controller has the statutory competence or legitimate authority (§ 7 para 1) for video surveillance of several objects or persons, he may submit a combined notification based on their similar quality or local connection, if the legal basis is identical.

Information by signs

§ 50d. (1) The controller of a video surveillance shall put up appropriate signs. The sign shall specify who the controller is, unless already known to the data subjects based on the circumstances of the case. The information sign has to be fixed in places in a way, that any potential data subject approaching the surveyed object or person has the possibility to bypass the video surveillance.

(2) Video surveillances within the frame of implementation of official executive tasks, being exempted from the obligation of notification according to § 17 para 3, need not be marked with signs.

Right of information

§ 50e. (1) Deviating from § 26 para 1, the person requesting information, after having indicated the timeframe during which he/she might have been captured by the surveillance and after having indicated the location as precisely as possible and after having proven his/her identity in adequate manner, is to be granted information on the data processed on his/her person, by sending of a copy on the data processed to his/her person in a common technical format. Alternately, the person requesting information may request inspection on a reading device of the controller and is also entitled to be handed over a copy in such case. The other elements of the information (available data on the origin, recipient or circles of recipients of data transmitted, purpose, legal basis and eventually service providers) are to be given in writing also in case of surveillance, unless the person requesting information agrees to oral information.

mündlichen Auskunftserteilung zustimmt.

(2) § 26 Abs. 2 ist mit der Maßgabe anzuwenden, dass in dem Fall, dass eine Auskunft wegen überwiegender berechtigter Interessen Dritter oder des Auftraggebers nicht in der in Abs. 1 geregelten Form erteilt werden kann, der Auskunftswerber Anspruch auf eine schriftliche Beschreibung seines von der Überwachung verarbeiteten Verhaltens oder auf eine Auskunft unter Unkenntlichmachung der anderen Personen hat.

(3) In Fällen der Echtzeitüberwachung ist ein Auskunftsrecht ausgeschlossen.

10. Abschnitt

Strafbestimmungen

Datenverwendung in Gewinn- oder Schädigungsabsicht

§ 51. 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 zu bestrafen.

Verwaltungsstrafbestimmung

§ 52. (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 25 000 Euro zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält oder
2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 15) übermittelt, insbesondere Daten, die ihm gemäß §§ 46 oder 47 anvertraut wurden, vorsätzlich für andere Zwecke verwendet oder
3. Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtigstellt oder nicht löscht oder
4. Daten vorsätzlich entgegen § 26 Abs. 7 löscht;
5. sich unter Vortäuschung falscher Tatsachen vorsätzlich Daten gemäß § 48a verschafft.

(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit

(2) § 26 para 2 is to be applied with the proviso, that in case, that an information cannot be disclosed because of overriding legitimate interests of third parties or of the controller in a manner as described in para 1, the person requesting information is entitled to a written description of his/her behaviour processed by the surveillance or to an information, in which other persons have been made unrecognizable.

(3) In cases of real time surveillance there is no right for information.

Part 10

Penal Provisions

Use of Data with the Intention to make a Profit or to Cause Harm

§ 51. (1) Whoever with the intention to enrich himself or a third person unlawfully or to harm someone in his entitlement guaranteed according to § 1 para 1 deliberately uses personal data that have been entrusted to or made accessible to him solely because of professional reasons, or that he has acquired illegally, for himself or makes such data available to others or publishes such data with the intention to make a profit or to harm others, despite the data subject's interest in secrecy deserving protection, shall be punished by a court with imprisonment up to a year, unless the offence shall be subject to a more severe punishment pursuant to another provision.

Administrative Penalties

§ 52. (1) Insofar as the act does not realise the legal elements of a criminal offence subject to the jurisdiction of the courts of law and is not subject to more severe penalties according to another administrative provision, an administrative offence punishable by a fine of up to 25 000 Euro is committed by anyone who

1. intentionally and illegally gains access to a data application [Datenanwendung] or maintains an obviously illegal means of access or
2. transmits data intentionally in violation of the rules on confidentiality (§ 15), and in particular anybody who uses data entrusted to him according to § 46 and 47 for other purposes or
3. uses or fails to grant information, to rectify or erase data in violation of a final judicial decision or ruling [Bescheid],
4. intentionally erases data in violation of § 26 para. 7;
5. by pretending incorrect facts intentionally obtains data according to § 48a.

(2) Insofar as the act does not realise the legal elements of a criminal offence subject to the jurisdiction of the courts of law, an administrative offence punishable by

Geldstrafe bis zu 10 000 Euro zu ahnden ist, wer

1. Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß den §§ 17 oder 50c erfüllt zu haben oder eine Datenanwendung auf eine von der Meldung abweichende Weise betreibt oder
2. Daten ins Ausland übermittelt oder überlässt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 Abs. 1 eingeholt zu haben oder
3. gegen gemäß § 13 Abs. 2 Z 2, § 19 oder § 50c Abs. 1 abgegebene Zusagen oder von der Datenschutzkommission gemäß § 13 Abs. 1 oder § 21 Abs. 2 erteilte Auflagen verstößt oder
4. seine Offenlegungs- oder Informationspflichten gemäß den §§ 23, 24, 25 oder 50d verletzt oder
5. die gemäß § 14 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht lässt oder
6. die gemäß § 50a Abs. 7 und § 50b Abs. 1 erforderlichen Sicherheitsmaßnahmen außer Acht lässt oder
7. Daten nach Ablauf der in § 50b Abs. 2 vorgesehene Löschungsfrist nicht löscht.

(2a) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit einer Strafe bis zu 500 Euro zu ahnden ist, wer Daten entgegen den §§ 26, 27 oder 28 nicht fristgerecht beauskunftet, richtigstellt oder löscht.

(3) Der Versuch ist strafbar.

(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 oder 2 in Zusammenhang stehen.

(5) Zuständig für Entscheidungen nach Abs. 1 bis 4 ist die Bezirksverwaltungsbehörde, in deren Sprengel der Auftraggeber (Dienstleister) seinen gewöhnlichen Aufenthalt oder Sitz hat. Falls ein solcher im Inland nicht gegeben ist, ist die am Sitz der Datenschutzkommission eingerichtete Bezirksverwaltungsbehörde zuständig.

11. Abschnitt

Übergangs- und Schlußbestimmungen

Befreiung von Gebühren, Abgaben und vom Kostenersatz

§ 53. (1) Die durch dieses Bundesgesetz unmittelbar veranlaßten Eingaben der

a fine of up to 10 000 Euro is committed by anyone who

1. collects, processes and transmits data without having fulfilled his obligation to notification according to §§ 17 or 50c or operates a data application in a manner deviating from the notification.
2. engages in transborder data transmissions [Übermittlungen] or committings [Überlassungen] without the necessary permit of the Data Protection Commission [Datenschutzkommission] according to § 13 para 1or
3. violates declarations given according to § 13 para 2 sub-para. 2, § 19 or 50c para 1 or conditions imposed by the Data Protection Commission according to § 13 para 1 or § 21 para 2 or
4. violates his obligations of disclosure and information according to sects. 23, 24, 25 and 50d or
5. grossly neglects the required data security measures according to § 14 or
6. disregards the safety measures required according to § 50a para 7 and § 50b para 1 or
7. does not delete data after expiring of the period provided for in § 50b para 2 for deletion.

(2a) To the extent the act does not constitute a criminal offence within the jurisdiction of the courts or is punishable under other administrative penal regulations, who, contrary to §§ 26, 27 or 28, does not in time give information on, corrects or deletes data, commits an administrative offence to be punished with a fine up to € 500.

(3) Attempts shall be punished.

(4) Data media or programs as well as picture transmitting or -recording devices can be confiscated (sects. 10, 17 and 18 VStG), if they are linked to an administrative offence according to para. 1 and 2.

(5) The District Administrative Authority [Bezirksverwaltungsbehörde] at the controllers [Auftraggeber] (processors [Dienstleister]) domicile or seat shall be the competent authority for decisions according to para. 1 to 4. If there is no domicile or seat in Austria, the District Administrative Authority at the seat of the Data Protection Commission [Datenschutzkommission] shall be competent.

Part 11

Transitional and Final Provisions

Exemption from Fees

§ 53. (1) All applications submitted according to this Federal Act [Bundesgesetz]

Betroffenen zur Wahrung ihrer Interessen sowie die Eingaben im Registrierungsverfahren und die gemäß § 21 Abs. 3 zu erstellenden Registerauszüge sind von den Stempelgebühren und von den Verwaltungsabgaben des Bundes befreit.

(2) Für Abschriften aus dem Datenverarbeitungsregister, die ein Betroffener zur Verfolgung seiner Rechte benötigt, ist kein Kostenersatz zu verlangen.

Mitteilungen an die Europäische Kommission und an die anderen Mitgliedstaaten der Europäischen Union

§ 54. (1) Von der Erlassung eines Bundesgesetzes, das die Zulässigkeit der Verarbeitung sensibler Daten betrifft, hat der Bundeskanzler anläßlich der Kundmachung des Gesetzes im Bundesgesetzblatt der Europäischen Kommission Mitteilung zu machen.

(2) Die Datenschutzkommission hat den anderen Mitgliedstaaten der Europäischen Union und der Europäischen Kommission mitzuteilen, in welchen Fällen

1. keine Genehmigung für den Datenverkehr in ein Drittland erteilt wurde, weil die Voraussetzungen des § 13 Abs. 2 Z 1 nicht als gegeben erachtet wurden;
2. der Datenverkehr in ein Drittland ohne angemessenes Datenschutzniveau genehmigt wurde, weil die Voraussetzungen des § 13 Abs. 2 Z 2 als gegeben erachtet wurden.

Feststellungen der Europäischen Kommission

§ 55. Der Inhalt der in einem Verfahren gemäß Art. 31 Abs. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S. 31, getroffenen Feststellungen der Europäischen Kommission über

1. das Vorliegen oder Nichtvorliegen eines angemessenen Datenschutzniveaus in einem Drittland oder
2. die Eignung bestimmter Standardvertragsklauseln oder Verpflichtungserklärungen zur Gewährleistung eines ausreichenden Schutzes der Datenverwendung in einem Drittland

ist vom Bundeskanzler im Bundesgesetzblatt gemäß § 4 des Bundesgesetzblattgesetzes, BGBl. I Nr. 100/2003, kundzumachen.

Verwaltungsangelegenheiten gemäß Art. 30 B-VG

§ 56. Der Präsident des Nationalrats ist Auftraggeber jener Datenanwendungen, die für Zwecke der ihm gemäß Art. 30 B-VG übertragenen Angelegenheiten durchgeführt werden. Übermittlungen von Daten aus solchen Datenanwendungen dürfen nur über Auftrag des Präsidenten des Nationalrats vorgenommen werden. Der Präsident trifft Vorsorge dafür, daß im Falle eines Übermittlungsauftrags die

by data subjects [Betroffener] to safeguard their interests as well as all applications in the proceedings for notification and for register statements according to § 21 para. 3 shall be exempt from stamp duties and federal administrative fees.

(2) No fee shall be charged for copies of entries in the Data Processing Register [Datenverarbeitungsregister] needed by a data subject to assert his rights.

Communication to the European Commission and to the other Member States of the European Union

§ 54. (1) The Federal Chancellor [Bundeskanzler] shall communicate to the European Commission whenever a Federal Act [Bundesgesetz] concerning the right to process sensitive data has been adopted upon its promulgation in the Federal Law Gazette [Bundesgesetzblatt].

(2) The Data Protection Commission [Datenschutzkommission] shall communicate to the other member states of the European Union and the European Commission in which cases

1. no permit was issued for transborder data flows to a third country because the requirements of § 13 para. 2 sub-para 1 were considered not to have been met;
2. a permit was issued for transborder data flows to a third country without an adequate level of data protection because the requirements of § 13 para. 2 sub-para 2 are deemed to have been met.

Measures of the European Commission

§ 55. The content of findings of the European Commission made according to Art. 31 para. 2 of the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23 November 1995 p. 0031, on

1. whether a third country has an adequate level of data protection or
2. the suitability of certain standard contractual clauses or pledges to safeguard sufficient protection to the use of data [Datenverwendung] in a third country

shall be promulgated by the Federal Chancellor [Bundeskanzler] in the Federal Law Gazette according to § 4 BGBlG , Federal Law Gazette I No. 100/2003.

Administrative Matters pursuant to Art. 30 of the Federal Constitution

§ 56. The President of the National Council [Nationalrat] is the controller [Auftraggeber] of such data applications [Datenanwendungen] for purposes of such matters with which he has been entrusted pursuant to art. 30 B VG . Transmissions of data [Übermittlungen] from such data applications shall only take place if ordered by the President of the National Council. The President shall make provisions that in case

Voraussetzungen des § 7 Abs. 2 vorliegen und insbesondere die Zustimmung des Betroffenen in jenen Fällen eingeholt wird, in welchen dies gemäß § 7 Abs. 2 mangels einer anderen Rechtsgrundlage für die Übermittlung notwendig ist.

Sprachliche Gleichbehandlung

§ 57. Soweit in diesem Artikel 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.

Manuelle Dateien

§ 58. Soweit manuell, dh. ohne Automationsunterstützung geführte Dateien für Zwecke solcher Angelegenheiten bestehen, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist, gelten sie als Datenanwendungen im Sinne des § 4 Z 7. § 17 gilt mit der Maßgabe, daß die Meldepflicht nur für solche Dateien besteht, deren Inhalt gemäß § 18 Abs. 2 der Vorabkontrolle unterliegt.

Umsetzungshinweis

§ 59. Mit diesem Bundesgesetz wird die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S 31, umgesetzt.

Inkrafttreten

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

(2) Die übrigen Bestimmungen dieses Bundesgesetzes treten ebenfalls mit 1. Jänner 2000 in Kraft.

(3) §§ 26 Abs. 6 und 52 Abs. 1 und 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 136/2001 treten mit 1. Jänner 2002 in Kraft.

(4) § 48a Abs. 5 in der Fassung des Bundesgesetzes BGBl. I Nr. 135/2009 tritt mit 1. Jänner 2010 in Kraft.

(5) Das Inhaltsverzeichnis, § 4 Abs. 1 Z 4, 5, 7 bis 9, 11 und 12, § 8 Abs. 1, 2 und 4, § 12 Abs. 1, die Umnummerierung der Absätze in § 13, § 16 Abs. 1 und 3, § 17 Abs. 1, 1a und 4, § 19 Abs. 1 Z 3a und Abs. 2, die Umnummerierung der Absätze in § 19, die §§ 20 bis 22a samt Überschriften, § 24 Abs. 2a, § 24 Abs. 4, § 26 Abs. 1 bis 8 und 10, § 28 Abs. 3, § 30 Abs. 2a, 5 bis 6a, die §§ 31 und 31a samt Überschriften, § 32 Abs. 1, 4, 6 und 7, § 34 Abs. 1, 3 und 4, § 36 Abs. 3, 3a und 9, § 39 Abs. 5, § 40 Abs. 1 und 2, § 41 Abs. 2 Z 4a, § 42 Abs. 1 Z 1, § 42 Abs. 5, § 46 Abs. 1 Z 2 und 3, Abs. 2 bis 3a, § 47 Abs. 4, § 49 Abs. 3, § 50 Abs. 1 bis 2a, der 9a. Abschnitt, § 51, § 52 Abs. 2

of a transmission order the requirements of § 7 para. 2 are met and, in particular, that the consent of the data subject [Betroffener] is obtained in such cases where it is necessary pursuant to § 7 para. 2 for lack of another legal basis for the transmission.

Gender-Neutral Use of Language

§ 57. Insofar as expressions relating to natural persons in this article 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.

Manual Filing Systems

§ 58. Insofar as manual filing systems, i.e., filing systems [Dateien] managed without automatic processing, exist for such purposes and fields where the Federation [Bund] has the power to pass laws, they are deemed to be data applications [Daten¬anwendungen] according to § 4 sub-para. 7. § 17 shall apply insofar as the obligation to notification applies only to those filing systems whose content is subject to prior checking [Vorabkontrolle] according to § 18 para. 2.

Implementation Notice

§ 59. This Federal Act [Bundesgesetz] implements the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23 November 1995 p. 31 .

Entry into Force

§ 60. *(Note: Repealed by Federal Law Gazette I No. 2/2008)*

(2) The other provisions of this Federal Act shall enter into force on 1 January 2000 as well.

(3) Sects. 26 para. 6 and 52 para. 1 and 2 as formulated in the federal law published in Federal Law Gazette I No. 136/2001 shall enter into force on 1 January 2002.

(4) § 48a para 5 in the version of the Federal Act, Federal Law Gazette I No. 135/2009 enters into force on 1st January 2010.

(5) The table of contents, § 4 para 1 sub-para. 4, 5, 7 to 9, 11 and 12, § 8 para 1, 2 and 4, § 12 para 1, the re-numbering of the paragraphs in § 13, § 16 para 1 and 3, § 17 para 1, 1a and 4, § 19 para 1 sub-para. 3a and para 2, the re-numbering of the paragraphs in § 19, the §§ 20 to 22a including captions, § 24 para 2a, § 24 para 4, § 26 para 1 to 8 and 10, § 28 para 3, § 30 para 2a, 5 to 6a, the §§ 31 and 31a including captions, § 32 para 1, 4, 6 and 7, § 34 para 1, 3 and 4, § 36 para 3, 3a and 9, § 39 para 5, § 40 para 1a and 2, § 41 para 2 sub-para. 4a, § 42 para 1 sub-para. 1, § 42 para 5, § 46 para 1 sub-para. 2 and 3, para 2 to 3a, § 47 para 4, § 49 para 3, § 50 para 1 to 2a, chapter 9a., § 51, § 52 para 2

und 4, § 55, § 61 Abs. 6 bis 9 sowie § 64 in der Fassung des Bundesgesetzes BGBl. I Nr. 133/2009 treten mit 1. Jänner 2010 in Kraft. Gleichzeitig treten § 4 Abs. 1 Z 10, § 13 Abs. 3 sowie § 51 Abs. 2 außer Kraft.

(6) § 36 Abs. 6 in der Fassung des Bundesgesetzes BGBl. I Nr. 133/2009 tritt am 1. Juli 2010 in Kraft.

Übergangsbestimmungen

§ 61. (1) Meldungen, die vor Inkrafttreten dieses Bundesgesetzes an das Datenverarbeitungsregister erstattet wurden, gelten als Meldungen im Sinne des § 17, soweit sie nicht im Hinblick auf das Entfallen von Meldepflichten gemäß § 17 Abs. 2 oder 3 gegenstandslos geworden sind. Desgleichen gelten vor Inkrafttreten dieses Bundesgesetzes durchgeführte Registrierungen als Registrierungen im Sinne des § 21.

(2) Soweit nach der neuen Rechtslage eine Genehmigung für die Übermittlung von Daten ins Ausland erforderlich ist, muß für Übermittlungen, für die eine Genehmigung vor Inkrafttreten dieses Bundesgesetzes erteilt wurde, eine Genehmigung vor dem 1. Jänner 2003 neu beantragt werden. Wird der Antrag rechtzeitig gestellt, dürfen solche Übermittlungen bis zur rechtskräftigen Entscheidung über den Genehmigungsantrag fortgeführt werden.

(3) Datenschutzverletzungen, die vor dem Inkrafttreten dieses Bundesgesetzes stattgefunden haben, sind, soweit es sich um die Feststellung der Rechtmäßigkeit oder Rechtswidrigkeit eines Sachverhalts handelt, nach der Rechtslage zum Zeitpunkt der Verwirklichung des Sachverhalts zu beurteilen; soweit es sich um die Verpflichtung zu einer Leistung oder Unterlassung handelt, ist die Rechtslage im Zeitpunkt der Entscheidung in erster Instanz zugrundezulegen. Ein strafbarer Tatbestand ist nach jener Rechtslage zu beurteilen, die für den Täter in ihrer Gesamtauswirkung günstiger ist; dies gilt auch für das Rechtsmittelverfahren.

(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.

(5) Manuelle Datenanwendungen, die gemäß § 58 der Meldepflicht unterliegen, sind, soweit sie schon im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bestanden haben, dem Datenverarbeitungsregister bis spätestens 1. Jänner 2003 zu melden. Dasselbe gilt für automationsunterstützte Datenanwendungen gemäß § 17 Abs. 3, für die durch die nunmehr geltende Rechtslage die Meldepflicht neu eingeführt wurde.

(6) Videoüberwachungen, die vor dem Inkrafttreten der §§ 50a bis 50e registriert wurden, bleiben in ihrer registrierten Form rechtmäßig, wenn sie den am 31. Dezember

and 4, § 55, § 61 para 6 to 9 as well as § 64 in the version of the Federal Act, Federal Law Gazette I No. 133/2009, enter into force on 1st January 2010. Simultaneously § 4 para 1 v 10, § 13 para 3 as well as § 51 para 2 become ineffective.

(6) § 36 para 6 in the version of the Federal Act, Federal Law Gazette I No. 133/2009, enters into force on 1st July 2010.

Transitional Provisions

§ 61. (1) Notifications that were made to the Data Processing Register [Datenverarbeitungsregister] before this Federal Act [Bundesgesetz] entered into force shall count as notifications according to § 17, insofar as they have not become irrelevant because the obligation to notify is no longer applicable. Likewise, registrations made before this Federal Act entered into force shall count as registrations according to § 21.

(2) Insofar as the law as it now stands requires a permit for transborder data transmission [Übermittlung], an application for a new permit must be filed before 1 January 2003 for such transmissions for which a permit was granted prior to this Federal Acts entry into force. If the application is filed in time, such transmissions may be carried out until the final decision about the application for the permit.

(3) Data protection violations that have taken place before this Federal Act entered into force shall, insofar as the legality or illegality of a set of facts is concerned, be adjudicated according to the legal provisions in force at the time the act was committed; insofar as an obligation to act or a forbearance is concerned, the law as its stands at the time when the decision of first instance is rendered shall be applied. A criminal offence shall be adjudicated according to the law that is more favourable to the offender overall; this also extends to appeal proceedings.

(4) (Constitutional Provision) Data applications [Daten¬anwendungen] 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 sub-para. 1 to 3 until federal regulations covering the functions and powers in these fields are enacted.

(5) Manual filing systems subject to notification according to § 58 shall be notified to the Data Processing Register no later than 1 January 2003, provided they already existed when this Federal Act entered into force. The same shall apply to automated data applications according to § 17 para. 3 that were made subject to notification by the new regulations.

(6) Notifications for video surveillance that were registered before §§ 50a to 50e entered into force remain lawful in the registered version if they correspond with the

2009 geltenden datenschutzrechtlichen Bestimmungen genügen und die Datenschutzkommission keine Befristung verfügt hat. Hat die Datenschutzkommission hingegen eine Befristung einer solchen Videoüberwachung verfügt, bleibt diese bis zum Ablauf der Befristung, längstens aber bis zum 31. Dezember 2012 rechtmäßig.

(7) Soweit in einzelnen Vorschriften Verweise auf das Datenschutzgesetz, BGBl. Nr. 565/1978, enthalten sind, gelten diese bis zu ihrer Anpassung an dieses Bundesgesetz sinngemäß weiter.

(8) Die Verordnung nach § 16 Abs. 3 ist vom Bundeskanzler nach Maßgabe der technischen Möglichkeiten des Datenverarbeitungsregisters bis spätestens 1. Jänner 2012 neu zu erlassen. Bis zum Inkrafttreten dieser Verordnung sind die §§ 16 bis 22, § 30 Abs. 3 und 6 sowie § 40 Abs. 1 (letzterer mit Ausnahme des Verweises auf § 31a Abs. 3) in der Fassung vor dem Bundesgesetz BGBl. I Nr. 133/2009 anzuwenden; § 22a, § 30 Abs. 2a und 6a, § 31a Abs. 1 und 2 sowie § 32 Abs. 7 sind bis dahin nicht anzuwenden. § 31 Abs. 3 in der Fassung vor dem Bundesgesetz BGBl. I Nr. 133/2009 ist bis dahin zusätzlich weiter anzuwenden. Die Erklärung, ob eine Datenanwendung einen oder mehrere der in § 18 Abs. 2 Z 1 bis 4 genannten Tatbestände erfüllt (§ 19 Abs. 1 Z 3a), ist der Datenschutzkommission bei im Zeitpunkt des Inkrafttretens der neuen Verordnung nach § 16 Abs. 3 registrierten Datenanwendungen anlässlich der ersten über eine Streichung hinausgehenden Änderungsmeldung zu melden, die nach diesem Zeitpunkt erstattet wird. Eine Meldung allein im Hinblick auf § 19 Abs. 1 Z 3a ist nicht erforderlich.

Verordnungserlassung

§ 62. 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

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

Vollziehung

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

regulations on data protection in force on 31 December 2009 and the Data Protection Commission has not imposed a time limit. If, however, the Data Protection Commission has imposed a time limit for such video surveillance, it remains lawful till the time limit has expired, the latest till 31 December 2012.

(7) Insofar as individual provisions contain references to the Data Protection Act [Datenschutzgesetz], Federal Law Gazette No. 565/1978, such provisions shall be valid by analogous application until adjusted to conform to this Federal Act.

(8) The ordinance according to § 16 para 3 shall be re-issued by the Federal Chancellor, in accordance with the technical possibilities of the data processing register, on 1st January 2012 at the latest. Until this ordinance enters into force §§ 16 to 22, § 30 para 3 and 6 as well as § 40 para 1 (the latter with the exception of the reference to § 31a para 3) in the version of the Federal Act, Federal Law Gazette I No. 133/2009, is to be applied, § 22a, § 30 para 2a and 6a, § 31a para 1 and 2 as well as § 32 para 7 are not to be applied; up to such date. § 31 para 3 in the version before the Federal Act, Federal Law Gazette I No. 133/2009, is, in addition, to be applied. The statement, whether a data application matches at least one of the elements of § 18 para 2 sub-para. 1 to 4 (§ 19 para 1 sub-para. 3a), is to be notified to the data protection commission for data applications which are already registered when the new ordinance according to § 16 para 3 enters in to force at the occasion of the first notification of any change other than deletion. A notification solely with regard to § 19 para 1 sub-para. 3a is not necessary.

Enactment of Ordinances

§ 62. Ordinances [Verordnungen] based on this Federal Act [Bundesgesetz] in the current version in force 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

§ 63. Insofar as provisions of this Federal Act [Bundesgesetz] refer to provisions of other Federal Acts, these shall be applied in the current version in force .

Execution

§ 64. The Federal Chancellor [Bundeskanzler] and the other Federal Ministers [Bundesminister] within their purview shall execute this Federal Act [Bundesgesetz] insofar as the execution has not been entrusted to the Federal Government [Bundesregierung].