

1024 der Beilagen zu den stenographischen Protokollen des Nationalrates XIV. GP

Bericht

des Verfassungsausschusses

**über die Regierungsvorlage (72 der Beilagen):
Bundesgesetz über den Schutz personsbezogener
Daten (Datenschutzgesetz – DSG)
und
über den Antrag 21/A der Abgeordneten Dr.
Ermacora und Genossen betreffend ein
Bundesverfassungsgesetz über Datenschutz
und Datensicherung**

Der vom Verfassungsausschuß zur Vorbehandlung der gegenständlichen Vorlagen eingesetzte Unterausschuß, dem von der SPÖ die Abgeordneten Dr. Fischer – bis 7. Oktober 1977 – bzw. an dessen Stelle Dr. Veselsky – ab 14. Oktober 1977 –, Dr. Gradenegger, Ing. Hobl, Mondl und Wuganigg, von der ÖVP die Abgeordneten Dr. Ermacora, Dr. Hauser, Dr. Pelikan und Steinbauer sowie von der FPÖ der Abgeordnete Dr. Schmidt angehörten, hat die Gesetzentwürfe in insgesamt 24 Sitzungen beraten.

An den Unterausschußberatungen haben teilgenommen:

in Vertretung des Bundeskanzlers, des zuständigen Mitgliedes der Bundesregierung, Staatssekretär Dr. Veselsky bis zu seiner Wahl zum Obmann des Unterausschusses am 14. Oktober 1977, nach diesem Zeitpunkt Staatssekretär Univ.-Prof. DDr. Nussbaumer und bei dessen Verhinderung die Staatssekretäre Elfriede Karl bzw. Dr. Löschnak;

als Experten Dr. Michael Arié, Dr. Walter Dohr, Dr. Alfred Duschanek, Dr. Günter Gerber, Univ.-Prof. Dr. Helmut Kerner, Dipl.-Ing. DDr. Werner Koenne, Senatsrat Dipl.-Ing. Lucian Koloseus, Dr. Peter Kostelka, Dr. Walther Richter, Dr. Norbert Rozsenich und Mag. Norbert Vanas;

seitens des Bundeskanzleramtes – Verfassungsdienst der zuständige Abteilungsleiter Mag. Dr. Gerhard Stadler.

Am 27. September 1978 hat der Unterausschuß Vertreter der Länder, des Städtebundes und des Gemeindebundes zu Fragen des Datenschutzes gehört.

Als Ergebnis der Unterausschußberatungen wurde dem Verfassungsausschuß am 5. Oktober 1978 der

gegenständliche Gesetzentwurf vorgelegt, in dem die Bestimmungen über den Datenschutz gegenüber der Regierungsvorlage 72 der Beilagen zur Gänze neu gefaßt sind. Insbesondere enthält der Entwurf nunmehr im Sinne des Initiativantrages 21/A verfassungsgesetzliche Bestimmungen über ein Grundrecht auf Datenschutz. Ferner wurden neben einem Abschnitt über den Datenschutz im öffentlichen Bereich ein weiterer gleichartig gegliederter Abschnitt über den Datenschutz im privaten Bereich aufgenommen. Schließlich enthält der Gesetzentwurf Bestimmungen über den internationalen Datenverkehr und sieht außer der Einrichtung einer Datenschutzkommission, die insbesondere – neben den Gerichten – zur Einhaltung der Bestimmungen des Gesetzes berufen ist, die Schaffung eines Datenschutzzrates vor, der vor allem den Datenschutz betreffende rechtspolitische Fragen zu beraten hat.

Zum vorliegenden Gesetzentwurf wird allgemein festgestellt:

1. Der Entwurf gliedert sich in 58 Paragraphen mit mehreren Verfassungsbestimmungen. Im Art. 1 des Entwurfes sind als Verfassungsbestimmung eine Grundrechtsbestimmung sowie die Festlegung der Kompetenzverteilung vorgesehen; der Art. 2 gliedert sich in 7 Abschnitte: Allgemeine Bestimmungen, Bestimmungen für den öffentlichen Bereich, Bestimmungen für den privaten Bereich, internationaler Datenverkehr, Kontrolle des Datenschutzes, Strafbestimmungen, Schlußbestimmungen.

Auf eine Verwendung römischer Zahlen in der Gliederung wurde entgegen der traditionellen Gesetzgebungspraxis verzichtet, da dies die Einspeicherung des Gesetzes in Informationssysteme unnötig erschweren würde.

2. Rechtspolitischer Grundgedanke der Beratungen war, die Persönlichkeitssphäre des Menschen auch in Anbetracht des Einsatzes moderner Informationstechnologien zu wahren und ihm Rechtsschutz gegen ungerechtfertigte Verwendung seiner Daten zu ermöglichen. Die

Anwendung der modernen Informationstechnologien soll den rechtsstaatlichen Bedingungen eines ordnungsgemäßen rechtlichen Verfahrens unterworfen werden. Dem Einsatz der modernen Informationstechnologien soll rechtlich ein Gegengewicht in Form des Datenschutzes gegeben werden. Ein wesentliches Bemühen war es dabei, einen Ausgleich zwischen den schutzwürdigen Interessen des einzelnen an einem wirksamen Datenschutz und den legitimen Interessen an der Informationsbeschaffung und Datenverarbeitung herbeizuführen.

3. In diesem Sinn enthält der Gesetzentwurf ein neues Grundrecht auf Schutz der Privatsphäre, das die in Art. 8 der Europäischen Menschenrechtskonvention enthaltenen Grundsätze fortführt und erweitert in Richtung auf ein grundsätzliches Informationsrecht des Betroffenen über seine verarbeiteten Daten. In welcher Weise dieses neue Grundrecht jedoch auf das Medienrecht einwirkt, wurde bei der Beratung des Datenschutzgesetzes bewußt nicht entschieden. Eine endgültige Gestaltung der gegenseitigen Beziehungen von Datenschutzrecht und Medienrecht soll erst vom Gesetzgeber anlässlich der Beschlußfassung des in einem Unterausschuß des Justizausschusses derzeit in Beratung befindlichen Medienrechtes erfolgen.

4. Da der Schutz der Privatsphäre ein Grundrecht bilden soll, wird er prinzipiell unabhängig davon auszugestalten sein, ob die Verarbeitung der personenbezogenen Daten in Behörden oder sonstigen Einrichtungen des Bundes, der Länder, der Gemeinden oder anderer Selbstverwaltungskörper erfolgt; die Gefährdung der Privatsphäre ist nicht danach zu bemessen, in welcher sich aus anderen Kriterien ableitenden Behördenorganisation Daten verarbeitet werden (z. B. Verarbeitung von Daten für die mittelbare Bundesverwaltung und für die Landesverwaltung im Amt der Landesregierung). Daher wird für die Gesetzgebung betreffend den Schutz automationsunterstützt verarbeiteter personenbezogener Daten eine einheitliche Bundeskompetenz vorgesehen. Dadurch soll die Zuständigkeit der Länder zur Regelung der Erhebung und Verarbeitung von Daten nicht geschmälert werden; die Kompetenz des Bundes hat lediglich den Schutz dieser Daten zum Inhalt.

Für die Vollziehung wiederum wäre es weder mit den Grundsätzen einer möglichst sparsamen Verwaltung, noch mit der für den Betroffenen uneinsichtigen Unterscheidung, ob dasselbe Datum für Zwecke der einen oder der anderen Gebietskörperschaft verwendet wird, vereinbar, Landesbehörden neben Bundesbehörden mit der Vollziehung zu betrauen. Die Vereinheitlichung des Rechtsschutzes, die Verminderung des Kostenaufwandes und die

Verhinderung der Aufblähung des Rechtsschutzapparates läßt es ratsam erscheinen, den eigentlichen Datenschutz einer zentralen Bundesbehörde anzuvertrauen. Die Datenschutzkommission berücksichtigt die Interessen der Länder insofern, als auch die Länder des kooperativen Föderalismus die Zuständigkeit erhalten sollen, Mitglieder ihrer Wahl in die Datenschutzkommission zu entsenden. Eine Unterstreichung föderalistischer Zielsetzungen ist es auch, daß die ursprünglich vorgesehene Kompetenz des Bundes auch für den Landesbereich in Datenschutzangelegenheiten, Durchführungsvorordnungen zu erlassen, gestrichen wurde (Regierungsvorlage § 1 letzter Satz). Bei der organisatorischen Zuordnung dieser Datenschutzkommission wird darauf zu achten sein, daß es sich um eine Behörde handelt, die über verfassungsgesetzlich gewährleistete Rechte und über grundsätzliche Fragen der Behördenorganisation und des Verwaltungsrechtes zu entscheiden hat.

5. Datenschutz ist ein Problem nicht nur im öffentlichen, sondern auch im privaten Bereich. Die von der Regierungsvorlage her vorgegebenen Ansätze für eine Regelung des privaten Datenverkehrs wurden erweitert mit der Tendenz, möglichst gleiche Regelungen für den öffentlichen wie für den privaten Bereich vorzusehen.

6. Wenngleich mit dem Einsatz des Computers ohne Zweifel nicht nur eine neue Quantität, sondern auch eine neue Qualität der Informationsverarbeitung eingesetzt hat, würde ein Datenschutzgesetz, das sich auf sämtliche Techniken der Informationsverarbeitung bezieht, keine Realisierung in der Praxis ermöglichen. Auf der anderen Seite würde ein Datenschutzgesetz, das sich nur auf eine bestimmte technische Form der Verarbeitung bezieht, Gefahr laufen, rasch überholt zu sein und Umgehungsmöglichkeiten herausfordern. Der Entwurf sucht einen Mittelweg: Jegliche Form der „automationsunterstützten“ Verarbeitung personenbezogener Daten soll unter das Datenschutzgesetz fallen. Wird ein Datum auch nur in einer Phase automationsunterstützt, d. h. mit vorgegebenem Programm und maschinell verarbeitet, so fällt jede Phase der Verarbeitung unter das Gesetz (§ 3 Z. 6 in Verbindung mit Z. 10). Die nunmehr gegenüber der Regierungsvorlage im Entwurf vorgesehene Trennung der Verantwortlichkeiten zwischen einem „Verarbeiter“ und einem „Auftraggeber“ (§ 3) entspricht der häufig bei der Datenverarbeitung gegebenen Arbeitsteilung; der Schwerpunkt der Verantwortung des Verarbeiters liegt bei der Datensicherung, bei der Durchführung der Verarbeitung sowie bei der gesetzmäßigen Erfüllung der Weisungen seines Auftraggebers, wogegen der Auftragge-

ber vor allem die rechtliche Zulässigkeit der einzelnen Verarbeitungsschritte überhaupt zu verantworten hat.

7. Der Schutz der Privatsphäre ist eine Aufgabe der Gesetzgebung unserer Zeit. Mit der Erlassung eines Datenschutzgesetzes ist aber der Schutz der Privatsphäre nicht als gesichert anzusehen. Im Sinne des § 6 und des § 7 wird die Erlassung gesetzlicher Bestimmungen über die Zulässigkeit der Ermittlung, Verarbeitung, Benützung und Übermittlung personenbezogener Daten zu prüfen sein. Bei der Erlassung derartiger gesetzlicher Bestimmungen wird das verfassungsgesetzlich gewährleistete Recht des § 1 zu beachten sein. Der Entwurf beschränkt sich nicht auf Vorkehrungen für die Kontrolle der Einhaltung der Bestimmungen des Datenschutzgesetzes durch eine Behörde, sondern er sieht auch einen Datenschutzrat als politisches Beobachtungsorgan vor, das die Verwaltung, den Gesetzgeber und die Öffentlichkeit aufmerksam machen soll auf weitere Gefährdungen der Privatsphäre und auf die Notwendigkeit der Ergänzung des Rechtsschutzes.
8. Datenschutzgesetze sind gegenwärtig erlassen in Schweden, den USA, der BRD, Frankreich, Kanada, Neuseeland, Dänemark und Norwegen. Weitere werden folgen. Der Beachtung der internationalen Entwicklung kommt gerade auf diesem Gebiet eine besondere Bedeutung zu, da die Verbindung von Computern mit der Telecommunication, der Aufbau multinationaler Datennetze, eine Realität darstellen, der ein nur nationaler Gesetzgeber nicht gerecht werden könnte. Die Entstehung von „Datenoasen“, in denen nationale Datenschutzgesetze zum Schaden des Betroffenen umgangen werden können, soll verhindert werden einerseits durch die Harmonisierung der nationalen Gesetze und andererseits durch die Zusammenarbeit in internationalen Organisationen, wo gegenwärtig im Europarat eine internationale Datenschutzkonvention und in der OECD eine Richtlinie für den grenzüberschreitenden Datenverkehr vorbereitet werden. Deswegen wurde in den Entwurf ein eigener Abschnitt über den grenzüberschreitenden Datenverkehr aufgenommen.
9. Der Betroffene soll rechtliche Möglichkeiten haben, den Schutz seiner Privatsphäre gegenüber der öffentlichen und der privaten Datenverarbeitung durchzusetzen. Dazu muß er wissen, wer über ihn Daten verarbeitet. Dem dienen die Einrichtungen eines Datenverarbeitungsregisters und Informationspflichten. Weiters soll eine Behörde rasch entscheiden können, ob das Datenschutzgesetz verletzt wurde oder nicht, und zwar unabhängig von der Rechtsstellung des Verarbeiters oder des Auftraggebers. Im öffentlichen Bereich soll diese Behörde die Datenschutzkommission sein

(vor der der Verarbeiter oder Auftraggeber der Verarbeitung und der Betroffene die gleiche verfahrensrechtliche Stellung haben), im privaten Bereich das dem Betroffenen nächste Landesgericht, wobei hier dem Betroffenen eine Begünstigung der prozessualen Stellung insofern gegeben wird, als die Datenschutzkommission die Möglichkeit haben muß, unter bestimmten Voraussetzungen als Nebenintervenient im zivilrechtlichen Verfahren aufzutreten. In diesen Verfahren soll im Rahmen der Klage die Prüfung der Einhaltung der Bestimmungen des Datenschutzgesetzes sowie der Durchführungsverordnungen einschließlich der Betriebsordnungen für alle Schritte der Verarbeitung möglich sein. Eine umfassende Aufklärung über alle aus diesem Bundesgesetz erwachsenden Rechte und Verpflichtungen sollte von der Bundesregierung und anderen zuständigen Stellen erfolgen.

10. Internationale Untersuchungen haben ergeben, daß durch ein Datenschutzgesetz ein Mehraufwand von 2 bis 10% der für die Verarbeitung personalbezogene Daten aufzuwendenden ADV-Kosten erwächst. Das Datenschutzgesetz wird daher keine erheblichen Mehrkosten für Verarbeiter und Auftraggeber bringen, die sich bereits bisher an den Grundsätzen ordnungsgemäßer Datenverarbeitung orientiert und beim Umfang der Verarbeitung im Bereiche der zulässigen Unternehmungszwecke bzw. im Rahmen der gesetzlichen Ermächtigungen gearbeitet haben. Die dem einzelnen zustehenden Informations- und Berichtigungsrechte werden je nach der Anzahl der Antragstellungen unterschiedliche Kosten verursachen, doch sieht der Entwurf hier die Möglichkeit von Kostenersatz vor.

Die Vollziehung des Datenschutzgesetzes wird für die Bundesverwaltung einen Mehraufwand zunächst beim Österreichischen Statistischen Zentralamt bedingen, dem die Führung des Datenverarbeitungsregisters, sowie die damit verbundenen Auskunfterteilungen zukommen werden. Dabei wird auch mit einem personellen Mehraufwand zu rechnen sein. Wieviel an Personal der Geschäftsführung der Datenschutzkommission vom Bundeskanzler ständig zuzuweisen sein wird, ist nicht vorhersehbar, da dies zum Teil von der Inanspruchnahme der Datenschutzkommission durch Beschwerden abhängt. Für die Vorbereitung der allgemeinen Entscheidungen der Datenschutzkommission wird jedenfalls Personal notwendig sein, das juristische, wirtschaftliche und Kenntnisse der Informatik haben sollte.

Die Entscheidungen der Datenschutzkommission werden überwiegend in Anwendung des verfassungsgesetzlich gewährleisteten Rechtes auf Datenschutz ergehen müssen und

einer unmittelbaren Prüfung durch die Gerichtshöfe des öffentlichen Rechts unterliegen. Da Entscheidungen über den Schutz der Privatsphäre wegen der Gefahr des Eintrittes von nicht wieder gutzumachenden Schäden möglichst rasch ergehen sollen, sieht der Entwurf auch vor, daß bei Säumigkeit der Datenschutzkommission eine Beschwerde an den Verwaltungsgerichtshof erhoben werden kann, was gegenüber der üblichen Rechtslage bei der Behörde nach Art. 133 Z. 4 B-VG eine Fortbildung des Rechtsschutzes bedeutet.

Zu den einzelnen Bestimmungen wird bemerkt:

Zu § 1:

Ein besonderes Grundrecht war bereits im OVP-Initiativantrag 21/A und in den Erläuterungen zur Regierungsvorlage angeregt worden. Das nun im Entwurf vorgeschlagene Grundrecht sucht unter Verwendung der Begriffe des Art. 8 der Europäischen Menschenrechtskonvention einen im Grundsatz von der technischen Form der Verarbeitung unabhängigen Schutz aufzustellen. Es geht auch im Hinblick auf seine unmittelbare Durchsetzbarkeit über die Amtsverschwiegenheit gemäß Art. 20 Abs. 3 B-VG hinaus (vergleiche VfGH Erk. Slg. 7455/1975 zur mangelnden Durchsetzbarkeit der Wahrung der Amtsverschwiegenheit). Da Datenschutz in jedem Fall eine Abwägung von Interessen bedingt, wird es von der Beurteilung des Naheverhältnisses der einzelnen, konkreten Information zur Privatsphäre abhängen, ob die Garantie der Geheimhaltung gegeben ist. Der letzte Satz des Abs. 2 soll zeigen, daß im Zweifelsfall der Geheimhaltung der Vorzug zu geben ist, daß also das private Interesse gegenüber einem öffentlichen überwiegen soll. Da die Abs. 1 und 2 nicht auf die automationsunterstützte Datenverarbeitung abstellen, werden sie von über den Geltungsbereich des Datenschutzgesetzes hinausgehender Bedeutung für Gesetzgebung und Vollziehung sein.

Die Abs. 3 und 4 statuieren für automationsunterstützt verarbeitete Daten positive Rechte des Betroffenen, die allerdings der Durchführung durch einfaches Bundesgesetz bedürfen. Abs. 6 sieht als weitere Neuerung für die österreichische Rechtsordnung eine ausdrückliche Drittwirkung des Grundrechtes vor. Die Rechtsansprüche des Betroffenen nach dem 4. Abschnitt sind vor den ordentlichen Gerichten durchzusetzen; die Gerichte haben dabei das Grundrecht des § 1 anzuwenden.

Zu § 3 Z. 1:

Unter personenbezogenen Daten sind beispielsweise zu verstehen: Name, Geburtsdatum, Adresse, Geschlecht, Personenkennzeichen sowie Information über Religion, Gesundheit, Einkommen, Vermögen, Leumund, Lebensgewohnheiten, Intelligenzquotient, Umsatz, Gewinn, Beschäftigtenzahl und Bonität.

Zu § 3 Z. 8:

Unter Aufgabengebiet sind die einem Organ eines Rechtsträgers durch Gesetz zugewiesenen Aufgaben

in einer bestimmten Verwaltungsmaterie (z. B. Personalverwaltung) zu verstehen.

Zu § 4 Abs. 3:

Diese Bestimmung des Entwurfes sucht dem Problem zu begegnen, daß die Informationsverarbeitung der Sicherheitsverwaltung und der Landesverteidigung nicht in demselben Maße determinierbar und publizierbar ist wie die anderer Bereiche der staatlichen Verwaltung. Trotzdem soll das Datenschutzgesetz im Grundsatz auch auf sie Anwendung finden und eine Zuständigkeit der Datenschutzkommission gegeben sein. Vergleichbare Ausnahmeregelungen sind in allen Datenschutzgesetzen des Auslandes enthalten.

Durch § 4 Abs. 3 Z. 1 soll klargestellt werden, daß die bei den Sicherheitsbehörden zum Zwecke der Verbrechensvorbeugung und Tataufklärung automationsunterstützt verarbeiteten Daten zu diesem Ausnahmebereich gehören. Darunter fallen sowohl nationale und internationale polizeiliche Fahndungsinformationen als auch Daten, die für präventive oder repressive Zwecke vergleichende Auswertungen durch festgestellte gleichartige Arbeitsweisen bekannter und unbekannter Täter gestatten. Auch das Speichern und Auswerten von Fingerabdruckformeln, Personenbeschreibungen usw. würden unter diese Ausnahmeregelung fallen, desgleichen Erkenntnisse, die zum Zwecke der Terrorbekämpfung und der Bekämpfung internationaler Bandenkriminalität gesammelt und ausgewertet werden.

Zu § 6:

Der unbestimmte Gesetzesbegriff der „wesentlichen Voraussetzungen“ für die Vollzugsaufgaben der konkreten Behörde soll nicht bedeuten, daß nur die Anwendung der ADV die Gesetzesvollziehung ermöglichen würde; es soll auch der verwaltungswirtschaftliche Einsatz der ADV zulässig sein, wenn also die Verarbeitung auch in herkömmlicher Weise möglich, nicht aber sparsam und zweckmäßig wäre. Voraussetzung ist allerdings, daß die Daten für die Vollzugsaufgabe wesentlich sind.

Zu § 7:

Ausgehend vom Geheimhaltungsgrundsatz des § 1 werden hier Ausnahmen von dieser Geheimhaltung vorgesehen. Abs. 2 wird in Entsprechung des Art. 22 B-VG zu verstehen sein.

Zu § 7 Abs. 1 Z. 1:

Das Erfordernis der „ausdrücklichen“ schriftlichen Zustimmung des Betroffenen stellt klar, daß eine derartige Zustimmung keinesfalls dann vorliegen kann, wenn sie als Bestandteil von allgemeinen Geschäftsbedingungen vom Betroffenen zur Kenntnis genommen wurde. Vielmehr liegt eine „ausdrückliche“ schriftliche Zustimmung nur dann vor, wenn der Betroffene sein Einverständnis zur Datenübermittlung getrennt von etwaigen sonstigen vertraglichen Vereinbarungen gegeben hat.

Zu § 7 Abs. 1 Z. 5:

Wenn dem Bundesstatistikgesetz 1965, BGBl. Nr. 91, entsprechende Landesstatistikgesetze die Organisation und Geheimhaltung für die Landes- und Gemeindestatistik geregelt haben, so wird eine Ergänzung dieser Bestimmung im Hinblick auf Übermittlungsberechtigungen auch an Landesämter für Statistik und ähnliches zu erfolgen haben. Die Entwicklung der entsprechenden Landesgesetzgebung wird der Datenschutzrat zu prüfen haben.

Zu § 10 Abs. 3:

Der Ausdruck „Echtverarbeitung“ (Z. 4) soll die Abgrenzung zwischen der Planung und dem Prüfen von Programmen mit fingierten Daten einerseits und der operationellen Durchführung mit der Wirklichkeit entnommenen personenbezogenen Daten andererseits bezeichnen.

Die Dauer der Aufbewahrung der Protokolle (Z. 5) wird nach dem materiellen Recht zu bemessen sein (z. B. Verjährungsfristen); eine Protokollierungspflicht wird auch bei Serviceleistungen notwendig sein.

Zu § 13:

Die bisher wegen der mangelnden gesetzlichen Ausnahme von der Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) bedenkliche Übergabe von Daten auch nur für Zwecke der Verarbeitung an andere Rechtsträger des öffentlichen oder des privaten Rechts soll durch diese Bestimmung in dem in ihr gegebenen Rahmen zulässig werden. Hier wird Grenze nicht nur der Schutz der Privatsphäre sein, sondern auch das öffentliche Interesse, das etwa gegen eine Übermittlung von für den Staat sensiblen Datenbeständen an Dritte, insbesondere in das Ausland, spricht.

Zu § 14:

Die Datenschutzkommission soll in erster und einziger Instanz erkennen, gleichgültig, ob die bekämpfte Verarbeitung von einer Behörde oder einer anderen dem öffentlichen Bereich zugehörigen Einrichtung durchgeführt wurde. Abs. 3 folgt dem von § 38 AVG vorgegebenen Lösungsmodell für Vorfragen, verpflichtet aber gleichzeitig die für die Daten sachlich zuständige Behörde, ein Verfahren bei der Datenschutzkommission einzuleiten. Diese Regelung wird wegen der Notwendigkeit rascher und von denselben Auslegungen getragenen Entscheidungen einer auf Fragen des Datenschutzes spezialisierten Behörde als zur Regelung des Gegenstandes erforderlich angesehen (Art. 11 Abs. 2 letzter Halbsatz B-VG).

Zu § 17:

Diese Bestimmung soll die Verarbeitung personenbezogener Daten durch Private wie § 14 der

Regierungsvorlage auf den (von der Rechtsordnung anerkannten) Zweck des privaten Rechtsträgers abstellen. Wesentliches Kriterium ist also, daß ein solcher Rechtsträger die Daten im Rahmen seines Geschäftsverkehrs, im Rahmen der durch die Nichtuntersagung von Vereinsstatuten vorgegebenen Vereinstätigkeit benötigt, wobei der allgemeinen Geschäftsauffassung Bedeutung zukommen wird, die aber Grenzen an den schutzwürdigen Interessen des Betroffenen finden soll. Dabei wird durch die Hervorhebung des Privat- und Familienlebens ein innerer Kreis von Informationen vom Gesetzgeber einem bevorzugten Schutz empfohlen.

Zu § 18:

Das grundsätzliche Verbot der Übermittlung von automationsunterstützt verarbeiteten Daten soll sichern, daß Daten, die von einem Unternehmen durchaus berechtigt im Sinne des § 18 für eigene Zwecke verarbeitet werden, nicht an nicht gleichermaßen berechtigte Dritte weitergegeben werden; Informationsübermittlung soll nicht zum Nebenzweck eines Unternehmens werden. Dort, wo nicht besondere gesetzliche Verschwiegenheitspflichten bestehen (z. B. § 10 des Ärztegesetzes, BGBl. Nr. 92/1949), werden Übermittlungen unter einer der Voraussetzungen des Abs. 1 möglich sein. Die in Abs. 1 Z. 3 genannten „berechtigten Interessen“ werden entsprechend dieser Formulierung in anderen Bestimmungen solche sein müssen, die von der Rechtsordnung anerkannt sind.

Zu § 20:

Die bestehenden Verschwiegenheitspflichten für einzelne Berufe sollen um eine allgemeine Verschwiegenheitspflicht für alle Personen ergänzt werden, denen automationsunterstützt verarbeitete Daten berufsmäßig bekannt wurden. Diese Verschwiegenheitspflicht soll nicht nur den ständig bei Datenverarbeitungen oder mit Daten Befassten binden, sondern auch den, der als nicht dem Betrieb des Verarbeiters oder Auftraggebers Angehöriger Zugang zu solchen Daten erhält (z. B. Servicetechniker).

Der letzte Satz des Abs. 2 bedeutet, daß das Datengeheimnis nicht nur nach Beendigung des Arbeitsverhältnisses zu wahren ist, sondern auch bei Aufnahme einer anderen Tätigkeit im selben Unternehmen.

Zu § 21 Abs. 4:

Diese Bestimmung schließt nicht aus, daß der Verarbeiter die Möglichkeit hat, durch Datensicherungsmaßnahmen eigener Wahl ebenfalls dem Gesetz entsprechend zu verarbeiten.

Zu § 23:

Der international anerkannte Grundsatz der Möglichkeit der Kenntnisnahme des Betroffenen, wo

welche Informationen über ihn gespeichert sind (vergleiche Punkt 5 der Resolution des Ministerkomitees des Europarates 73/22 vom 20. September 1974) setzt voraus, daß es grundsätzlich keine gegenüber dem Betroffenen „geheimen“ Datenverarbeitungen gibt. Dieses Ziel suchen die ausländischen Gesetze unterschiedlich zu verwirklichen: Zum Teil durch eine Informationspflicht des Bearbeiters an dem Betroffenen (BRD), zum Teil durch die Pflicht zur Eintragung von Datenverarbeitungen in ein öffentliches Register (Frankreich, Schweden). Der vorliegende Entwurf sucht einen Mittelweg zwischen beiden Systemen: Während bei Datenverarbeitungen, die grundsätzlich nur für interne Zwecke ohne die Absicht der Übermittlung von Daten eingerichtet werden, Informationen des Betroffenen genügen (§ 23), sind andere Verarbeitungen zu registrieren. Die Registrierung ist beim Österreichischen Statistischen Zentralamt zu beantragen. Die Registrierung ist von diesem vorzunehmen, außer es hat Bedenken gegen die Rechtmäßigkeit. In diesem Fall ist der Akt der Datenschutzkommission zu übermitteln, die entweder die Registrierung bescheidmäßig abzulehnen hat (etwa, wenn sich die Unterlagen – z. B. Vereinssatzung, Gesellschaftsvertrag, Konzession – über den berechtigten Zweck des Rechtsträgers mit der beabsichtigten Verarbeitung nicht decken, wobei aber eine Frist zur Behebung eines solchen Mangels zu geben ist) oder dem Statistischen Zentralamt mitzuteilen hat, daß keine Bedenken gegen die Registrierung bestehen. Auch wenn eine Registrierung vorgenommen würde, bleibt es den Gerichten in einem späteren Verfahren unbenommen, die Rechtmäßigkeit der Datenverarbeitung im generellen oder im konkreten zu überprüfen.

Zum 5. Abschnitt:

Der Entwurf geht davon aus, daß neben den Gerichten die Datenschutzkommission und der Datenschutzrat zur Prüfung der Einhaltung der Bestimmungen des Datenschutzgesetzes berufen sein sollen. Ist die Datenschutzkommission organisatorisch eine weisungsfreie Kollegialbehörde nach Art. 133 Z. 4 B-VG, so soll der Datenschutzrat nach dem Vorbild des Landesverteidigungsrates und des Rates für Auswärtige Angelegenheiten bei auf Grund dieses Gesetzes zu treffenden rechtspolitischen Entscheidungen anzuhören sein (vergleiche § 4 Abs. 3 Z. 3); er soll auch die Auswirkungen des Gesetzes beobachten, und Vorschläge über dessen Ergänzung oder Änderung beschließen.

Die Datenschutzkommission hat aber nicht nur die Aufgabe, Bescheide auf Grund von Beschwerden einzelner zu erlassen; ihr kommen auch Befugnisse genereller Art (z. B. Zustimmung zu Betriebsordnungen) und in Verfahren vor anderen Behörden zu (z. B. § 48 Abs. 2). Da diese Zuständigkeiten der Datenschutzkommission gegenüber anderen Kollegialbehörden nach Art. 133 Z. 4 B-VG erweiterte Funktionen als weisungsfreies Organ der Vollziehung geben,

werden diese Bestimmungen als verfassungsändernd zu qualifizieren sein.

Die Bestimmungen des § 45 Abs. 1 und Abs. 2 werden als verfassungsändernd zu behandeln sein, weil sie über Art. 20 Abs. 3 und Art. 22 B-VG hinausgehen.

Zu § 37 Abs. 2:

Diese Befugnis wird einem Mandatsbescheid nach § 57 AVG gleichzuhalten sein.

Zu § 47:

Das Datenverarbeitungsregister ist öffentlich zu führen. Da seine Führung mittels automationsunterstützter Datenverarbeitung wahrscheinlich ist, sollen auch Vorkehrungen getroffen werden, um eine dezentrale Einsichtnahme (etwa in den Landeshauptstädten) zu ermöglichen. Diesbezügliche Überlegungen sollten vom Bundeskanzleramt und vom Österreichischen Statistischen Zentralamt bei Bedarf angestellt werden.

Die in Abs. 4 vorgesehene Registernummer, die für je einen Auftraggeber dieselbe ist, auch wenn er Daten zu unterschiedlichen Zwecken und auf Grund mehrerer Registrierungen verarbeitet, hat den Zweck, jedes automationsunterstützt verarbeitete Datum bei der Übermittlung mit der Information auszustatten, von welchem Auftraggeber es stammt. Es soll sichergestellt werden, daß die Herkunft der Daten feststellbar ist.

Damit soll es möglich sein, nach Antwort des Datenverarbeitungsregisters, welchem Rechtsträger diese Nummer zugeordnet ist, unmittelbar bei diesem Rechtsträger seine Rechte wahren zu können. Von Bedeutung wird die Registernummer insbesondere dort sein, wo Daten durch die Hände mehrerer Zwischenträger gehen.

Zu § 48:

Die Regierungsvorlage sah vor, daß die Ahndung von Geheimnisverletzungen in bezug auf Datenbanken des öffentlichen Bereichs (§ 27 der Regierungsvorlage) anderen Regeln unterliegen soll als in bezug auf private Datenbanken (§ 28 der Regierungsvorlage). Der Ausschuss ist jedoch der Ansicht, daß Geheimnisverletzungen von Beamten grundsätzlich nach den Vorschriften über die Verletzung des Amtsgeheimnisses nach § 310 StGB geahndet werden. Auf jenen Personenkreis, den § 27 der Regierungsvorlage außer den Beamten erfaßt, nämlich auf Grund eines Werkvertrages oder in Lohnarbeit, etwa bei der Datenerfassung, bei Servicearbeiten usw. beschäftigte Personen, sollen die Vorschriften über die Geheimnisverletzung bei privaten Datenbanken Anwendung finden. Aus diesem Grunde werden beide oben angeführten Strafbestimmungen der Regierungsvorlage zu einer Strafbestimmung zusammengezogen und im übrigen die Beschreibung des Tatbestandes

den gegenüber der Regierungsvorlage geänderten Begriffsbestimmungen angepaßt.

§ 28 der Regierungsvorlage war als Privatanklagedelikt gefaßt. Der Ausschuß vermeint, daß in Anbetracht der bei der Erforschung der Tatsachen im Bereich der ADV zu erwartenden Schwierigkeiten und dem damit auch verbundenen Kostenrisiko die Verfolgung durch den Staatsanwalt günstiger erscheint, der aber an den Antrag des in seinen Rechten auf Geheimhaltung Verletzten gebunden ist. Neben dem Verletzten soll auch die Datenschutzkommission antragsberechtigt sein.

Der Strafraum entspricht dem des § 49. Damit ist auch hier der Gerichtshof für das Strafverfahren zuständig.

Besondere, von den Vorschriften der StPO 1975 abweichende Regeln über den Ausschluß der Öffentlichkeit in der Hauptverhandlung sollen die Geheimhaltung der geheimzuhaltenden Daten im Strafverfahren sicherstellen.

Zu § 49:

Der Ausschuß ist der Ansicht, daß nicht nur das rechtswidrige Verschaffen von Daten, sondern auch rechtswidrige Angriffe auf den Bestand der Daten, sei es durch Löschen, Verfälschen oder sonstiges Verändern der Daten, strafbar sein sollen, soweit die Tathandlung in Schädigungsabsicht gesetzt wird. Eine Subsidiaritätsklausel stellt sicher, daß strengere Strafbestimmungen des sonstigen Strafrechts gegebenenfalls in Anwendung kommen können. Weiters ist die gegenständliche Strafbestimmung nun als Offizialdelikt konstruiert.

Zu § 50:

Diese Verwaltungsstrafbestimmung soll im Bereiche der Datenverarbeitung Privater die Einhaltung der Informations- und Registrierpflichten (§§ 23, 24) sichern. Die Strafe des Verfalls nach Abs. 3 soll auch die Möglichkeit des Verfalls von software einschließen, nicht aber die des Verfalls von hardware.

Zu § 51:

Diese Bestimmung soll die verwaltungsökonomische Zusammenfassung von Datenverarbeitung innerhalb eines Bundesministeriums oder einer Landesverwaltung ermöglichen und bringt damit eine Erweiterung der Zulässigkeitsvoraussetzungen des § 6, der in Verbindung mit § 3 Z. 3, zweiter Satz, ja die Zuständigkeit der konkreten Dienststelle als Voraussetzung für die automationsunterstützte Datenverarbeitung fordert. Die Führung solcher Datenverarbeitungen durch eine andere Dienststelle als den Auftraggeber im Sinne des § 6 wird allerdings nicht bedeuten, daß solche Daten von anderen Dienststellen als den gemäß § 6 berechtigten verwendet werden dürfen.

Zu § 52:

Das Datenschutzgesetz verlangt vor der Aufnahme der automationsunterstützten Verarbeitung personenbezogener Daten umfangreiche rechtliche und organisatorische Maßnahmen. Nun ist aber gerade im Bereiche der ADV vor der operationellen Durchführung einer neuen Applikation eine Versuchsphase, ein Prüfen mehrerer Alternativen notwendig und zweckmäßig. Diese Möglichkeit soll mit dieser Bestimmung geschaffen werden. Wohl müssen solche versuchsweisen Verarbeitungen dem Datenverarbeitungsregister gemeldet werden, wohl unterliegen sie dem Auskunft- und Berichtigungsrecht, doch ist für sie weder die nach den §§ 6 und 7 grundsätzlich notwendige gesetzliche Ermächtigung noch eine Datenschutzverordnung noch eine Betriebsordnung notwendig. Gerade aus den Erfahrungen während eines solchen Versuches sollen Erkenntnisse für die notwendige legislative Vorbereitung und für die operationelle Einführung einer Datenverarbeitung in ganz Österreich oder für den Bereich eines Landes gewonnen werden.

Zu § 54:

Bei dieser Bestimmung des Entwurfes geht der Ausschuß davon aus, daß bei den Beratungen über die Regierungsvorlage des Mediengesetzes (54 der Beilagen des Nationalrates XIV. GP) die Gedanken des Datenschutzes gebührende Beachtung finden werden. Das Grundrecht des § 1 soll allerdings bereits ab dem Inkrafttreten des Datenschutzgesetzes auch für Medienunternehmungen gelten.

Zu § 58:

Für das Inkrafttreten der einzelnen Bestimmungen des Entwurfes ist ein Zeitraum vom 1. Jänner 1980 bis zum 1. Juli 1981 vorgesehen. Diese relativ langen Übergangsfristen sollen es dem betroffenen Rechtsträger ermöglichen, sich mit der neuen Rechtslage vertraut zu machen und ihre Verarbeitung zeitgerecht anzupassen. Da die Notwendigkeit einer raschen Anpassung besonders von organisatorischen und technischen Vorkehrungen unverhältnismäßig hohe Kosten verursachen würde, wurden hierfür besonders lange Übergangsfristen vorgesehen. Andererseits soll auch der Anfangsaufwand beim Datenverarbeitungsregister und bei der Datenschutzkommission im Verhältnis zum später mit den Anträgen auf Registrierung verbundenen Aufwand vergleichbar bleiben, sodaß § 57 Abs. 2 für die mit Inkrafttreten des Datenschutzgesetzes zu beantragenden Registrierungen die sechswöchige Frist für die Eintragung unbeachtlich läßt, allerdings nicht zum Nachteil für die Antragsteller, die bis zur Entscheidung die Verarbeitung im gegebenen Umfang fortführen dürfen.

Am 5. Oktober 1978 hat der Verfassungsausschuß den durch Abgeordneten Dr. Veselsky erstatteten Bericht des Unterausschusses entgegengenommen und nach Wortmeldungen der Abgeordneten Dr. Ermacora, Dr. Schmidt und Ing. Hobl einstimmig beschlossen, dem Hohen Hause die Annahme des Gesetzentwurfes in der vom Unterausschuß vorgeschlagenen Fassung und unter Berücksichtigung eines gemeinsamen Abänderungsantrages der Abgeordneten Dr. Veselsky, Dr. Ermacora und Dr. Schmidt zu empfehlen.

Abänderungsanträge des Abgeordneten Dr. Schmidt, welche die in den Abs. 3 und 4 des § 1 statuierten positiven Rechte und die Kompetenzregelung des § 2 Abs. 1 nicht auf den automationsunterstützten Datenverkehr einschränken wollten, fanden nicht die entsprechende Mehrheit.

Ferner hat der Ausschuß eine EntschlieÙung betreffend eine schadensrechtliche Regelung angenommen.

Hiezu stellt der Ausschuß fest:

Angesichts der Tatsache, daß das Datenschutzgesetz viereinhalb Jahre lang während zweier Legislaturperioden beraten wurde, erschien es nicht zweckmäßig, eine Beschlußfassung über dieses Bundesgesetz durch weitere Beratungen über besondere schadenersatzrechtliche Bestimmungen noch

weiter zu verzögern. Solange solche besonderen Bestimmungen über das Schadenersatzrecht im Datenverkehr nicht getroffen sind, müssen daher die allgemeinen Bestimmungen des privatrechtlichen Schadenersatzrechtes und des Amtshaftungsrechtes Anwendung finden. Auf Grund der, in dem zur Beratung des Datenschutzgesetzes eingesetzten Unterausschusses geführten, grundsätzlichen Debatten über ein besonderes Schadenersatzrecht im Bereich des Datenschutzes gelangte der Verfassungsausschuß zur Auffassung, daß bei einer schadenersatzrechtlichen Regelung für den gegenständlichen Rechtsbereich eine Vereinfachung der Haftung, eine eingeschränkte Erfolgshaftung sowie ein Ersatz auch immaterieller Schäden angestrebt werden sollten. Die Bundesregierung wird daher mit dem, dem Ausschußbericht beigedruckten EntschlieÙungsantrag ersucht, dem Nationalrat baldmöglichst eine entsprechende Regierungsvorlage vorzulegen.

Der Verfassungsausschuß stellt somit den Antrag, der Nationalrat wolle

1. dem angeschlossenen Gesetzentwurf die verfassungsmäßige Zustimmung erteilen, /1
2. die beigedruckte EntschlieÙung annehmen. /2

Wien, 1978 10 05

Mondl
Berichterstatte

Thalhammer
Obmann

/1

Bundesgesetz vom XXXX über den Schutz personenbezogener Daten (Daten- schutzgesetz – DSGVO)

Der Nationalrat hat beschlossen:

Artikel 1

(Verfassungsbestimmung)

GRUNDRECHT AUF DATENSCHUTZ

§ 1. (1) Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf Achtung seines Privat- und Familienlebens, hat.

(2) Beschränkungen des Rechtes nach Abs. 1 sind nur zur Wahrung berechtigter Interessen eines anderen oder auf Grund von Gesetzen zulässig, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (BGBl. Nr. 210/1958) genannten Gründen notwendig sind. Auch im Falle solcher Beschränkungen muß der vertraulichen Behandlung personenbezogener Daten Vorrang gegeben werden.

(3) Jedermann hat, soweit Daten über ihn automationsunterstützt verarbeitet werden, nach Maßgabe gesetzlicher Bestimmungen das Recht auf Auskunft darüber, wer Daten über ihn ermittelt oder verarbeitet, woher die Daten stammen, welcher Art und welchen Inhaltes die Daten sind und wozu sie verwendet werden.

(4) Jedermann hat, soweit Daten über ihn automationsunterstützt verarbeitet werden, nach Maßgabe gesetzlicher Bestimmungen das Recht auf Richtigstellung unrichtiger und das Recht auf Löschung unzulässigerweise ermittelter oder verarbeiteter Daten.

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

(6) Soweit Rechtsträger in Formen des Privatrechts tätig sind, ist das Grundrecht auf Datenschutz im ordentlichen Rechtsweg geltend zu machen.

ZUSTÄNDIGKEIT ZUR GESETZGEBUNG UND VOLLZIEHUNG

§ 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, ermittelt, verarbeitet oder übermittelt werden, sind diese Bundesgesetze von den Ländern zu vollziehen, soweit nicht durch Bundesgesetz die Datenschutzkommission, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden.

Artikel 2

1. Abschnitt

ALLGEMEINE BESTIMMUNGEN

§ 3. Im Sinne dieses Bundesgesetzes bedeuten:

1. Daten: auf einem Datenträger gespeicherte Angaben, die Informationen über eine bestimmte oder mit Wahrscheinlichkeit bestimmbare natürliche oder juristische Person oder handelsrechtliche Personengesellschaft darstellen (personenbezogene Daten);
2. Betroffene: natürliche oder juristische Personen oder handelsrechtliche Personengesellschaften, über die Daten ermittelt, verarbeitet oder übermittelt werden;
3. Auftraggeber: der Rechtsträger, der die Ermittlung, Verarbeitung oder Übermittlung von Daten veranlaßt oder selbst durchführt. Im öffentlichen Bereich (2. Abschnitt) ist darunter das örtlich und sachlich zuständige Organ eines Rechtsträgers zu verstehen;
4. Verarbeiter: die Einrichtung, die Daten verarbeitet;
5. Ermitteln von Daten (Ermittlung): das Erheben oder sonstige Beschaffen von Daten ohne Rücksicht auf die dabei angewendeten Verfahren;
6. Verarbeiten von Daten (Verarbeitung): das Erfassen, Speichern, Ordnen, Verändern, Verknüpfen, Vervielfältigen, Ausgeben oder Löschen von Daten im oder für den automationsunterstützten Datenverkehr;
7. Benützen von Daten (Benützung): das Verwenden von Daten durch den Auftraggeber der Verarbeitung;
8. Übermitteln von Daten (Übermittlung): das Weitergeben, Übertragen, Bekanntgeben, Veröffentlichung oder sonstige Offenbaren von

verarbeiteten Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder den Verarbeiter. Einer Übermittlung ist gleichzuhalten das Verknüpfen von für ein Aufgabengebiet ermittelten oder verarbeiteten Daten mit solchen Daten eines anderen Aufgabengebietes;

9. Löschen von Daten (Löschen): das Unkenntlichmachen von erfaßten oder gespeicherten Daten ohne die Möglichkeit ihrer Rekonstruktion;
10. Datenverkehr: das Ermitteln, Verarbeiten, Benützen und Übermitteln von Daten oder einer dieser Vorgänge.

§ 4. (1) Die Bestimmungen des 2. Abschnittes sind auf den Datenverkehr von oder im Auftrag von Rechtsträgern anzuwenden, die durch Gesetz eingerichtet sind, soweit es sich nicht um Rechtsträger nach § 5 handelt.

(2) Durch Verordnung der Bundesregierung sind nach Anhörung des Datenschutzrates Rechtsträger im Sinne des Abs. 1, soweit sie in Formen des Privatrechts tätig sind, für diese Tätigkeitsbereiche von der Anwendung des 2. Abschnittes auszunehmen. Für diese Bereiche findet der 3. Abschnitt Anwendung. Verordnungen nach dem ersten Satz bedürfen der Zustimmung des Hauptausschusses des Nationalrates.

(3) Die §§ 8, 9, 11 und 12 finden keine Anwendung auf die Verarbeitung von Daten, soweit diese notwendig ist:

1. für Zwecke des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich und für Zwecke der Strafrechtspflege, oder
2. für Zwecke der Sicherung der Einsatzbereitschaft des Bundesheeres, oder
3. für Zwecke der umfassenden Landesverteidigung. Diese Ausnahme bedarf einer von der Bundesregierung nach Anhörung des Datenschutzrates im Einvernehmen mit dem Hauptausschuß des Nationalrates zu erlassenden Verordnung. In dieser Verordnung sind die Ausnahmen wie Arten der Daten, Elemente der Verarbeitung, im einzelnen zu bestimmen.

§ 5. (1) Auf die Verarbeitung von Daten von oder im Auftrage von Ländern oder von Rechtsträgern, die durch Gesetze eingerichtet sind, und deren Einrichtung hinsichtlich der Vollziehung in die Zuständigkeit der Länder fällt, sowie von oder im Auftrage von Gemeinden oder Gemeindeverbänden sind die Bestimmungen des 2. Abschnittes mit der Maßgabe anzuwenden, daß die Datenschutzverordnung (§ 9) und die Höhe der Verwaltungsabgabe für die Erteilung einer Auskunft (§ 11 Abs. 3) durch die Landesregierung festzulegen sind.

(2) In einer nach Anhörung des Datenschutzrates zu erlassenden Verordnung der Landesregierung sind Rechtsträger im Sinne des Abs. 1, soweit sie in Formen des Privatrechts tätig sind, für diese Tätigkeitsbereiche von der Anwendung des 2. Abschnittes auszunehmen. Für diese Bereiche findet der 3. Abschnitt Anwendung.

2. Abschnitt

ÖFFENTLICHER BEREICH

ZULÄSSIGKEIT DER ERMITTLUNG UND VERARBEITUNG

§ 6. Daten dürfen zum Zwecke des automationsunterstützten Datenverkehrs nur ermittelt und verarbeitet werden, wenn dafür eine ausdrückliche gesetzliche Ermächtigung besteht, oder soweit dies für den Auftraggeber zur Wahrnehmung der ihm gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung bildet.

ZULÄSSIGKEIT DER ÜBERMITTLUNG

§ 7. (1) Verarbeitete Daten dürfen nur übermittelt werden, soweit

1. eine ausdrückliche gesetzliche Ermächtigung hierfür besteht, oder
2. der Betroffene der Übermittlung ausdrücklich schriftlich zugestimmt hat, wobei ein schriftlicher Widerruf möglich ist, oder
3. durch geeignete Maßnahmen sichergestellt ist, daß der Betroffene nicht bestimmbar ist, oder
4. mit der Auszahlung von Geldleistungen zusammenhängende Daten an eine Kreditunternehmung übermittelt werden, oder
5. sie ausschließlich zu statistischen Zwecken an das Österreichische Statistische Zentralamt übermittelt und dort anonymisiert verarbeitet werden.

(2) Eine Übermittlung von Daten an Organe des Bundes, der Länder, der Gemeinden, einschließlich der Körperschaften des öffentlichen Rechts ist weiters insoweit zulässig, als die Daten für den Empfänger zur Wahrnehmung der ihm gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung bilden.

MELDUNG DER VERARBEITUNG

§ 8. (1) Jeder Auftraggeber hat vor der Aufnahme einer Echtverarbeitung von Daten dem Datenverarbeitungsregister (§ 47) eine schriftliche Meldung gemäß Abs. 2 zu erstatten.

(2) In der Meldung sind die Rechtsgrundlage, der Zweck der Ermittlung, der Verarbeitung und der Übermittlung der Daten, die Art der Daten und der Kreis der Betroffenen anzugeben.

DATENSCHUTZVERORDNUNG

§ 9. (1) Die obersten Organe des Bundes und der Länder haben, unbeschadet der Bestimmungen des Abs. 2, für jeden ihrer Aufsicht unterstehenden Auftraggeber nach Anhörung der Datenschutzkommission eine Datenschutzverordnung zu erlassen, in der je nach Art der zu verarbeitenden Daten die Grundsätze für deren Ermittlung, Verarbeitung, Benützung und Übermittlung bei möglichstem Schutz der personenbezogenen Daten festzulegen sind.

(2) Selbstverwaltungskörper sind, soweit sie Daten verarbeiten, zur Erlassung einer Datenschutzverordnung nach Abs. 1 verpflichtet. Die Verordnung bedarf aufsichtsbehördlicher Genehmigung. Die Aufsichtsbehörde hat die Datenschutzkommission anzuhören. Die Genehmigung ist zu erteilen, wenn die Verordnung gesetzlichen Bestimmungen entspricht.

BETRIEBSORDNUNG

§ 10. (1) Für jeden Verarbeiter ist von dem für die Durchführung der Verarbeitung zuständigen Organ eine Betriebsordnung zu erlassen, die der Zustimmung der Datenschutzkommission bedarf. Diese Zustimmung ist, gegebenenfalls mit Auflagen oder Bedingungen, zu erteilen, wenn die Betriebsordnung gesetzlichen Bestimmungen und den auf Grund dieses Bundesgesetzes erlassenen Verordnungen entspricht.

(2) In dieser Betriebsordnung sind unter Bedachtnahme auf die wirtschaftliche Vertretbarkeit und auf die technischen Möglichkeiten jene Maßnahmen organisatorischer, personeller, technischer und baulicher Art festzulegen, die je nach der Art der Daten und der technischen Durchführung sowie des Umfangs der Verarbeitung und Übermittlung notwendig sind, um sicherzustellen, daß die Verarbeitung ordnungsgemäß erfolgt, und daß die Daten Dritten rechtswidrig weder zur Kenntnis gelangen noch übermittelt noch durch dazu nicht berechnete Personen eingesehen, verarbeitet oder übermittelt werden können.

(3) Die Betriebsordnung hat insbesondere Bestimmungen zu enthalten über:

1. den Zutritt zu den Räumlichkeiten, in denen Daten verarbeitet werden, und zu den Datenträgern,
2. die technischen und baulichen Sicherheitsvorkehrungen zur Verhinderung einer unbefugten, fahrlässigen oder zufälligen Verarbeitung oder Übermittlung von Programmen und Daten,
3. Maschinen- und Programmtests mit Daten,
4. die Genehmigung von Programmen und Programmänderungen vor der Aufnahme der Echtverarbeitung von Daten,
5. die Protokollierung von Übermittlungen und die Dauer der Aufbewahrung der Protokolle,
6. die zur Verarbeitung und Übermittlung berechtigten Personengruppen und deren Verpflichtung zur Geheimhaltung der ihnen im Zusammenhang mit der Verarbeitung bekanntgewordenen Tatsachen und Informationen sowie
7. die Dauer der Speicherung von Daten.

(4) Sollen Daten unter Voraussetzung des § 7 Abs. 1 Z. 3 übermittelt werden, so hat die Betriebsordnung Bestimmungen über die Sicherstellung der Anonymisierung der Daten zu enthalten.

(5) Weiters ist in der Betriebsordnung unter Bedachtnahme auf § 7 die Übermittlung in einer Weise zu regeln, daß dadurch die Rechte der Betroffenen an der Geheimhaltung ihrer Daten gewährleistet werden.

(6) Die Betriebsordnung ist dem Stand der jeweiligen technischen Entwicklung anzupassen, sofern es die im Abs. 2 und Abs. 5 genannten Zwecke erfordern.

AUSKUNFTSRECHT

§ 11. (1) Dem Betroffenen sind bei Nachweis seiner Identität auf schriftlichen Antrag beim Auftraggeber seine Daten in allgemein verständlicher Form sowie deren Herkunft und die Rechtsgrundlage für deren Ermittlung, Verarbeitung, Benützung und Übermittlung binnen vier Wochen schriftlich mitzuteilen, soweit es sich dabei nicht um solche Daten handelt, die auf Grund eines Gesetzes oder einer Verordnung bei überwiegendem öffentlichem Interesse auch ihm gegenüber geheimzuhalten sind. Werden oder wurden Daten übermittelt, kann der Betroffene auch Auskunft über den Empfänger verlangen.

(2) Wird einem Antrag nach Abs. 1 nicht oder nicht vollinhaltlich stattgegeben, so ist dies dem Betroffenen binnen vier Wochen unter Angabe des Grundes schriftlich mitzuteilen.

(3) Für die Erteilung einer Auskunft kann in der Datenschutzverordnung nach Anhörung des Datenschutzrates ein pauschalierter Kostenersatz vorgeschrieben werden. Die Festsetzung der Höhe dieses Kostenersatzes ist derart vorzunehmen, daß die notwendigen aus der Verarbeitung des Auskunftsantrages tatsächlich erwachsenden Kosten gedeckt sind. Von der Bearbeitung des Auskunftsersuchens kann abgesehen werden, wenn der festgesetzte Kostenersatz nicht entrichtet wurde.

PFLICHT ZUR RICHTIGSTELLUNG ODER LÖSCHUNG

§ 12. (1) Jeder Auftraggeber hat unrichtige oder entgegen den Bestimmungen des § 6 ermittelte oder verarbeitete Daten unverzüglich, längstens jedoch binnen zwei Wochen nach Feststellung des der Verarbeitung zugrunde zu legenden Sachverhaltes richtigzustellen, zu löschen oder die Richtigstellung oder Löschung zu veranlassen.

(2) Eine Richtigstellung oder Löschung nach Abs. 1 ist durchzuführen oder zu veranlassen

1. von Amts wegen, oder
2. auf begründeten Antrag des Betroffenen, oder
3. auf Grund einer Entscheidung der für die Feststellung der Daten sachlich zuständigen Behörde, oder
4. auf Grund einer Entscheidung der Datenschutzkommission, oder
5. auf Grund einer Entscheidung des Verwaltungsgerichtshofes.

(3) Erfolgt binnen zwölf Wochen nach dem Einlangen eines Antrages des Betroffenen nicht die Feststellung des der Verarbeitung zugrunde zu legenden Sachverhaltes, so ist dies dem Antragsteller unter Angabe des Grundes unverzüglich schriftlich mitzuteilen.

(4) Wird ein Antrag des Betroffenen (Abs. 2 Z. 2) abgelehnt, so ist ihm dies schriftlich binnen vier Wochen unter Angabe des Grundes mitzuteilen.

(5) Der Beweis der Richtigkeit der Daten obliegt dem Auftraggeber, soweit die Daten nicht ausschließlich auf Grund von Angaben des Betroffenen ermittelt wurden.

(6) Ist die Richtigstellung oder Löschung auf Antrag des Betroffenen oder auf Grund einer Entscheidung der Datenschutzkommission durchgeführt worden, so ist hievon der Betroffene, im Falle einer Richtigstellung oder Löschung auf Grund einer Entscheidung der Datenschutzkommission auch diese, vom Auftraggeber zu verständigen.

(7) 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 zu verständigen, sofern der Betroffene es verlangt, ein berechtigtes Interesse glaubhaft macht und die Empfänger noch feststellbar sind.

(8) Eine Richtigstellung und eine Löschung sind ausgeschlossen, wenn die Daten im Zeitpunkt ihrer Ermittlung richtig und vollständig waren und der Zweck der Ermittlung oder der Verarbeitung eine Veränderung der Daten in Entsprechung von Änderungen des ihnen zugrunde liegenden Sachverhaltes ausschließt.

(9) Erfolgt eine Richtigstellung oder Löschung auf Grund einer Entscheidung der für die Feststellung der Daten sachlich zuständigen Behörde, so ist der Auftraggeber an diese Entscheidung gebunden.

(10) Bei der Übermittlung und Benützung von Daten, deren Richtigkeit vom Betroffenen bestritten wurde, und bei denen sich weder die Richtigkeit noch die Unrichtigkeit feststellen ließ, ist über Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. Der Auftraggeber kann bei der Datenschutzkommission die Feststellung beantragen, ob der Bestreitungsvermerk aufrechtzubleiben hat.

VERTRAGLICHE INANSPRUCHNAHME VON DIENSTLEISTUNGEN IM DATENVER- KEHR DURCH DIE IN § 4 UND IN § 5 GENANNTEN RECHTSTRÄGER

§ 13. (1) Soweit Auftraggeber nach § 6 zur Ermittlung und Verarbeitung berechtigt sind, dürfen sie andere Verarbeiter desselben Rechtsträgers oder andere Rechtsträger für Dienstleistungen im Datenverkehr in Anspruch nehmen. Eine solche Inanspruchnahme darf nur erfolgen, soweit dies aus Gründen der Zweckmäßigkeit und Wirtschaftlichkeit der Verwaltung geboten ist und wenn weder schutzwürdige Interessen von Betroffenen noch öffentliche Interessen entgegenstehen.

(2) Im Falle der Inanspruchnahme nach Abs. 1 haben die in § 4 und in § 5 genannten Rechtsträger, soweit die Inanspruchnahme nicht auf Grund einer gesetzlichen Bestimmung erfolgt, vertraglich sicherzustellen, daß bei der Verarbeitung die gesetzlichen

Bestimmungen und die Bestimmungen der auf Grund dieses Bundesgesetzes erlassenen Verordnungen eingehalten werden. In solchen Verträgen ist insbesondere eine den Bestimmungen des § 10 entsprechende Betriebsordnung zu vereinbaren.

(3) Vor dem Abschluß eines Vertrages im Sinne des Abs. 2 durch einen in § 4 genannten Rechtsträger sind die Datenschutzkommission und – ausgenommen im Anwendungsbereich des § 9 Abs. 2 – das Bundeskanzleramt anzuhören; Inanspruchnahmen durch in § 5 und in § 9 Abs. 2 genannte Rechtsträger sind der Datenschutzkommission mitzuteilen.

RECHTSSCHUTZ DES BETROFFENEN

§ 14. (1) Die Datenschutzkommission (§ 36) erkennt, soweit nicht der Antrag des Betroffenen auf Auskunft (§ 11), Richtigstellung oder Löschung (§ 12) bereits Gegenstand eines Verfahrens vor der sachlich zuständigen Behörde ist, über Beschwerden wegen Verletzung von Bestimmungen dieses Bundesgesetzes oder der auf Grund dieses Bundesgesetzes erlassenen Durchführungsbestimmungen, soweit der Beschwerdeführer behauptet, dadurch in seinen Rechten verletzt worden zu sein, sowie über Anträge gemäß Abs. 3.

(2) Erfolgte eine Richtigstellung oder Löschung auf Grund einer Entscheidung der für die Feststellung der Daten sachlich zuständigen Behörde, so ist die Datenschutzkommission an die rechtskräftige Entscheidung gebunden.

(3) Wird in einem Verwaltungsverfahren, in dem verarbeitete Daten benützt werden, die Verletzung von Bestimmungen dieses Bundesgesetzes oder der auf Grund dieses Bundesgesetzes erlassenen Durchführungsbestimmungen behauptet, so ist das Verwaltungsverfahren, außer bei Gefahr im Verzug, bis zur Entscheidung der Datenschutzkommission auszusetzen (§ 38 AVG 1950). Gleichzeitig ist ein solches Verfahren zu beantragen.

AMTSWEGIGE VERFAHREN

§ 15. (1) Ergibt ein Verfahren nach § 14, daß auch andere Personen in ihren Rechten nach den Bestimmungen dieses Bundesgesetzes oder der auf Grund dieses Bundesgesetzes erlassenen Durchführungsbestimmungen verletzt wurden, so hat dies die Datenschutzkommission bescheidmäßig auszusprechen und dem Auftraggeber und dem Verarbeiter mitzuteilen. Dieser Bescheid ist von der Datenschutzkommission im Amtsblatt zur Wiener Zeitung kundzumachen.

(2) Der Auftraggeber oder der Verarbeiter haben dem Bescheid der Datenschutzkommission binnen einer von dieser festzusetzenden, angemessenen Frist zu entsprechen.

VERBINDUNG EINGELEITETER VERFAHREN

§ 16. Wenn die Zweckmäßigkeit, Raschheit, Einfachheit und Kostenersparnis von Verfahren es erfordern, hat die Datenschutzkommission eingeleitete Verfahren, die denselben Auftraggeber oder Verarbeiter betreffen, zu verbinden.

3. Abschnitt

PRIVATER BEREICH

ZULÄSSIGKEIT DER ERMITTLUNG UND VERARBEITUNG

§ 17. Daten dürfen zum Zwecke des automationsunterstützten Datenverkehrs durch einen nicht den Bestimmungen der §§ 4 und 5 unterliegenden Rechtsträger nur ermittelt und verarbeitet werden, soweit sich dies in Art und Umfang auf den berechtigten Zweck des Rechtsträgers beschränkt und hiebei schutzwürdige Interessen des Betroffenen, insbesondere im Hinblick auf Achtung seines Privat- und Familienlebens, beachtet werden.

ZULÄSSIGKEIT DER ÜBERMITTLUNG

§ 18. (1) Die Übermittlung von Daten durch nicht den Bestimmungen der §§ 4 und 5 unterliegende Rechtsträger ist unter Beachtung der im § 17 genannten Bedingungen nur zulässig, soweit:

1. der Betroffene der Übermittlung ausdrücklich schriftlich zugestimmt hat, wobei ein schriftlicher Widerruf dieser Zustimmung möglich ist, oder
2. die Übermittlung von Daten zum berechtigten Zweck des Rechtsträgers gehört, oder
3. die Übermittlung zur Wahrung überwiegender berechtigter Interessen eines Dritten notwendig ist, oder
4. durch geeignete Maßnahmen sichergestellt ist, daß der Betroffene für den Empfänger der Daten nicht mehr bestimmbar ist.

(2) Abs. 1 findet keine Anwendung, soweit gesetzliche Verpflichtungen zur Übermittlung bestehen.

(3) Bestehende Verschwiegenheitspflichten werden durch die Zulässigkeit der Übermittlung gemäß Abs. 1 nicht berührt.

DIENSTLEISTUNG IM DATENVERKEHR

§ 19. (1) Werden Daten zum Zwecke einer Dienstleistung einem anderen als dem gemäß § 17 berechtigten Rechtsträger überlassen, so hat der Verarbeiter die Daten und etwaige Ergebnisse der Verarbeitung ausschließlich dem Auftraggeber zurückzugeben oder nach dessen Auftrag zu übermitteln. Bei der Auftragserteilung sind die einzuhaltenden Verschwiegenheitspflichten und die besonderen Sorgfaltspflichten festzulegen.

(2) Gesetzliche oder vertragliche Verschwiegenheitspflichten, die der Auftraggeber zu beachten hat, sind auch vom Verarbeiter und seinen beschäftigten Personen einzuhalten. Diese Personen sind vor Aufnahme ihrer Tätigkeit zur Einhaltung der Verschwiegenheitspflichten ausdrücklich zu verpflichten.

DATENGEHEIMNIS

§ 20. (1) Automationsunterstützt verarbeitete Daten, die ausschließlich auf Grund einer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, dürfen unbeschadet sonstiger Verschwiegenheitspflichten nur auf Grund einer ausdrücklichen Anordnung des Auftrag- oder Arbeitgebers oder deren Beauftragten übermittelt werden (Datengeheimnis).

(2) Personen, denen berufsmäßig Daten anvertraut sind oder zugänglich gemacht werden, sind vor Aufnahme ihrer Tätigkeit zur Einhaltung des Datengeheimnisses ausdrücklich zu verpflichten. Die Pflicht zur Wahrung des Datengeheimnisses besteht auch nach Beendigung ihrer Tätigkeit.

(3) Weiterreichende gesetzliche Verschwiegenheitspflichten bleiben unberührt.

(4) Aus der Verweigerung der Ausführung eines Auftrages, der gegen das Datengeheimnis verstoßen würde, darf dem Arbeitnehmer kein Nachteil erwachsen.

(5) In einem behördlichen Verfahren nach diesem Bundesgesetz kann sich niemand seiner Zeugenpflichten unter Berufung auf das Datengeheimnis entziehen.

DATENSICHERUNG

§ 21. (1) Der Verarbeiter hat für den Datenverkehr unter Bedachtnahme auf die wirtschaftliche Vertretbarkeit und auf die technischen Möglichkeiten organisatorische, personelle, technische und bauliche Sicherungsmaßnahmen zu treffen. Diese Maßnahmen sollen je nach Art der Daten und der technischen Ausstattung sowie des Umfangs der Verarbeitung und Übermittlung sicherzustellen, daß Daten Dritten rechtswidrig weder zur Kenntnis gelangen, noch übermittelt, noch durch nicht berechnete Personen eingesehen, verarbeitet oder übermittelt werden können.

(2) Im Falle einer Dienstleistung nach § 19 hat der Verarbeiter von sich aus jene notwendigen Datensicherungsmaßnahmen (Abs. 1) zu treffen, die eine Durchführung des Auftrages entsprechend den ihm obliegenden gesetzlichen Verschwiegenheits- und besonderen Sorgfaltspflichten (§ 19 Abs. 1, letzter Satz) sicherstellen.

(3) Durch Verordnung des Bundeskanzlers können nach Anhörung des Datenschutzzrates ÖNORMEN über das Mindestausmaß von Datensicherungsmaßnahmen nach den Abs. 1 oder 2, die unter sinngemäßer Anwendung des § 10 festgelegt wurden, für bestimmte Arten von Daten, für bestimmte

Methoden der Verarbeitung oder Übermittlung oder für bestimmte Arten von Rechtsträgern für verbindlich erklärt werden.

(4) Die Verpflichtungen nach Abs. 1 oder 2 gelten als erfüllt, wenn der Verarbeiter die nach Abs. 3 für solche Verarbeitungen oder Übermittlungen verbindlich erklärten ÖNORMEN eingehalten hat.

VERARBEITUNG FÜR EIGENE ZWECKE

§ 22. (1) Werden Daten von Personen verarbeitet, die mit dem Auftraggeber dieser Verarbeitung in einem Vertragsverhältnis stehen oder gestanden sind, so sind die Betroffenen bei der Aufnahme der Verarbeitung der Daten aus solchen Rechtsverhältnissen für eigene Zwecke darüber ausdrücklich deutlich lesbar zu informieren; dasselbe gilt für Vereine hinsichtlich der Daten ihrer Mitglieder.

(2) Diese Information hat außerdem folgende Angaben zu enthalten:

1. Name und Adresse des Auftraggebers, und
2. die Art der Daten, und
3. den Zweck der Verarbeitung, und
4. daß Übermittlungen nur zulässig sind bei gesetzlichen Verpflichtungen, für den Geld- und Zahlungsverkehr sowie – nach besonderer Zustimmung des Betroffenen – im Einzelfall an genau bezeichnete Empfänger.

(3) Übermittlungen aus Verarbeitungen gemäß Abs. 1 sind nur zulässig:

1. bei gesetzlichen Pflichten, oder
2. zur Abwicklung des Geld- und Zahlungsverkehrs, oder
3. bei besonderer Zustimmung des Betroffenen im Einzelfall und an einem dem Betroffenen genau bezeichneten Empfänger.

(4) Der Bundeskanzler kann nach Anhörung des Datenschutzrates durch Verordnung bestimmte Arten von Verarbeitungsbereichen, die unter Abs. 1 fallen, einer Registrierungspflicht nach § 23 unterwerfen, wenn die Wahrung der im § 1 dieses Bundesgesetzes genannten Rechte es erforderlich erscheinen läßt. Solche Verarbeitungen unterliegen dann nicht der Informationspflicht des Abs. 1.

(5) Auftraggeber können für Verarbeitungen, die unter Abs. 1 fallen, die Registrierung nach § 23 beantragen. Mit der Registrierung entfällt die Informationspflicht nach Abs. 1.

REGISTRIERUNG VON VERARBEITUNGEN

§ 23. (1) Auftraggeber von anderen als nach § 22 zulässigen Verarbeitungen haben beim Datenverarbeitungsregister (§ 47) vor der Aufnahme der Echtverarbeitung von Daten die Registrierung zu beantragen.

(2) Der Antrag hat folgende Angaben zu enthalten:

1. Name und Anschrift des Auftraggebers;
2. die gesetzlichen Bestimmungen, behördlichen Bescheide oder sonstigen Vorschriften, aus denen sich der berechtigte Zweck des Rechtsträgers ergibt (§ 17);

3. den Zweck der Verarbeitung;

4. die Art der zu verarbeitenden Daten und den Kreis der Betroffenen;

5. ob und welcher Art und an welchen Kreis von Empfängern Übermittlungen vorgesehen sind.

(3) Jeder im Rahmen einer Dienstleistung (§ 19) tätige Verarbeiter hat – sofern er nicht über eine Gewerbeberechtigung nach § 103 Abs. 1 lit. a Z. 2 der Gewerbeordnung 1973 verfügt – beim Datenschutzregister vor der erstmaligen Übernahme von Verarbeitungen die Registrierung zu beantragen. Auf diesen Antrag sind Abs. 2 Z. 2 und 3 sinngemäß anzuwenden; weiters ist im Antrag der Kreis der Auftraggeber, für den Dienstleistungen verrichtet werden sollen, anzugeben. Eintragungen in die Gewerberegister, die sich auf Gewerbe nach § 103 Abs. 1 lit. a Z. 2 der Gewerbeordnung 1973 beziehen, sind dem Datenverarbeitungsregister mitzuteilen.

(4) Die Registrierung est binnen sechs Wochen nach Einlangen des Antrages vorzunehmen.

(5) Die Ablehnung der Registrierung hat nach Anhörung des Österreichischen Statistischen Zentralamtes durch Bescheid der Datenschutzkommission zu erfolgen, wenn

1. die beabsichtigte Verarbeitung einer behördlichen Bewilligung nach dem 4. Abschnitt bedürfte und diese nicht erteilt ist, oder
2. der Antrag unvollständig ist und dieser Mangel binnen angemessener Frist nicht behoben wird.

GEBÜHREN

§ 24. Mit dem Antrag auf Registrierung (§ 23) ist eine Gebühr zu entrichten, deren Höhe durch eine vom Bundeskanzler nach Anhörung des Datenschutzrates zu erlassende Verordnung festzulegen ist. Die Gebühren sind so festzulegen, daß der mit den Aufgaben der Registrierung verbundene Verwaltungsaufwand im Durchschnitt gedeckt wird.

AUSKUNFTSRECHT

§ 25. (1) Ein Betroffener kann bei Nachweis seiner Identität beim Auftraggeber Auskunft über die zu seiner Person gespeicherten Daten und über deren Herkunft verlangen. Wurden diese Daten übermittelt, kann der Betroffene auch Auskunft über die Empfänger verlangen. Die Auskunft ist binnen vier Wochen schriftlich in allgemein verständlicher Form zu erteilen, sofern der Betroffene nicht mit einer mündlichen Auskunft einverstanden ist. Mit Zustimmung des Betroffenen kann anstelle der schriftlichen Auskunft die Einsichtnahme und die Möglichkeit der Abschrift oder Ablichtung gegeben werden.

(2) Werden Daten nach § 19 verarbeitet, so sind in der Auskunft auch Name und Anschrift des Verarbeiters anzugeben.

(3) Für die schriftliche Auskunft kann ein Entgelt verlangt werden, das über die notwendigen aus der Verarbeitung des Auskunftsantrages tatsächlich erwachsenden Kosten nicht hinausgehen darf. Ein

etwa geleistetes Entgelt ist ungeachtet weiterer Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig ermittelt, verarbeitet oder übermittelt wurden oder wenn die Auskunft sonst zu einer Richtigstellung führte.

(4) Gesetzliche Verschwiegenheitspflichten bleiben unberührt.

(5) Eine Auskunft muß nicht erteilt werden, soweit dadurch überwiegende berechnigte Interessen des Auftraggebers oder eines Dritten gefährdet werden und dies dem Betroffenen gegenüber begründet wird.

(6) Wird dem Ersuchen um Auskunft nicht nachgekommen, so ist dies dem Betroffenen unter Angabe der Gründe binnen vier Wochen schriftlich mitzuteilen.

PFLICHT ZUR RICHTIGSTELLUNG

§ 26. (1) Daten sind über begründetes Ansuchen des Betroffenen richtigzustellen, wenn sie unrichtig oder unvollständig sind. § 12 Abs. 3, 5, 7 und 8 sind sinngemäß anzuwenden.

(2) Bei der Übermittlung und Benützung von Daten, deren Richtigkeit vom Betroffenen bestritten wurde, und bei denen keine Einigung über ihre Richtigkeit oder Unrichtigkeit erzielt werden konnte, ist über Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. Dieser Vermerk darf ohne Zustimmung des Betroffenen nur auf Grund eines rechtskräftigen Urteils gelöscht werden. Ist das Richtigstellungsbegehren (Abs. 1) gerichtlich geltend gemacht, die Klage aber abgewiesen worden, so ist über Verlangen des Auftraggebers im Urteil die Löschung des Vermerks anzuordnen. Der Auftraggeber kann auch unter Nachweis der Richtigkeit der Daten (§ 12 Abs. 5) den Anspruch auf Löschung des Bestreitungsvermerkes gerichtlich geltend machen.

PFLICHT ZUR LÖSCHUNG

§ 27. Daten sind zu löschen, wenn

1. ihre Erfassung oder Speicherung rechtswidrig ist, oder
2. auf Antrag des Betroffenen, wenn ihre Erfassung oder Speicherung für die Erfüllung der Zwecke der Verarbeitung nicht mehr erforderlich ist und dem nicht überwiegende berechnigte Interessen des Auftraggebers, eines Dritten oder gesetzliche Aufbewahrungspflichten entgegenstehen.

ZIVILRECHTLICHE HAFTUNG

§ 28. (1) Ansprüche gegen nicht den Bestimmungen der §§ 4 und 5 unterliegende Rechtsträger, wie sie sich aus diesem Abschnitt dieses Bundesgesetzes ergeben, sind auf dem ordentlichen Rechtsweg geltend zu machen.

(2) Sind Daten entgegen den Bestimmungen dieses Bundesgesetzes oder den auf Grund dieses Bundesgesetzes erlassenen Durchführungsbestimmungen ver-

arbeitet, benützt oder übermittelt worden, so hat der Betroffene, unbeschadet etwaiger Ansprüche auf Schadenersatz, Anspruch auf Unterlassung und Beseitigung des diesem Bundesgesetz oder den auf Grund dieses Bundesgesetzes erlassenen Durchführungsbestimmungen widerstreitenden Zustandes.

ZIVILGERICHTLICHES VERFAHREN

§ 29. (1) Für Klagen nach diesem Bundesgesetz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht des Landes, in dem der Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat, zuständig. Klagen des Betroffenen können auch beim Landesgericht des Landes erhoben werden, in dem der Auftraggeber seinen gewöhnlichen Aufenthalt oder Sitz hat. Liegt der gewöhnliche Aufenthalt oder Sitz in Niederösterreich, ist das Landesgericht für Zivilrechtssachen Wien ausschließlich zuständig. Dieses Gericht ist auch zuständig, wenn sonst keine Zuständigkeit im Inland nach dem ersten Satz gegeben ist.

(2) Die Datenschutzkommission hat in gerichtlichen Verfahren, die Ansprüche aus diesem Bundesgesetz zum Gegenstand haben, sofern sie nicht selbst Parteistellung hat, über Ersuchen des Gerichtes Gutachten über technische und organisatorische Fragen des Datenschutzes abzugeben.

(3) Die Datenschutzkommission hat, wenn ein Betroffener es verlangt und es zur Wahrung der nach diesem Bundesgesetz geschützten Interessen des Datenschutzes und einer größeren Zahl von Betroffenen geboten ist, einem Rechtsstreit auf Seiten des Betroffenen als Nebenintervenient (§§ 17 ff. ZPO) beizutreten.

(4) Das Gericht kann im Urteil aussprechen, daß Entscheidungen im Datenverarbeitungsregister einzutragen sind, wenn es zur Wahrung der nach diesem Bundesgesetz geschützten Interessen des Datenschutzes und einer größeren Zahl von Betroffenen geboten ist.

EINSTWEILIGE VERFÜGUNGEN

§ 30. Zur Sicherung der auf dieses Bundesgesetz gestützten Ansprüche auf Unterlassung können einstweilige Verfügungen erlassen werden, auch wenn die im § 381 EO bezeichneten Voraussetzungen nicht zutreffen. Zuständig zur Erlassung von einstweiligen Verfügungen, die vor Einleitung eines Rechtsstreites beantragt werden, ist das im § 29 Abs. 1 bezeichnete Landesgericht.

RECHTE DES BETRIEBSRATES

§ 31. Die Einsichtsrechte des Betriebsrates nach § 89 Z. 1 und, bei Zustimmung des Arbeitnehmers, nach § 89 Z. 4 des Arbeitsverfassungsgesetzes (BGBl. Nr. 22/1974) und die Zustimmungsrechte des

Betriebsrates nach § 96 Abs. 1, des Arbeitsverfassungsgesetzes werden durch dieses Bundesgesetz nicht berührt. Das Datengeheimnis ist auch von den Mitgliedern des Betriebsrates zu wahren.

4. Abschnitt

INTERNATIONALER DATENVERKEHR VORAUSSETZUNGEN FÜR ÜBERLASSUNGEN VON DATEN IN DAS AUSLAND

§ 32. (1) Die Überlassung von automationsunterstützt verarbeiteten Daten aus Österreich durch die in den §§ 4, 5 und 17 genannten Rechtsträger in das Ausland ist unter den in § 7 oder § 18 genannten Voraussetzungen zulässig. Sie bedarf der Genehmigung der Datenschutzkommission.

(2) In folgenden Fällen bedarf jedoch die Überlassung durch unter den 3. Abschnitt fallende Rechtsträger keiner Genehmigung der Datenschutzkommission:

1. wenn es sich um Überlassungen von Daten des Auftraggebers als Betroffenen handelt, oder
 2. wenn die Überlassung in einen Staat, in dem auf die Daten ein diesem Bundesgesetz vergleichbarer Datenschutz Anwendung findet, erfolgt, oder
 3. wenn dies in völkerrechtlichen Vereinbarungen vorgesehen ist.
- (3) Eine nach Abs. 1 notwendige Genehmigung ist zu erteilen, wenn
1. nicht öffentliche Interessen einschließlich völkerrechtlicher Verpflichtungen entgegenstehen, und
 2. die Überlassung den Erfordernissen des § 7 oder § 18 entspricht, und
 3. glaubhaft gemacht wird, daß durch die Überlassung in das Ausland schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden, und
 4. soweit eine Überlassung in das Ausland zum Zwecke der Verarbeitung als Dienstleistung (§ 19) erfolgt, durch entsprechende Vereinbarungen sichergestellt wird, daß den Bestimmungen des § 19 entsprochen wird.

(4) Soweit gemäß §§ 8 oder 23 eine Registrierungspflicht besteht, bedürfen auch Überlassungen in das Ausland einer Registrierung (§ 47 Abs. 4 und 5).

(5) Durch Verordnung des Bundeskanzlers ist nach Anhörung der Datenschutzkommission festzustellen, inwieweit eine Gleichwertigkeit ausländischer Datenschutzbestimmungen (Abs. 1 Z. 2) gegeben ist. Dabei ist insbesondere auf die Wahrung der schutzwürdigen Interessen der Betroffenen Bedacht zu nehmen.

VERARBEITUNG IN ÖSTERREICH FÜR DAS AUSLAND

§ 33. Die Verarbeitung von Daten in Österreich für ausländische Rechtsträger ist dem Datenverarbeitungsregister zu melden (§ 47 Abs. 4 und 5). Sie

unterliegt einer Genehmigung der Datenschutzkommission, soweit dies in völkerrechtlichen Vereinbarungen vorgesehen ist.

DIREKTER ZUGRIFF ZU DATEN

§ 34. (1) § 32 findet auch Anwendung, wenn nur ein Arbeitsgang der Verarbeitung im Ausland oder für das Ausland stattfindet oder ein direkter Zugriff auf im Bundesgebiet gelegene Anlagen der automationsunterstützten Datenverarbeitung aus dem Ausland möglich ist.

(2) Wenn vom Bundesgebiet aus ein direkter Zugriff auf in Anlagen der automationsunterstützten Verarbeitung im Ausland gespeicherte Daten möglich ist, findet § 33 Anwendung.

5. Abschnitt

DATENSCHUTZKOMMISSION, DATENSCHUTZRAT UND DATENVERARBEITUNGSREGISTER

KONTROLLORGANE

§ 35. (1) Zur Wahrung des Datenschutzes im Sinne dieses Bundesgesetzes – unbeschadet der Zuständigkeit der ordentlichen Gerichte – werden eine Datenschutzkommission und ein Datenschutzrat eingerichtet.

(2) Die Geschäftsführung der in Abs. 1 genannten Organe obliegt dem Bundeskanzleramt. Der Bundeskanzler hat diesen Organen das notwendige Personal auf Vorschlag des Datenschutzrates zur Verfügung zu stellen. Im Rahmen ihrer Tätigkeit für diese Organe sind solche Personen an die Weisungen des jeweiligen Vorsitzenden oder der in den Geschäftsordnungen bezeichneten Mitglieder der in Abs. 1 genannten Organe gebunden.

AUFGABEN DER DATENSCHUTZKOMMISSION

§ 36. (1) Der Datenschutzkommission obliegen – abgesehen von den in den § 9 Abs. 1, § 9 Abs. 2, § 10 Abs. 1, § 12 Abs. 2 Z. 4, § 13 Abs. 3, § 16, § 37, § 38 Abs. 6, § 39 Abs. 1, § 44 Abs. 2, § 45 Abs. 3 und 4, § 50 Abs. 5 und § 52 Abs. 3 genannten Befugnissen – folgende Aufgaben:

1. die Durchführung von Beschwerdeverfahren (§ 14) und von Verfahren nach § 12 Abs. 10;
2. die amtswegige Einleitung und Durchführung von Verfahren nach § 15;
3. die Erlassung von mit Eintragungen in das Datenverarbeitungsregister zusammenhängenden Bescheiden (§ 47);
4. die Erteilung der für den internationalen Datenverkehr notwendigen Bewilligungen (§§ 32 bis 34);
5. die Erlassung ihrer Geschäftsordnung.

(2) (Verfassungsbestimmung) Weiters obliegen der Datenschutzkommission die Abfassung der Berichte

nach § 46 Abs. 1, von Empfehlungen nach § 41, Gutachten oder Zustimmungen zu Entwürfen von Rechtsvorschriften, die die Verarbeitung personenbezogener Daten betreffen, und zu Maßnahmen nach § 13 sowie Beteiligungen an gerichtlichen Verfahren.

(3) Auf das behördliche Verfahren der Datenschutzkommission ist das AVG 1950, im Verfahren nach § 50 Abs. 5 das VStG 1950 anzuwenden.

(4) Entscheidungen der Datenschutzkommission unterliegen nicht der Aufhebung oder Abänderung im Verwaltungswege. Die Beschwerde an den Verwaltungsgerichtshof ist zulässig.

(5) (Verfassungsbestimmung) Die Beschwerde an den Verwaltungsgerichtshof ist auch zulässig in den Fällen des Art. 130 Abs. 1 lit. c B-VG.

WIRKUNG VON BESCHIEDEN

§ 37. (1) Wenn die Datenschutzkommission eine Verletzung von Bestimmungen dieses Bundesgesetzes oder der auf Grund dieses Bundesgesetzes erlassenen Durchführungsbestimmungen festgestellt hat, so sind die Verwaltungsbehörden verpflichtet, mit den ihnen zu Gebote stehenden rechtlichen Mitteln unverzüglich den der Rechtsanschauung der Datenschutzkommission entsprechenden Zustand herzustellen. In den Bescheiden der Datenschutzkommission ist die Behörde zu bestimmen, die den Bescheid zu vollstrecken hat. Das Vollstreckungsverfahren richtet sich nach den für diese Behörde sonst geltenden Vorschriften.

(2) Bei Gefahr im Verzug für den Betroffenen kann die Datenschutzkommission die Benützung oder Übermittlung der Daten oder einzelne Verarbeitungsvorgänge bis zur Entscheidung der Datenschutzkommission nach § 14 oder § 15 untersagen.

ZUSAMMENSETZUNG DER DATENSCHUTZKOMMISSION

§ 38. (1) Die Datenschutzkommission besteht aus vier Mitgliedern, die über Vorschlag der Bundesregierung vom Bundespräsidenten für die Dauer von fünf Jahren bestellt werden. Wiederbestellungen sind zulässig. Ein Mitglied muß dem Richterstand angehören. Die Mitglieder sollen Erfahrungen auf dem Gebiet des Datenschutzes aufweisen.

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

1. Vom Präsidenten des Obersten Gerichtshofes einen Dreivorschlag für das richterliche Mitglied;
2. von den Ländern für zwei Mitglieder.
- (3) Ein Mitglied ist aus dem Kreise der rechtskundigen Bundesbeamten vorzuschlagen.
- (4) Für jedes Mitglied ist ein Ersatzmitglied zu bestellen. Das Ersatzmitglied tritt bei Verhinderung eines Mitgliedes an dessen Stelle.

(5) Der Datenschutzkommission können nicht angehören:

1. Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre;
2. Personen, die mit der Verarbeitung von Daten, auf die die Bestimmungen dieses Bundesgesetzes Anwendung finden, unmittelbar befaßt sind;
3. 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 zwei ihrer Mitglieder zustimmen müssen, seines Amtes für verlustig erklärt werden.

(7) Auf die Ersatzmitglieder finden die Abs. 2, 3, 5 und 6 sinngemäß Anwendung.

(8) Scheidet ein Mitglied wegen Todes, freiwillig oder gemäß Abs. 6 vorzeitig aus, so wird das betreffende Ersatzmitglied (Abs. 2 und 3) Mitglied der Datenschutzkommission, und es ist unter Anwendung der Absätze 2 und 3 bis zum Ablauf der Funktionsperiode der Mitglieder ein neues Ersatzmitglied zu bestellen.

(9) Die Mitglieder der Datenschutzkommission haben Anspruch auf Ersatz der Reisekosten (Gebührenstufe 5) nach Maßgabe der für Bundesbeamte der Allgemeinen Verwaltung geltenden Rechtsvorschriften. Sie haben ferner Anspruch auf eine dem Zeit- und Arbeitsaufwand entsprechende Vergütung, die auf Antrag des Bundeskanzlers von der Bundesregierung durch Verordnung festzusetzen ist.

VORSITZENDER UND GESCHÄFTSFÜHRUNG DER DATENSCHUTZKOMMISSION

§ 39. (1) Das richterliche Mitglied führt den Vorsitz in der Datenschutzkommission. Die Datenschutzkommission wählt aus ihrer Mitte einen stellvertretenden Vorsitzenden.

(2) (Verfassungsbestimmung) Die Datenschutzkommission gibt sich eine Geschäftsordnung, in der eines ihrer Mitglieder mit der Führung der laufenden Geschäfte zu betrauen ist. Diese Betrauung kann auch die Erlassung von verfahrensrechtlichen Bescheiden beinhalten.

(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.

WEISUNGSFREIHEIT DER MITGLIEDER DER DATENSCHUTZKOMMISSION

§ 40. (Verfassungsbestimmung) Die Mitglieder der Datenschutzkommission sind in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden.

EMPFEHLUNGEN DER DATENSCHUTZKOMMISSION

§ 41. Hat die Datenschutzkommission gegen die Rechtmäßigkeit einer Ermittlung, Verarbeitung, Benützung oder Übermittlung von Daten von oder für Rechtsträger nach § 4 oder § 5 Bedenken, so hat sie diese Bedenken samt Begründung und einer Empfehlung über die Herstellung des rechtmäßigen Zustandes dem für den Auftrag zur betreffenden Verarbeitung zuständigen obersten Verwaltungsorgan mitzuteilen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder diesen Empfehlungen zu entsprechen und dies der Datenschutzkommission mitzuteilen oder schriftlich zu begründen, warum den Empfehlungen nicht entsprochen wurde.

AUFGABEN DES DATENSCHUTZRATES

§ 42. (1) Dem Datenschutzrat obliegen – abgesehen von den in den § 4 Abs. 2, § 4 Abs. 3 Z. 3, § 5 Abs. 2, § 11 Abs. 3, § 21 Abs. 3, § 22 Abs. 4, § 24, § 35 Abs. 2, § 44, § 45 Abs. 3 und 4, § 47 Abs. 3 und § 52 Abs. 3 genannten Befugnissen – folgende Aufgaben:

1. Auskünfte und Berichte über Fragen des Datenschutzes bei der Verarbeitung von Daten im öffentlichen Bereich von den zuständigen Organen zu verlangen;
2. Auswirkungen des automationsunterstützten Datenverkehrs auf die Wahrung schutzwürdiger Interessen, insbesondere auf Achtung des Privat- und Familienlebens im Sinne des § 1 dieses Bundesgesetzes zu beobachten und die Ergebnisse solcher Beobachtungen dem Bericht der Datenschutzkommission nach § 46 Abs. 1 sowie allfälligen ADV-Berichten und Plänen der Bundesregierung beizufügen;
3. Anregungen zur allfälligen Verbesserung des Schutzes von Daten, die infolge der Entwicklung des Datenverkehrs zum Schutz der verfassungsgesetzlich gewährleisteten Rechte notwendig werden, der Bundesregierung und den Landesregierungen sowie über Vermittlung dieser den gesetzgebenden Organen gegenüber auszusprechen;
4. auf Antrag eines der dem Datenschutzrat angehörenden Vertreter der politischen Parteien Fragen von grundsätzlicher Bedeutung für den Datenschutz in Beratung zu ziehen;
5. die Erlassung seiner Geschäftsordnung.

(2) Die zuständigen Bundesminister und Landesregierungen haben auf Ersuchen des Datenschutzrates

diesem über Erfahrungen auf dem Gebiete des Datenschutzes aus ihrem Bereich zu berichten.

(3) Gerichtliche Entscheidungen und Vergleiche in Verfahren auf Grund dieses Bundesgesetzes sind dem Datenschutzrat zuzustellen.

ZUSAMMENSETZUNG DES DATENSCHUTZRATES

§ 43. (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. Bei Mandatsgleichheit der beiden im Nationalrat am stärksten vertretenen Parteien entsendet jede dieser Parteien drei Vertreter.
2. Je ein Vertreter des Österreichischen Arbeiterkammertages und der Bundeskammer der gewerblichen Wirtschaft;
3. zwei Vertreter der Länder;
4. je ein Vertreter des Gemeindebundes und des Städtebundes;
5. ein vom Bundeskanzler zu ernennender Vertreter des Bundes.

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

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

(4) § 38 Abs. 5 ist sinngemäß anzuwenden.

(5) Die Mitglieder gehören dem Datenschutzrat solange an, bis von den namhaft machenden Stellen (Abs. 1) andere Vertreter namhaft gemacht worden sind.

(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 5) nach Maßgabe der für Bundesbeamte der Allgemeinen Verwaltung geltenden Rechtsvorschriften.

VORSITZ UND GESCHÄFTSFÜHRUNG DES DATENSCHUTZRATES

§ 44. (1) Der Datenschutzrat wählt aus seiner Mitte einen Vorsitzenden und zwei stellvertretende Vorsitzende. Die Funktionsperiode des Vorsitzenden (stellvertretenden Vorsitzenden) dauert, unbeschadet der Änderung der Vertretung gemäß § 43 Abs. 5, fünf Jahre. Wiederbestellungen sind zulässig.

(2) Die Sitzungen des Datenschutzrates sind nach Bedarf einzuberufen. Begehrt ein Mitglied oder die Datenschutzkommission die Einberufung einer Sitzung, so hat der Vorsitzende eine Sitzung einzuberufen, die binnen vier Wochen stattzufinden hat.

(3) Für Beratungen und Beschlußfassungen im Datenschutzrat ist die Anwesenheit von mehr als der Hälfte seiner Mitglieder erforderlich. Zur Beschlußfassung genügt die einfache Mehrheit der abgegebenen Stimmen. Bei Stimmgleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig.

(4) Die Beifügung von Minderheitenvoten ist zulässig.

(5) 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 (Berichtserstatter) zu übertragen.

(6) Jedes Mitglied des Datenschutzzrates ist verpflichtet, an den Sitzungen – außer im Fall der gerechtfertigten Verhinderung – teilzunehmen. Jedes Mitglied hat seine Verhinderung an der Teilnahme rechtzeitig bekanntzugeben, worauf das Ersatzmitglied einzuladen ist.

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

GEMEINSAME BESTIMMUNGEN FÜR DATENSCHUTZKOMMISSION UND DATENSCHUTZRAT

§ 45. (1) (Verfassungsbestimmung) Alle Organe von Rechtsträgern nach §§ 4 und 5 haben die Datenschutzkommission und den Datenschutzrat bei der Besorgung ihrer Aufgaben zu unterstützen, ihnen Einsicht in Akten, Datenträger und sonstige Einrichtungen der Ermittlung, Verarbeitung und Übermittlung zu gewähren und auf Verlangen die erforderlichen Auskünfte zu erteilen.

(2) (Verfassungsbestimmung) Die Beratungen der Datenschutzkommission und des Datenschutzzrates sind vertraulich. Die Organe können die Vertraulichkeit ihrer Beratungen insoweit aufheben, als sie dies nach dem Gegenstand und dem Zwecke der Beratungen für notwendig erachten und nicht die Geheimhaltung im öffentlichen Interesse oder im Interesse einer Partei geboten ist.

(3) Die Datenschutzkommission und der Datenschutzrat können nach Bedarf zur Beratung besonderer Fragen Sachverständige zuziehen.

(4) Der Bundeskanzler beruft die jeweils erste Sitzung der Datenschutzkommission und des Datenschutzzrates ein. Im Datenschutzrat führt das an Jahren älteste Mitglied bis zur Wahl des Vorsitzenden den Vorsitz.

DATENSCHUTZBERICHTE

§ 46. (1) Die Datenschutzkommission verfaßt jedes zweite Jahr einen Bericht über ihre Tätigkeit und die

hiebei gesammelten Erfahrungen und übermittelt diesen Bericht dem Bundeskanzler.

(2) Der Bundeskanzler legt diesen Bericht mit einer Stellungnahme der Bundesregierung und des Datenschutzzrates (§ 42 Abs. 1 Z. 2) sowie mit Aussagen über die Entwicklung der Verarbeitung und des Schutzes von Daten im Ausland und mit allfälligen Empfehlungen dem Nationalrat vor. Soweit sich der Bericht auf die Verarbeitung von Daten im Bereich der Länder (§ 5) bezieht, übermittelt der Bundeskanzler den Bericht mit der Stellungnahme des Datenschutzzrates den Ländern.

DATENVERARBEITUNGSREGISTER

§ 47. (1) Beim Österreichischen Statistischen Zentralamt ist ein Register der automationsunterstützten Verarbeitung von Daten (Datenverarbeitungsregister) einzurichten. Die Führung des Datenverarbeitungsregisters obliegt dem Österreichischen Statistischen Zentralamt nach den Anordnungen des Bundeskanzleramtes.

(2) Jedermann kann in das Datenverarbeitungsregister Einsicht nehmen, aus ihm Abschriften anfertigen oder Auszüge gegen Ersatz der tatsächlich notwendigen Kosten verlangen.

(3) Der Bundeskanzler hat nach Anhörung des Datenschutzzrates die näheren Bestimmungen über die Registrierung und die Führung des Registers durch Verordnung zu erlassen. Dabei ist auf die Übersichtlichkeit der Eintragungen, auf die Vergabe einer Registernummer, auf die Einfachheit der Einsichtnahme und das Register sowie bei Eintragung gerichtlicher Entscheidungen auf die Anonymisierung von Daten Bedacht zu nehmen.

(4) Für jeden Auftraggeber (§ 8, § 24 Abs. 1) ist eine Registernummer zu vergeben. Übermittlungen im Sinne des § 3 Z. 8 und Mitteilungen an den Betroffenen dürfen, unabhängig von ihrer Form, nur unter Zusatz der Registernummer des Auftraggebers erfolgen. Wiedergaben und Abschriften der übermittelten Daten haben die Registernummer zu enthalten.

(5) Dem Anmelder ist die Durchführung der Eintragung schriftlich mit einem Registerauszug mitzuteilen. Mit dieser Mitteilung kann die Echtverarbeitung aufgenommen werden. Durch die Registrierung wird allfälligen behördlichen Entscheidungen über die Rechtmäßigkeit der Verarbeitungen nicht vorgegriffen.

(6) Jede Änderung der für die Eintragung in das Datenverarbeitungsregister maßgeblichen Umstände ist dem Datenverarbeitungsregister unverzüglich zu melden. Die §§ 8 und 24 sowie Abs. 5 sind sinngemäß anzuwenden.

(7) Eine Streichung aus dem Datenverarbeitungsregister ist auf Antrag des Eingetragenen oder durch Bescheid auf Grund eines die Rechtswidrigkeit der Verarbeitung aussprechenden gerichtlichen Urteils vorzunehmen.

(8) Das Datenverarbeitungsregister kann mit automationsunterstützter Datenverarbeitung geführt werden. Wenn Ausfertigungen unter Verwendung

der automationsunterstützten Datenverarbeitung erstellt werden, bedürfen sie weder einer Unterschrift noch einer Beglaubigung; sie haben aber den Namen des die Eingabe genehmigenden Organs zu enthalten.

(4) Zuständig für Entscheidungen nach Abs. 1 bis 3 ist der Landeshauptmann.

(5) (Verfassungsbestimmung) Über Berufungen gegen Bescheide nach Abs. 4 entscheidet die Datenschutzkommission.

(6) Rechtskräftige Entscheidungen nach Abs. 4 sind der Datenschutzkommission zu übermitteln.

6. Abschnitt

STRAFBESTIMMUNGEN

GEHEIMNISBRUCH

§ 48. (1) Wer Daten widerrechtlich offenbart oder verwertet, die ihm ausschließlich kraft seiner berufsmäßigen Beschäftigung mit Aufgaben der Verarbeitung anvertraut worden oder zugänglich geworden sind, und deren Offenbarung oder Verwertung geeignet ist, ein berechtigtes Interesse des Betroffenen zu verletzen, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

(2) Der Täter ist nur auf Antrag eines in seinem Interesse an der Geheimhaltung Verletzten oder auf Antrag der Datenschutzkommission zu verfolgen.

(3) Die Öffentlichkeit in der Hauptverhandlung ist auszuschließen, wenn dies

1. der Staatsanwalt, der Beschuldigte oder ein Privatbeteiligter beantragt, oder
2. das Gericht zur Wahrung von Interessen am Verfahren nicht beteiligter Personen für notwendig hält.

UNBEFUGTE EINGRIFFE IN VERARBEITUNGEN

§ 49. Wer widerrechtlich einem anderen in seinen Rechten dadurch absichtlich einen Schaden zufügt, daß er automationsunterstützt verarbeitete Daten löscht, verfälscht oder sonst verändert oder daß er sich automationsunterstützt verarbeitete Daten verschafft, 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

§ 50. (1) Eine Verwaltungsübertretung, die mit einer Geldstrafe bis zu 150 000 S zu ahnden ist, begeht, wer Daten automationsunterstützt verarbeitet, ohne die ihm nach diesem Bundesgesetz obliegenden Informations- oder Registrierungspflichten erfüllt zu haben, oder wer Daten entgegen den Bestimmungen des § 47 Abs. 4 übermittelt.

(2) Der Versuch ist strafbar.

(3) Die Strafe des Verfalls von Datenträgern und Programmen kann ausgesprochen werden (§§ 10, 17 und 18 VStG 1950), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 in Zusammenhang stehen.

7. Abschnitt

ÜBERGANGS- UND SCHLUSSBESTIMMUNGEN

GEMEINSAME VERARBEITUNG VON DIENSTSTELLEN DESSELBEN VERWALTUNGSBEREICHES

§ 51. (1) Im Bereich der unmittelbaren Bundesverwaltung kann die Verarbeitung abweichend von § 6 von einem Bundesministerium als sachlich in Betracht kommende Oberbehörde für die Unterbehörden oder von einer Unterbehörde für andere Unterbehörden desselben Bundesministeriums geführt werden.

(2) Abs. 1 ist sinngemäß für die Landesverwaltung und die mittelbare Bundesverwaltung anzuwenden. Deren Datenverarbeitung kann durch die Landesregierung oder durch eine sonstige Einrichtung der Landesverwaltung geführt werden.

ERPROBUNG NEUER ARBEITSWEISEN UND TECHNIKEN DER VERWALTUNG

§ 52. (1) Die Bestimmungen der §§ 6, 7, 9 und 10 finden keine Anwendung auf Verarbeitungen, soweit diese von den in den §§ 4 und 5 genannten Rechtsträgern eingesetzt werden zur Erprobung neuer Arbeitsweisen und Techniken der Verwaltung, bevor diese zum allgemeinen Einsatz gelangen.

(2) In sinngemäßer Anwendung des § 10 Abs. 2 und 3 sind für Verarbeitungen nach Abs. 1 die zum Schutz der Rechte des Betroffenen notwendigen Sicherungsmaßnahmen zu treffen.

(3) Für Maßnahmen nach Abs. 1 sind nach Anhörung der Datenschutzkommission und des Datenschutzrates Verordnungen zu erlassen. In diesen Verordnungen ist auf die Grundsätze der Zweckmäßigkeit und Sparsamkeit der Verwaltung Bedacht zu nehmen und der sachliche und räumliche Bereich von Modellversuchen nach Abs. 1 sowie die Art und die Verwendung der Daten anzugeben. Die Verordnungen sind zu befristen, wobei die Fristsetzung in Entsprechung der für die Beurteilung der Modellversuche notwendigen Zeit zu erfolgen hat.

(4) Die Verordnungen nach Abs. 3 sind zu erlassen:

1. soweit es sich um Verarbeitungen im Bereich des Bundes handelt (§ 4), vom zuständigen Bundesminister oder der Bundesregierung;
2. soweit es sich um Verarbeitungen im Bereich der Länder handelt (§ 5), von der Landesregierung.

ANWENDUNG DES § 7 AUF VERWALTUNGS- ANGELEGENHEITEN GEMÄSS ART. 30 B-VG

§ 53. § 7 findet auf personenbezogene Daten aus dem Bereich der dem Präsidenten des Nationalrates gemäß Art. 30 B-VG übertragenen Verwaltungsangelegenheiten mit der Maßgabe Anwendung, daß, sofern der Betroffene nicht ausdrücklich schriftlich zugestimmt hat, diese Daten jeweils nur mit Zustimmung des Präsidenten des Nationalrates übermittelt werden dürfen.

AUSNAHME FÜR MEDIENUNTERNEHMEN

§ 54. Bis zum Inkrafttreten von Datenschutzbestimmungen eines Mediengesetzes finden die einfachgesetzlichen Bestimmungen dieses Bundesgesetzes keine Anwendung, insoweit Medienunternehmen oder redaktionelle Hilfsunternehmen Daten ausschließlich für ihre publizistische Tätigkeit ermitteln, verarbeiten, benützen oder übermitteln.

VERHÄLTNIS ZU ANDEREN RECHTSVOR- SCHRIFTEN

§ 55. (1) Die den gesetzlich anerkannten Religionsgesellschaften nach § 118 Abs. 2 BAO, BGBl. Nr. 194/1961, zustehenden Rechte bleiben unberührt.

(2) Die Bestimmungen der §§ 11 und 12 sind auf das Strafregister (Strafregistergesetz 1968, BGBl. Nr. 277) nicht anzuwenden.

(3) § 23 Abs. 7 des Wehrgesetzes 1978, BGBl. Nr. 150/1978, und § 2 Abs. 6 des Hochschüler-schaftsgesetzes 1973, BGBl. Nr. 309, bleiben unberührt.

(4) Mit Ablauf des 31. Dezember 1979 tritt § 8 Abs. 4 des Bundesrechnamtsgesetzes, BGBl. Nr. 123/1978, außer Kraft.

GEBÜHREN- UND ABGABENBEFREIUNG

§ 56. Die durch dieses Bundesgesetz unmittelbar veranlaßten Eingaben der Betroffenen zur Wahrung ihrer Interessen sind von den Stempelgebühren und von den Verwaltungsabgaben des Bundes befreit.

EIGENER WIRKUNGSBEREICH DER GEMEINDE

§ 57. Soweit dieses Bundesgesetz auf die Verarbeitung von Daten von oder im Auftrage von Gemeinden anzuwenden ist, sind von der Gemeinde nach diesem Bundesgesetz durchzuführende Aufgaben solche des eigenen Wirkungsbereiches, soweit die Daten ausschließlich oder überwiegend im Interesse der Gemeinde ermittelt, verarbeitet, benützt oder übermittelt werden.

INKRAFTTRETEN

§ 58. (1) Dieses Bundesgesetz tritt, soweit in den folgenden Absätzen nicht anderes bestimmt ist, mit 1. Jänner 1980 in Kraft.

(2) Verarbeitungen nach den §§ 8 und 23, die am 1. Jänner 1980 bereits in Betrieb stehen, sind bis zum 1. April 1980 für das Datenverarbeitungsregister anzumelden. Die Frist des § 23 Abs. 4 gilt für solche Anmeldungen nicht; Übermittlungen dürfen in dem Umfang, in dem sie im Zeitpunkt der Anmeldung durchgeführt wurden, bis zur Vergabe der Registernummer ohne deren Beifügung erfolgen.

(3) Verarbeitungen, die am 1. Jänner 1980 in Betrieb stehen, dürfen bis zum 1. Jänner 1981 fortgeführt werden; insoweit finden auf sie die §§ 6, 7, 17, 18, 22, 32 bis 34 bis zum 1. Jänner 1981 keine Anwendung.

(4) Wurden Betroffene nicht von Verarbeitungen gemäß § 22 bis zum 1. Jänner 1982 informiert, so sind deren Daten zu löschen.

(5) § 21 tritt am 1. Juli 1981 in Kraft.

(6) Werden Durchführungsbestimmungen nach den §§ 9 und 10 erlassen sowie ÖNORMEN nach § 21 Abs. 3 für verbindlich erklärt, so treten diese Vorschriften frühestens sechs Monate nach ihrer Erlassung in Kraft.

(7) Die Fristen, die in diesem Bundesgesetz für die Auskunftserteilung und für die Richtigstellung festgelegt sind (§§ 11, 12, 25, 26), werden für Anträge von Betroffenen, die bis zum 30. Juni 1980 gestellt werden, verdoppelt.

(8) Anträge von Betroffenen nach § 12 Abs. 7 sowie über die Empfänger übermittelter Daten können sich nicht auf Ermittlungen und Übermittlungen beziehen, die vor dem 1. Juli 1979 stattgefunden haben.

(9) Verordnungen auf Grund dieses Bundesgesetzes können ab dem auf seine Kundmachung folgenden Tag erlassen werden.

(10) Die Durchführungsbestimmungen zu den §§ 9 und 10 sind bis zum 1. Juli 1980 zu erlassen.

(11) Für Verarbeitungen nach § 13 sind die notwendigen Verträge bis 1. Juli 1980 abzuschließen.

(12) Die für das Inkrafttreten dieses Bundesgesetzes notwendigen organisatorischen und personellen Maßnahmen können ab dem 1. Jänner 1979 getroffen werden, die Mitglieder der Datenschutzkommission und des Datenschutzrates sind bis zum 1. April 1979 zu bestellen. Die erste Sitzung der Datenschutzkommission und des Datenschutzrates ist vom Bundeskanzler bis zum 1. Juli 1979 einzuberufen.

VOLLZIEHUNG

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

/2

Entschließung

Aus Anlaß der Beschlußfassung des Datenschutzgesetzes wird die Bundesregierung ersucht, dem Nationalrat ehestmöglich eine Regierungsvorlage über ein Bundesgesetz vorzulegen, durch das die, zur Ergänzung des Datenschutzgesetzes notwendigen, schadenersatzrechtlichen Bestimmungen getroffen werden. Hierbei mögen die Möglichkeiten einer Vereinfachung der Haftung, einer eingeschränkten Erfolgshaftung sowie eines Ersatzes auch immaterieller Schäden für das Schadenersatzrecht im Bereich des Datenschutzes geprüft werden.