www.bka.gv.at/datenschutz/ - v3post@bka.gv.at

Gesetz vom 20. März 2001 über den Schutz personenbezogener Daten in nicht automationsunterstützt geführten Dateien (Steiermärkisches Datenschutzgesetz - StDSG)

LGBl. Nr. 39/2001

Inhaltsverzeichnis

1. Abschnitt - Allgemeines

§ 1 - Allgemeines

(1) Dieses Gesetz regelt die Angelegenheiten des Schutzes personenbezogener Daten bei nicht automationsunterstützt geführten Dateien.

(2) Dieses Gesetz gilt nicht für

- Dateien, die für Zwecke von Angelegenheiten geführt werden, in denen die Gesetzgebung Bundessache ist,
- die Verwendung personenbezogener Daten durch natürliche Personen für ausschließlich persönliche und familiäre Tätigkeiten.

§ 2 - Räumlicher Anwendungsbereich

(1) Dieses Gesetz ist auf die Verwendung von personenbezogenen Daten im Land Steiermark anzuwenden. Darüber hinaus ist dieses Gesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in der Steiermark gelegenen Haupt oder Zweigniederlassung eines Auftraggebers geschieht.

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

(3) Weiters ist dieses Gesetz nicht anzuwenden, soweit personenbezogene Daten durch die Steiermark nur durchgeführt werden.

§ 3 - Begriffsbestimmungen

Im Sinne dieses Landesgesetzes bedeuten:

1. Daten (personenbezogene Daten): Angaben über Betroffene (Z. 4), deren Identität bestimmt oder bestimmbar ist;

2. nur indirekt personenbezogene Daten: Daten für einen Auftraggeber (Z. 5), Dienstleister (Z. 6) oder Empfänger einer Übermittlung (Z. 13), deren Personenbezug derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;
3. sensible Daten (besonders schutzwürdige Daten): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;
4. Betroffener: jede vom Auftraggeber (Z. 5) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z. 9) werden;
5. Auftraggeber: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft und die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Z. 10), und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Als Auftraggeber gelten sie auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten. Wurde jedoch dem Auftragnehmer anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt oder hat der Auftragnehmer die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 5 Abs. 2 eigenverantwortlich zu treffen, so gilt der mit der Herstellung des Werkes Betraute als datenschutzrechtlicher Auftraggeber;
6. Dienstleister: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft und die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden (Z. 9);
7. Datei: strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;
8. Datenanwendung: die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z. 9), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind;
9. Verwenden von Daten: jede nicht automationsunterstützte Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten (Z. 10) als auch das Übermitteln (Z. 13) von Daten.
10. Verarbeiten von Daten: das Ermitteln, Erfassen, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Benützen, Überlassen (Z. 12), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittelns (Z. 13) von Daten, soweit diese Schritte nicht automationsunterstützt erfolgen;
11. Ermitteln von Daten: das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden;
12. Überlassen von Daten: die Weitergabe von Daten vom Auftraggeber an einen Dienstleister;
13. Übermitteln von Daten: die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;
14. Zustimmung: die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;
15. Niederlassung: jede durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die am Ort ihrer Einrichtung auch tatsächlich Tätigkeiten ausübt;
16. Datenschutzkommission: die nach dem 7. Abschnitt des Datenschutzgesetzes 2000 eingerichtete Datenschutzkommission;
17. Datenverarbeitungsregister: das nach dem 4. Abschnitt des Datenschutzgesetzes 2000 eingerichtete Datenverarbeitungsregister.

§ 4 - Öffentlicher und privater Bereich

(1) Datenanwendungen sind dem öffentlichen Bereich im Sinne dieses Gesetzes zuzurechnen, wenn sie für Zwecke eines Auftraggebers des öffentlichen Bereichs (Abs. 2) durchgeführt werden.

(2) Auftraggeber des öffentlichen Bereichs sind alle Auftraggeber,

1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer

Gebietskörperschaft, oder
2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

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

2. Abschnitt - Verwendung von Daten

§ 5 - Grundsätze

(1) Daten dürfen nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werden;
2. für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden; die Weiterverwendung für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 31 und 32 zulässig;
3. verwendet werden, soweit sie für den Zweck der Datenanwendung wesentlich sind und über diesen Zweck nicht hinausgehen;
4. so verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
5. so lange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

(2) Für den privaten Bereich können die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen durch Verhaltensregeln festlegen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist. Solche Verhaltensregeln dürfen nur veröffentlicht werden, nachdem sie der Landesregierung zur Begutachtung vorgelegt wurden und diese ihre Übereinstimmung mit den Bestimmungen dieses Gesetzes als gegeben erachtet hat.

§ 6 - Pflichten des Auftraggebers

(1) Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der in § 5 Abs. 1 genannten Grundsätze; dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.

(2) Der Auftraggeber einer diesem Gesetz unterliegenden Datenanwendung hat, wenn er nicht im Gebiet der Europäischen Union niedergelassen ist, einen in Österreich ansässigen Vertreter zu benennen, der neben dem Auftraggeber verantwortlich gemacht werden kann.

§ 7 - Zulässigkeit der Verwendung von Daten

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

(2) Daten dürfen nur übermittelt werden, wenn

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

(3) Die Zulässigkeit einer Datenverwendung setzt voraus, dass

- die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß

und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und
- die Grundsätze des § 5 eingehalten werden.

§ 8 - Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht sensibler Daten

(1) Schutzwürdige Geheimhaltungsinteressen im Sinne des § 1 Abs. 1 Datenschutzgesetz 2000 sind bei Verwendung nicht sensibler Daten dann nicht verletzt, wenn

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

(2) Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung solcher Daten gemäß § 23 Widerspruch zu erheben, bleibt unberührt.

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

1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder
2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder
3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder
4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem erforderlich ist oder
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat.

(4) Die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verstößt - unbeschadet der Bestimmungen des Abs. 2 - nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht oder
2. die Verwendung derartiger Daten für Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist oder
3. sich sonst die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden berechtigten Interessen des Auftraggebers ergibt und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen nach diesem Gesetz gewährleistet.

§ 9 - Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

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

1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder
2. die Daten in nur indirekt personenbezogener Form verwendet werden oder
3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen, oder
4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur

Amtshilfe geschieht oder
5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben, oder
6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder
8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist oder
9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
10. Daten für private Zwecke oder für wissenschaftliche Forschung oder Statistik gemäß § 31 oder zur Benachrichtigung oder Befragung des Betroffenen gemäß § 32 verwendet werden oder
11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse zur Datenverwendung unberührt bleiben, oder
12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen oder
13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten und es sich hiebei um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben; diese Daten dürfen, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden.

§ 10 - Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen

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

(2) Beabsichtigt ein Auftraggeber des öffentlichen Bereichs, einen Dienstleister im Rahmen einer Datenanwendung heranzuziehen, die der Vorabkontrolle gemäß § 16 unterliegt, hat er dies der Datenschutzkommission mitzuteilen. Dies gilt nicht, wenn

- die Inanspruchnahme des Dienstleisters auf Grund ausdrücklicher gesetzlicher Ermächtigung erfolgt oder
- als Dienstleister eine Organisationseinheit tätig wird, die mit dem Auftraggeber oder einem diesem übergeordneten Organ in einem Über oder Unterordnungsverhältnis steht.

(3) Kommt die Datenschutzkommission zur Auffassung, dass die geplante Inanspruchnahme eines Dienstleisters geeignet ist, schutzwürdige Geheimhaltungsinteressen der Betroffenen zu gefährden, so hat sie dies dem Auftraggeber unverzüglich mitzuteilen. Im Übrigen gilt § 25 Abs. 6 Z. 4.

§ 11 - Pflichten des Dienstleisters

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

1. die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden; insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten;
2. alle gemäß § 14 erforderlichen Datensicherheitsmaßnahmen zu treffen; insbesondere dürfen für die Dienstleistung nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen

Verschwiegenheitspflicht unterliegen;
3. weitere Dienstleister nur mit Billigung des Auftraggebers heranzuziehen und deshalb den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann;
4. - sofern dies nach der Art der Dienstleistung in Frage kommt - im Einvernehmen mit dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen;
5. nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten;
6. dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der unter Z. 1 bis 5 genannten Verpflichtungen notwendig sind.

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

§ 12 - Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland

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

(2) Keiner Genehmigung gemäß § 13 bedarf weiters der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutz. Die Landesregierung stellt unter Beachtung der Verordnung des Bundeskanzlers auf Grundlage von § 12 Abs. 2 DSG 2000 sowie des § 55 Z. 1 DSG 2000 mit Verordnung fest, welche Drittstaaten angemessenen Datenschutz gewährleisten. Maßgebend für die Angemessenheit des Schutzes ist die Ausgestaltung der Grundsätze des § 5 Abs. 1 in der ausländischen Rechtsordnung und das Vorhandensein wirksamer Garantien für ihre Durchsetzung.

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

1. die Daten im Inland zulässigerweise veröffentlicht wurden oder
2. Daten, die für den Empfänger nur indirekt personenbezogen sind, übermittelt oder überlassen werden oder
3. die Übermittlung oder Überlassung von Daten ins Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind, oder
4. der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat oder
5. ein vom Auftraggeber mit dem Betroffenen oder mit einem Dritten eindeutig im Interesse des Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann oder
6. die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und die Daten rechtmäßig ermittelt wurden oder
7. es sich um Datenverkehr mit österreichischen Dienststellen im Ausland handelt.

(4) Ist eine Übermittlung oder Überlassung von Daten ins Ausland

- zur Wahrung eines wichtigen öffentlichen Interesses oder
- zur Wahrung eines lebenswichtigen Interesses einer Person

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

(5) Voraussetzung für die Zulässigkeit jeder Übermittlung oder Überlassung in das Ausland ist die Rechtmäßigkeit der Datenanwendung im Inland gemäß § 7. Bei Überlassungen ins Ausland muss darüber

hinaus die schriftliche Zusage des ausländischen Dienstleisters an den inländischen Auftraggeber - oder in den Fällen des § 13 Abs. 4 an den inländischen Dienstleister - vorliegen, dass er die Dienstleisterpflichten gemäß § 11 Abs. 1 einhalten werde. Dies entfällt, wenn die Dienstleistung im Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind.

§ 13 - Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland

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

(2) Die Genehmigung ist unter Beachtung der gemäß § 55 Z. 2 DSG 2000 ergangenen Kundmachungen des Bundeskanzlers zu erteilen, wenn die Voraussetzungen des § 12 Abs. 5 vorliegen. Darüber hinaus muss

1. für die im Genehmigungsantrag angeführte Übermittlung oder Überlassung im konkreten Einzelfall angemessener Datenschutz bestehen; dies ist unter Berücksichtigung aller Umstände zu beurteilen, die bei der Datenverwendung eine Rolle spielen, wie insbesondere die Art der verwendeten Daten, die Zweckbestimmung sowie die Dauer der geplanten Verwendung, das Herkunfts- und das Endbestimmungsland und die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen, Standesregeln und Sicherheitsstandards oder
2. der Auftraggeber glaubhaft machen, dass die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Hiefür können insbesondere auch vertragliche Zusicherungen des Empfängers an den Antragsteller über die näheren Umstände der Datenverwendung im Ausland von Bedeutung sein.

(3) Auftraggeber des öffentlichen Bereichs haben im Genehmigungsverfahren auch hinsichtlich der Datenanwendungen Parteistellung, die sie in Vollziehung der Gesetze durchführen.

(4) Abweichend von Abs. 1 kann auch ein inländischer Dienstleister die Genehmigung beantragen, wenn er zur Erfüllung seiner vertraglichen Verpflichtungen gegenüber mehreren Auftraggebern jeweils einen bestimmten weiteren Dienstleister im Ausland heranziehen will. Die tatsächliche Überlassung darf jeweils nur mit Zustimmung des Auftraggebers erfolgen.

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

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

3. Abschnitt - Datensicherheit

§ 14 - Datensicherheitsmaßnahmen

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

und dass die Daten Unbefugten nicht zugänglich sind.

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

1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,
2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
3. jeder Mitarbeiter über seine nach diesem Gesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,
4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,
5. die Zugriffsberechtigung auf Daten und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,
6. eine Dokumentation über die nach Z. 1 bis 5 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

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

(3) Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck - das ist die Kontrolle der Zulässigkeit der Verwendung des dokumentierten Datenbestandes - unvereinbar sind.

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

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

§ 15 - Datengeheimnis

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

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

(3) Auftraggeber und Dienstleister dürfen Anordnungen zur Übermittlung von Daten nur erteilen, wenn dies nach den Bestimmungen dieses Gesetzes zulässig ist. Sie haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur Datenübermittlung wegen Verstoßes gegen die Bestimmungen dieses Gesetzes kein Nachteil erwachsen.

4. Abschnitt - Publizität der Datenanwendungen

§ 16 - Vorabkontrolle

(1) Datenanwendungen, die

1. sensible Daten enthalten oder
2. strafrechtlich relevante Daten im Sinne des § 8 Abs. 4 enthalten oder
3. die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben,

dürfen erst nach einer Vorabkontrolle durch die Datenschutzkommission aufgenommen werden. (2) Dies gilt nicht für Datenanwendungen, die

1. ausschließlich veröffentlichte Daten enthalten oder
2. die Führung von Registern oder Verzeichnissen zum Inhalt haben, die von Gesetzes wegen öffentlich einsehbar sind, sei es auch nur bei Nachweis eines berechtigten Interesses, oder
3. nur indirekt personenbezogene Daten enthalten.

§ 17 - Verfahren zur Vorabkontrolle

(1) Der Auftraggeber hat der Datenschutzkommission folgende Angaben über die Datenanwendung zu melden:

1. den Namen (die sonstige Bezeichnung) und die Anschrift des Auftraggebers sowie eines allfälligen Vertreters gemäß § 6 Abs. 2 und
2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit des Auftraggebers, soweit dies erforderlich ist, und
3. den Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z. 2 ergeben, und
4. die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten und
5. die Kreise der von beabsichtigten Übermittlungen Betroffenen, die zu übermittelnden Datenarten und die zugehörigen Empfängerkreise - einschließlich allfälliger ausländischer Empfängerstaaten - sowie die Rechtsgrundlagen der Übermittlung und
6. - soweit eine Genehmigung der Datenschutzkommission notwendig ist - die Geschäftszahl der Genehmigung durch die Datenschutzkommission sowie
7. allgemeine Angaben über die getroffenen Datensicherheitsmaßnahmen im Sinne des § 14, die eine vorläufige Beurteilung der Angemessenheit der Sicherheitsvorkehrungen erlauben.

(2) Eine Meldung ist mangelhaft, wenn Angaben fehlen, offenbar unrichtig, unstimmig oder so unzureichend sind, dass jemand im Hinblick auf die Wahrnehmung seiner Rechte nach diesem Gesetz keine hinreichende Information darüber gewinnen kann, ob durch die Datenanwendung seine schutzwürdigen Geheimhaltungsinteressen verletzt sein könnten. Unstimmigkeit liegt insbesondere auch dann vor, wenn der Inhalt einer Datenanwendung durch die angegebenen Rechtsgrundlagen nicht gedeckt ist.

(3) Die Datenschutzkommission hat alle Meldungen binnen zwei Monaten zu prüfen. Kommt sie dabei zur Auffassung, dass eine Meldung im Sinne des Abs. 2 mangelhaft ist, so ist dem Auftraggeber längstens innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung des Mangels unter Setzung einer Frist aufzutragen.

(4) Gleichzeitig ist mit einem allfälligen Auftrag zur Verbesserung darüber abzusprechen, ob die Verarbeitung bereits aufgenommen werden darf oder ob dies mangels Nachweises ausreichender Rechtsgrundlagen für die Datenanwendung nicht zulässig ist.

(5) Wird einem Verbesserungsauftrag nicht fristgerecht entsprochen, so hat die Datenschutzkommission die Zulässigkeit der Aufnahme der Datenanwendung mit Bescheid zu untersagen.

(6) Die Datenschutzkommission kann auf Grund der Ergebnisse des Prüfungsverfahrens dem Auftraggeber Auflagen für die Vornahme der Datenanwendung durch Bescheid erteilen, soweit dies zur Wahrung der durch dieses Gesetz geschützten Interessen der Betroffenen notwendig ist.

(7) Wird innerhalb von zwei Monaten nach Meldung kein Auftrag zur Verbesserung erteilt, darf die Verarbeitung aufgenommen werden.

(8) Auftraggeber des öffentlichen Bereichs haben im Verfahren auch hinsichtlich der Datenanwendungen Parteistellung, die sie in Vollziehung der Gesetze durchführen.

§ 18 - Datenverarbeitungsregister

(1) Meldungen gemäß § 17 sind in das Datenverarbeitungsregister einzutragen,

- wenn das Vorabkontrollverfahren die Zulässigkeit der Datenanwendung ergeben hat oder
- zwei Monate nach Einlangen der Meldung bei der Datenschutzkommission verstrichen sind, ohne dass ein Verbesserungsauftrag gemäß § 17 Abs. 3 erteilt wurde.

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

(2) Dem Auftraggeber ist die Durchführung der Registrierung schriftlich in Form eines Registerauszuges mitzuteilen.

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

(4) Streichungen und Änderungen im Datenverarbeitungsregister sind auf Antrag des Eingetragenen oder in den Fällen der Abs. 5 und 6 von Amts wegen durchzuführen.

(5) Gelangen der Datenschutzkommission aus amtlichen Verlautbarungen Änderungen in der Bezeichnung oder der Anschrift des Auftraggebers zur Kenntnis, so sind die Eintragungen von Amts wegen zu berichtigen. Ergibt sich aus einer amtlichen Verlautbarung der Wegfall der Rechtsgrundlage des Auftraggebers, ist von Amts wegen die Streichung aus dem Register anzuordnen.

(6) Werden der Datenschutzkommission andere als die in Abs. 5 bezeichneten Umstände bekannt, die den Verdacht der Mangelhaftigkeit einer Registrierung oder der rechtswidrigen Unterlassung einer Meldung begründen, so hat die Datenschutzkommission ein Verfahren zur Feststellung des für die Erfüllung der Meldepflicht erheblichen Sachverhalts einzuleiten und das Datenverarbeitungsregister entsprechend dem Ergebnis des Verfahrens zu berichtigen.

(7) Jedermann kann in das Register Einsicht nehmen. In den Registrierungsakt einschließlich darin allenfalls enthaltener Genehmigungsbescheide ist Einsicht zu gewähren, wenn der Einsichtswerber glaubhaft macht, dass er Betroffener ist, und soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen des Auftraggebers oder anderer Personen entgegenstehen.

§ 19 - Offenlegungspflicht des Auftraggebers

Auftraggeber haben jedermann auf Anfrage folgende Angaben über ihre Datenanwendungen, die nicht der Vorabkontrolle unterliegen, bekannt zu geben:

1. den Namen (die sonstige Bezeichnung) und die Anschrift des Auftraggebers sowie eines allfälligen Vertreters gemäß § 6 Abs. 2 und
2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit des Auftraggebers, soweit dies erforderlich ist, und
3. den Zweck der Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z. 2 ergeben, und
4. die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten und
5. die Kreise der von beabsichtigten Übermittlungen Betroffenen, die zu übermittelnden Datenarten und die zugehörigen Empfängerkreise - einschließlich allfälliger ausländischer Empfängerstaaten - sowie die Rechtsgrundlagen der Übermittlung.

§ 20 - Informationspflicht des Auftraggebers

(1) Der Auftraggeber einer Datenanwendung hat aus Anlass der Ermittlung von Daten die Betroffenen in geeigneter Weise

1. über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und
2. über Namen und Adresse des Auftraggebers zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen.

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

1. gegen eine beabsichtigte Verarbeitung oder Übermittlung von Daten ein Widerspruchsrecht des Betroffenen gemäß § 23 besteht oder
2. es für den Betroffenen nach den Umständen des Falles nicht klar erkennbar ist, ob er zur Beantwortung der an ihn gestellten Fragen rechtlich verpflichtet ist.

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

1. die Datenverwendung durch Gesetz oder Verordnung vorgesehen ist oder
2. die Information im Hinblick auf die mangelnde Erreichbarkeit von Betroffenen unmöglich ist oder
3. wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert. Dies liegt insbesondere dann vor, wenn Daten für Zwecke der wissenschaftlichen Forschung oder Statistik gemäß § 31 oder Adressdaten im Rahmen des § 32 ermittelt werden und die Information des Betroffenen in diesen Bestimmungen nicht ausdrücklich vorgeschrieben ist. Die Landesregierung kann durch Verordnung weitere Fälle festlegen, in welchen die Pflicht zur Information entfällt.

5. Abschnitt - Die Rechte des Betroffenen

§ 21 - Auskunftsrecht

(1) Der Auftraggeber hat dem Betroffenen Auskunft über die zu seiner Person verarbeiteten Daten zu geben, wenn der Betroffene dies schriftlich verlangt und seine Identität in geeigneter Form nachweist. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden.

(2) Die Auskunft hat in allgemein verständlicher Form anzuführen:

- die verarbeiteten Daten,
- die verfügbaren Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen,
- den Zweck der Datenverwendung und
- die Rechtsgrundlagen hiefür.

Auf Verlangen des Betroffenen sind auch Namen und Adressen von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Mit Zustimmung des Betroffenen kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.

(3) Die Auskunft ist nicht zu erteilen, soweit

- dies zum Schutz des Betroffenen aus besonderen Gründen notwendig ist oder
- überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen, der Auskunftserteilung entgegenstehen.

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

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

(6) Die Auskunft ist unentgeltlich zu erteilen, wenn

- sie den aktuellen Datenbestand einer Datenanwendung betrifft und
- der Betroffene im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat.

In allen anderen Fällen kann ein pauschalierter Kostenersatz von 19 Euro verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.

(7) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Betroffenen innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 26 an die Datenschutzkommission bis zum rechtskräftigen Abschluss des Verfahrens nicht vernichten.

(8) Soweit Datenanwendungen von Gesetzes wegen öffentlich einsehbar sind, hat der Betroffene ein Recht auf Auskunft in dem Umfang, in dem ein Einsichtsrecht besteht. Für das Verfahren der Einsichtnahme gelten die näheren Regelungen der das öffentliche Buch oder Register einrichtenden Gesetze.

(9) Im Falle der auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 5 Abs. 2 eigenverantwortlichen Entscheidung über die Durchführung einer Datenanwendung durch einen Auftragnehmer gemäß § 3 Z. 5 dritter Satz kann der Betroffene sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Betroffenen, soweit dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des eigenverantwortlichen Auftragnehmers mitzuteilen, damit der Betroffene sein Auskunftsrecht gemäß Abs. 1 gegen diesen geltend machen kann.

§ 22 - Recht auf Richtigstellung oder Löschung

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

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

(2) Der Pflicht zur Richtigstellung nach Abs. 1 Z. 1 unterliegen nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist.

(3) Die Unvollständigkeit verwendeter Daten bewirkt nur dann einen Berichtigungsanspruch, wenn sich aus der Unvollständigkeit im Hinblick auf den Zweck der Datenanwendung die Unrichtigkeit der Gesamtinformation ergibt.

(4) Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, dass ihre Archivierung rechtlich zulässig ist und dass der Zugang zu diesen Daten besonders geschützt ist. Die Weiterverwendung von Daten für einen anderen Zweck ist nur zulässig, wenn eine Übermittlung der Daten für diesen Zweck zulässig ist; die Zulässigkeit der Weiterverwendung für wissenschaftliche oder statistische Zwecke ergibt sich aus den §§ 31 und 32.

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

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

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

(8) Werden Daten verwendet, deren Richtigkeit der Betroffene bestreitet und lässt sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen, so ist auf Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. Der Bestreitungsvermerk darf nur mit Zustimmung des Betroffenen oder auf Grund einer Entscheidung des zuständigen Gerichtes oder der Datenschutzkommission gelöscht werden.

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

§ 23 - Widerspruchsrecht

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

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

§ 24 - Die Rechte des Betroffenen bei der Verwendung nur indirekt personenbezogener Daten

Die durch die §§ 21 bis 23 gewährten Rechte können nicht geltend gemacht werden, soweit nur indirekt personenbezogene Daten verwendet werden.

6. Abschnitt - Rechtsschutz

§ 25 - Kontrollbefugnisse der Datenschutzkommission

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

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

(3) Datenanwendungen, die der Vorabkontrolle unterliegen, dürfen auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden.

(4) Zum Zweck der Einschau ist die Datenschutzkommission nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) berechtigt,

- Räume, in welchen Datenanwendungen vorgenommen werden, zu betreten,
- die zu überprüfenden Verarbeitungen durchzuführen sowie
- Kopien von Datenträgern herzustellen.

Der Auftraggeber (Dienstleister) hat die für die Einschau notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Auftraggebers (Dienstleisters) und Dritter auszuüben.

(5) Informationen, die der Datenschutzkommission oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Die Pflicht zur Verschwiegenheit besteht auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden. Ergibt die Einschau den Verdacht einer strafbaren Handlung nach § 34 dieses Gesetzes oder eines Verbrechens, das mit mindestens fünfjähriger Freiheitsstrafe bedroht ist, ist jedoch Anzeige zu erstatten und hinsichtlich solcher Verbrechen und Vergehen auch dem Ersuchen der Strafgerichte nach § 26 StPO zu entsprechen.

(6) Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzkommission Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzkommission je nach der Art des Verstoßes von Amts wegen insbesondere

1. ein Verfahren zur Überprüfung der Registrierung gemäß § 18 Abs. 6 einleiten oder
2. Anzeige nach § 34 erstatten oder
3. bei schwer wiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 27 Abs. 4 erheben oder
4. bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, dass der Empfehlung der Datenschutzkommission entsprochen wird oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzkommission der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.

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

§ 26 - Beschwerde an die Datenschutzkommission

(1) Die Datenschutzkommission erkennt auf Antrag des Betroffenen über behauptete Verletzungen des Rechtes auf Auskunft gemäß § 21 durch den Auftraggeber einer Datenanwendung, soweit sich das Auskunftsbegehren nicht auf die Verwendung von Daten für Akte der Gesetzgebung oder der Gerichtsbarkeit bezieht.

(2) Die Datenschutzkommission ist zur Entscheidung über behauptete Verletzungen der Rechte eines Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung nach diesem Gesetz dann zuständig, wenn der Betroffene seine Beschwerde gegen einen Auftraggeber des öffentlichen Bereichs richtet, der nicht als Organ der Gesetzgebung oder der Gerichtsbarkeit tätig ist.

(3) Bei Gefahr im Verzug kann die Datenschutzkommission im Zuge der Behandlung einer Beschwerde nach Abs. 2 die weitere Verwendung von Daten zur Gänze oder teilweise untersagen oder auch - bei Streitigkeiten über die Richtigkeit von Daten - dem Auftraggeber die Anbringung eines Bestreitungsvermerks auftragen.

§ 27 - Anrufung der Gerichte

(1) Ansprüche gegen Auftraggeber des privaten Bereichs wegen Verletzung der Rechte des Betroffenen auf

Geheimhaltung, auf Richtigstellung oder auf Löschung sind vom Betroffenen auf dem Zivilrechtsweg geltend zu machen.

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

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

(4) Für Klagen und Anträge auf Erlassung einer einstweiligen Verfügung nach diesem Gesetz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen des Betroffenen können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Auftraggeber oder der Dienstleister seinen gewöhnlichen Aufenthalt oder Sitz hat.

(5) Die Datenschutzkommission hat in Fällen, in welchen der begründete Verdacht einer schwer wiegenden Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs besteht, gegen diesen eine Feststellungsklage (§ 228 ZPO) beim zuständigen Gericht zu erheben.

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

§ 28 - Schadenersatz

(1) Ein Auftraggeber oder Dienstleister, der Daten schuldhaft entgegen den Bestimmungen dieses Gesetzes verwendet, hat dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. Werden durch die öffentlich zugängliche Verwendung der in § 16 Abs. 1 Z. 1 bis 3 genannten Datenarten schutzwürdige Geheimhaltungsinteressen eines Betroffenen in einer Weise verletzt, die einer Eignung zur Bloßstellung gemäß § 7 Abs. 1 des Mediengesetzes gleichkommt, so gilt diese Bestimmung auch in Fällen, in welchen die öffentlich zugängliche Verwendung nicht in Form der Veröffentlichung in einem Medium geschieht. Der Anspruch auf angemessene Entschädigung für die erlittene Kränkung ist gegen den Auftraggeber der Datenverwendung geltend zu machen.

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

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

(4) Die Zuständigkeit für Klagen nach Abs. 1 richtet sich nach § 27 Abs. 4.

§ 29 - Gemeinsame Bestimmungen

(1) Der Anspruch auf Behandlung einer Eingabe nach § 25, einer Beschwerde nach § 26 oder einer Klage nach § 27 erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, einbringt. Dies ist dem Einschreiter im Falle einer verspäteten Eingabe gemäß § 25 mitzuteilen; verspätete Beschwerden nach § 26 und Klagen nach § 27 sind abzuweisen.

(2) Eingaben nach § 25, Beschwerden nach § 26, Klagen nach § 27 sowie Schadenersatzansprüche nach § 28 können nicht nur auf die Verletzung der Vorschriften dieses Gesetzes, sondern auch auf die Verletzung von datenschutzrechtlichen Vorschriften eines anderen Mitgliedstaates der Europäischen Union gegründet werden, soweit solche Vorschriften gemäß § 2 anzuwenden sind.

(3) Ist die vermutete Verletzung schutzwürdiger Geheimhaltungsinteressen eines Betroffenen im Land Steiermark gemäß § 2 nach der Rechtsordnung eines anderen Mitgliedstaats der Europäischen Union zu beurteilen, so kann die Datenschutzkommission im Falle ihrer Befassung die zuständige ausländische Datenschutzkontrollstelle um Unterstützung ersuchen.

(4) Die Datenschutzkommission hat den Unabhängigen Datenschutzkontrollstellen der anderen Mitgliedstaaten der Europäischen Union über Ersuchen Amtshilfe zu leisten.

§ 30 - Wirkung von Bescheiden der Datenschutzkommission

(1) Gegen Bescheide der Datenschutzkommission ist kein Rechtsmittel zulässig. Sie unterliegen nicht der Aufhebung oder Abänderung im Verwaltungsweg. Die Anrufung des Verwaltungsgerichtshofes durch die Parteien des Verfahrens ist zulässig. Dies gilt auch für die in Vollziehung der Gesetze tätigen Auftraggeber des öffentlichen Bereichs in jenen Fällen, in welchen ihnen gemäß § 13 Abs. 3 oder § 17 Abs. 8 Parteistellung zukommt oder durch Gesetz ausdrücklich ein Beschwerderecht an den Verwaltungsgerichtshof eingeräumt wurde.

(2) Bescheide, mit welchen gemäß § 13 Übermittlungen oder Überlassungen von Daten ins Ausland genehmigt wurden, sind zu widerrufen, wenn die rechtlichen und tatsächlichen Voraussetzungen für die Erteilung der Genehmigung, insbesondere auch infolge einer gemäß § 55 DSG 2000 ergangenen Kundmachung des Bundeskanzlers nicht mehr bestehen.

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

7. Abschnitt - Besondere Bestimmungen

§ 31 - Wissenschaftliche Forschung und Statistik

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

1. öffentlich zugänglich sind oder
2. der Auftraggeber für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für den Auftraggeber nur indirekt personenbezogen sind. Andere Daten dürfen nur unter den Voraussetzungen des Abs. 2 Z. 1 bis 3 verwendet werden.

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

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

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

1. die Einholung der Zustimmung der Betroffenen mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet und
2. ein öffentliches Interesse an der beantragten Verwendung besteht und
3. die fachliche Eignung des Antragstellers glaubhaft gemacht wird. Sollen sensible Daten übermittelt werden, muss ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muss gewährleistet sein, dass die Daten beim Empfänger nur von Personen verwendet werden, die

hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten notwendig ist.

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

(5) Auch in jenen Fällen, in welchen gemäß den vorstehenden Bestimmungen die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der direkte Personsbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit nur indirekt personenbezogenen Daten das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, ist der Personsbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

§ 32 - Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen

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

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

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

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

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

(4) Die Datenschutzkommission hat die Genehmigung zur Übermittlung zu erteilen, wenn der Antragsteller das Vorliegen der in Abs. 3 genannten Voraussetzungen glaubhaft macht und überwiegende schutzwürdige Geheimhaltungsinteressen der Betroffenen der Übermittlung nicht entgegenstehen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten als Auswahlkriterium, notwendig ist.

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

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

§ 33 - Datenanwendungen des Landtages

Der Präsident des Landtages ist Auftraggeber jener Datenanwendungen, die für Zwecke der ihm gemäß § 3 der Geschäftsordnung des Landtages übertragenen Angelegenheiten durchgeführt werden. Übermittlungen von Daten aus solchen Datenanwendungen dürfen nur über Auftrag des Präsidenten des Landtages vorgenommen werden. Der Präsident trifft Vorsorge dafür, dass im Falle eines Übermittlungsauftrags die Voraussetzungen des § 7 Abs. 2 vorliegen und insbesondere die Zustimmung des Betroffenen in jenen Fällen eingeholt wird, in welchen dies gemäß § 7 Abs. 2 mangels einer anderen Rechtsgrundlage für die Übermittlung notwendig ist.

8. Abschnitt - Straf-, Übergangs- und Schlussbestimmungen

§ 34 - Strafbestimmungen

(1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 20.000 Euro zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrecht hält;
2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 15) übermittelt, insbesondere Daten, die ihm gemäß §§ 31 oder 32 anvertraut wurden, vorsätzlich für andere Zwecke verwendet;
3. Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtig stellt oder nicht löscht;
4. Daten vorsätzlich entgegen § 21 Abs. 7 löscht.

(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 10.000 Euro zu ahnden ist, wer

1. Daten ohne Vorabkontrolle gemäß § 16 ermittelt, verarbeitet oder übermittelt;
2. Daten ins Ausland übermittelt oder überlässt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 eingeholt zu haben;
3. trotz einer Empfehlung der Datenschutzkommission seine Offenlegungs- oder Informationspflicht gemäß § 19 und § 20 verletzt;
4. die gemäß § 14 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht lässt.

(3) Der Versuch ist strafbar.

(4) Die Strafe des Verfalls von Datenträgern kann ausgesprochen werden, wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 oder 2 in Zusammenhang stehen.

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

§ 35 - Mitteilungen an die Europäische Kommission und an die anderen Mitgliedstaaten der Europäischen Union

(1) Von der Erlassung eines Landesgesetzes, das die Zulässigkeit der Verarbeitung sensibler Daten betrifft und über die in Artikel 8 Abs. 2 der Richtlinie 95/46/EG genannten Ausnahmen hinausgeht, hat die Landesregierung der Europäischen Kommission Mitteilung zu machen.

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

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

2. der Datenverkehr in ein Drittland ohne angemessenes Datenschutzniveau genehmigt wurde, weil die Voraussetzungen des § 13 Abs. 2 Z. 2 als gegeben erachtet wurden.

§ 36 - Anhörungsverfahren, Berichtspflicht

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

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

§ 37 - Personenbezogene Bezeichnungen

Personenbezogene Bezeichnungen in diesem Gesetz, die nur in der männlichen oder nur in der weiblichen Form verwendet werden, gelten jeweils für beide Geschlechter gleichermaßen.

§ 38 - Gemeinschaftsrecht

Mit diesem Gesetz wird die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr umgesetzt.

§ 39 - Verweise

(1) Verweise in diesem Gesetz auf Bundesgesetze sind als Verweise auf folgende Fassungen zu verstehen:

1. Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG), BGBl. I Nr. 165/1999;
2. Mediengesetz, BGBl. Nr. 314/1981, in der Fassung BGBl. Nr. 105/1997.

(2) Verweise auf Vorschriften der europäischen Union sind als Verweise auf folgende Fassungen zu verstehen:

1. Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S. 31.

§ 40 - Übergangsbestimmungen

(1) Die Verarbeitung von Daten, die zum Zeitpunkt des Inkrafttretens dieses Gesetzes in manuellen Dateien vorhanden sind, sind bis zum 1. Oktober 2007 mit den §§ 5 bis 9 dieses Gesetzes in Einklang zu bringen.

(2) Betroffene im Sinne dieses Gesetzes können unabhängig von Abs. 1 auf Antrag und insbesondere bei Ausübung des Auskunftsrechts die Berichtigung, Löschung oder Sperrung von Daten erreichen, die unvollständig, unzutreffend oder auf eine Art und Weise aufbewahrt sind, die mit den vom für die Verarbeitung Verantwortlichen verfolgten rechtmäßigen Zwecken unvereinbar ist.

(3) Bis zum 31. Dezember 2001 lautet § 21 Abs. 6 zweiter Satz wie folgt:

"In allen anderen Fällen kann ein pauschalierter Kostenersatz von 260 Schilling verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf."

(4) Bis zum 31. Dezember 2001 lautet § 34 Abs. 1 Einleitungssatz wie folgt:

"(1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht

eine Verwaltungsübertretung, die mit Geldstrafe bis zu 260.000 Schilling zu ahnden ist, wer".

(5) Bis zum 31. Dezember 2001 lautet § 34 Abs. 2 Einleitungssatz wie folgt:

"(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 130.000 Schilling zu ahnden ist, wer".

§ 41 - Inkrafttreten

Dieses Gesetz tritt mit dem der Kundmachung folgenden Monatsersten, das ist der 1. August 2001, in Kraft.