Gesetz vom ..... über den Schutz personenbezogener Daten bei nicht automationsunterstützt geführten Dateien (Burgenländisches Datenschutzgesetz – Bgld. DSG)

Der Landtag hat beschlossen:

INHALTSVERZEICHNIS

4. Abschnitt:
Publizität der Datenanwendungen

5. Abschnitt:
Rechte der Betroffenen

6. Abschnitt:
Rechtsschutz

7. Abschnitt:
Besondere Verwendungszwecke von Daten

8. Abschnitt:
Straf-, Übergangs- und Schlussbestimmungen

1. Abschnitt
Allgemeine Bestimmungen

§ 1
Sachlicher Geltungsbereich

(1) Dieses Gesetz regelt den Schutz personenbezogener Daten bei nicht automationsunterstützt geführten Dateien, soweit die Verwendung dieser Dateien für Zwecke von Angelegenheiten erfolgt, die in Gesetzgebung Landessache sind.

(2) Dieses Gesetz ist nicht anzuwenden auf die Verwendung personenbezogener Daten durch natürliche Personen für ausschließlich persönliche oder familiäre Tätigkeiten.

§ 2
Räumlicher Geltungsbereich

(1) Dieses Gesetz ist – nach Maßgabe des Abs. 1 - auf die Verwendung von personenbezogenen Daten im Burgenland 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 im Burgenland gelegenen Haupt- oder Zweigniederlassung (§ 3 Z 14) einer Auftraggeberin oder eines Auftraggebers (§ 3 Z 4) geschieht.

(2) Abweichend von Abs. 1 ist das Recht des Sitzstaats der Auftraggeberin oder des Auftraggebers auf eine Datenverarbeitung im Burgenland anzuwenden, wenn eine Auftraggeberin oder ein Auftraggeber des privaten Bereichs

(§ 4 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten im Burgenland zu einem Zweck verwendet, der keiner im Burgenland gelegenen Niederlassung dieser Auftraggeberin oder dieses Auftraggebers zuzurechnen ist.

(3) Weiters ist dieses Gesetz nicht anzuwenden, soweit personenbezogene Daten durch das Burgenland nur hindurchgeführt werden.

§ 3
Begriffsbestimmungen

Im Sinne der Bestimmungen dieses Gesetzes bedeuten die Begriffe:

1. *,,Daten" (,,personenbezogene Daten"):* Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; ,,nur indirekt personenbezogen" sind Daten
   a) für eine Auftraggeberin oder einen Auftraggeber (Z 4),
   b) eine Dienstleisterin oder einen Dienstleister (Z 5) oder
   c) eine Empfängerin oder einen Empfänger einer Übermittlung (Z 12)

   dann, wenn der Personenbezug der Daten derart ist, dass diese Auftraggeberin oder dieser Auftraggeber, diese Dienstleisterin oder dieser Dienstleister oder diese Übermittlungsempfängerin oder dieser Übermittlungsempfänger die Identität der oder des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;
2. *,,sensible Daten" (,,besonders schutzwürdige Daten"):* Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;
3. *,,Betroffene":* alle von der Auftraggeberin oder vom Auftraggeber (Z 4) verschiedene natürlichen oder juristischen Personen oder Personengemeinschaften, deren Daten verwendet (Z 8) werden;

4. *„Auftraggeberinnen“ und „Auftraggeber“":* natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft bzw. die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Z 9), und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Als Auftraggeberinnen oder Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie jemand anderem Daten zur Herstellung eines von ihnen aufgetragenen Werks überlassen und die Auftragnehmerin oder der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten. Wurde jedoch der Auftragnehmerin oder dem Auftragnehmer anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt oder hat die Auftragnehmerin oder 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. 4 eigenverantwortlich zu treffen, so gilt die oder der mit der Herstellung des Werks Betraute als datenschutzrechtliche Auftraggeberin oder datenschutzrechtlicher Auftraggeber;
5. *„Dienstleisterinnen“ und „Dienstleister":* natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft bzw. die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werks überlassen wurden, verwenden (Z 8);
6. *„Datei":* strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;
7. *„Datenanwendung":* die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zwecks der Datenanwendung) geordnet sind;

8. *„Verwenden von Daten":* jede nicht automationsunterstützte Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten;
9. *„Verarbeiten von Daten":* das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch die Auftraggeberin oder den Auftraggeber oder die Dienstleisterin oder den Dienstleister mit Ausnahme des Übermittelns (Z 12) von Daten, soweit diese Schritte nicht automationsunterstützt erfolgen;
10. *„Ermitteln von Daten":* das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden;
11. *„Überlassen von Daten":* die Weitergabe von Daten von der Auftraggeberin oder vom Auftraggeber an eine Dienstleisterin oder einen Dienstleister;
12. *„Übermitteln von Daten":* die Weitergabe von Daten einer Datenanwendung an andere Empfängerinnen oder Empfänger als die Betroffene oder den Betroffenen, die Auftraggeberin oder den Auftraggeber oder eine Dienstleisterin oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet der Auftraggeberin oder des Auftraggebers;
13. *„Zustimmung":* die gültige, insbesondere ohne Zwang abgegebene Willenserklärung der oder des Betroffenen, dass sie oder er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;
14. *„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;

15. *„Datenschutzkommission“:* die nach dem 7. Abschnitt des Datenschutzgesetzes 2000 – DSG 2000, BGBl. I Nr. 165/1999, in der Fassung der Gesetze BGBl. I Nr. 136/2001 und BGBl. I Nr. 13/2005, eingerichtete Datenschutzkommission;
16. *„Datenverarbeitungsregister“:* das nach dem 4. Abschnitt des DSG 2000 eingerichtete Datenverarbeitungsregister.

§ 4
Öffentlicher und privater Bereich

(1) Datenanwendungen sind dem öffentlichen Bereich im Sinne dieses Gesetzes zuzurechnen, wenn sie für Zwecke einer Auftraggeberin oder 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 Auftraggeberinnen und Auftraggeber gelten als Auftraggeberinnen und 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 des § 30 zulässig;
3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;
4. so verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
5. solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

(2) Die Auftraggeberin oder der Auftraggeber trägt bei jeder ihrer oder seiner Datenanwendungen die Verantwortung für die Einhaltung der im Abs. 1 genannten Grundsätze; dies gilt auch dann, wenn sie oder er für die Datenanwendung Dienstleisterinnen oder Dienstleister heranzieht.

(3) Die Auftraggeberin oder der Auftraggeber einer diesem Gesetz unterliegenden Datenanwendung hat, wenn sie oder er nicht im Gebiet der Europäi-

schen Union niedergelassen ist, eine im Burgenland ansässige Vertreterin oder einen im Burgenland ansässigen Vertreter zu benennen, die oder der - unbeschadet der Möglichkeit eines Vorgehens gegen die Auftraggeberin oder den Auftraggeber selbst - namens der Auftraggeberin oder des Auftraggebers verantwortlich gemacht werden kann.

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

§ 6
Zulässigkeit der Verwendung von Daten

(1) Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen der jeweiligen Auftraggeberin oder 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. die Empfängerin oder der Empfänger der oder dem Übermittelnden ihre oder 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 der oder des Betroffenen nicht verletzt werden.

(3) Die Zulässigkeit einer Datenverwendung setzt voraus, dass die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz (§ 1 DSG 2000) nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und dass die Grundsätze des § 5 eingehalten werden.

§ 7
Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten

(1) Gemäß § 1 Abs. 1 DSG 2000 bestehende schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn

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

   die Verwendung erfordern.

(2) Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhal-

tungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung solcher Daten gemäß § 22 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 einer oder eines Dritten erforderlich ist oder
4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeberin oder Auftraggeber und Betroffener oder Betroffenem erforderlich ist oder
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen der Auftraggeberin oder des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
6. ausschließlich die Ausübung einer öffentlichen Funktion durch die Betroffene oder den Betroffenen zum Gegenstand hat oder
7. im Katastrophenfall, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig ist; im letztgenannten Fall gilt § 32 Abs. 3.

(4) Die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verstößt - unbeschadet der Bestimmungen des Abs. 2 - nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen der oder 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 der oder des Betroffenen überwiegenden berechtigten Interessen der Auftraggeberin oder des Auftraggebers ergibt und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen nach diesem Gesetz gewährleistet.

§ 8
Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

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

1. die oder 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 die oder den Betroffenen zum Gegenstand haben, oder

6. die oder der Betroffene ihre oder 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 der oder des Betroffenen notwendig ist und ihre oder seine Zustimmung nicht rechtzeitig eingeholt werden kann oder
8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen anderer Personen notwendig ist oder
9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen der Auftraggeberin oder des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
10. Daten für wissenschaftliche Forschung oder Statistik gemäß § 30 oder zur Benachrichtigung oder Befragung der oder des Betroffenen gemäß § 31 oder im Katastrophenfall gemäß § 32 verwendet werden oder
11. die Verwendung erforderlich ist, um den Rechten und Pflichten der Auftraggeberin oder des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz, BGBl. Nr. 22/1974, zuletzt geändert durch das Gesetz BGBl. I Nr. 8/2005, zustehenden Befugnisse im Hinblick auf die Datenverwendung unberührt bleiben, oder
12. die Verwendung der 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 Tä-

tigkeit 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.

§ 9
Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen

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

(2) Beabsichtigt ein Auftraggeber des öffentlichen Bereichs, eine Dienstleisterin oder einen Dienstleister im Rahmen einer Datenanwendung heranzuziehen, die der Vorabkontrolle gemäß § 15 unterliegt, so hat er dies der Datenschutzkommission mitzuteilen. Dies gilt nicht, wenn der Auftraggeber die Dienstleisterin oder den Dienstleister auf Grund ausdrücklicher gesetzlicher Ermächtigung in Anspruch nimmt oder als Dienstleisterin oder Dienstleister eine Organisationseinheit tätig wird, die mit dem Auftraggeber oder einem diesem übergeordneten Organ in einem Über- oder Unterordnungsverhältnis steht.

(3) Kommt die Datenschutzkommission im Falle des Abs. 2 zur Auffassung, dass die geplante Inanspruchnahme einer Dienstleisterin oder eines

Dienstleisters geeignet ist, schutzwürdige Geheimhaltungsinteressen der Betroffenen zu gefährden, so hat sie dies dem Auftraggeber unverzüglich mitzuteilen. Im Übrigen gilt § 24 Abs. 6 Z 4.

§ 10
Pflichten der Dienstleisterin und des Dienstleisters

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

1. die Daten ausschließlich im Rahmen der Aufträge der Auftraggeberin oder des Auftraggebers zu verwenden; insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag der Auftraggeberin oder des Auftraggebers verboten;
2. alle gemäß § 13 erforderlichen Datensicherheitsmaßnahmen zu treffen; insbesondere dürfen für die Dienstleistung nur solche Mitarbeiterinnen und Mitarbeiter herangezogen werden, die sich der Dienstleisterin oder dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen;
3. weitere Dienstleisterinnen oder Dienstleister nur mit Billigung der Auftraggeberin oder des Auftraggebers heranzuziehen und deshalb die Auftraggeberin oder den Auftraggeber von der beabsichtigten Heranziehung einer weiteren Dienstleisterin oder eines weiteren Dienstleisters so rechtzeitig zu verständigen, dass sie oder er dies allenfalls untersagen kann;
4. - sofern dies nach der Art der Dienstleistung in Frage kommt - im Einvernehmen mit der Auftraggeberin oder dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht der Auftraggeberin oder des Auftraggebers zu schaffen;

5. nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, der Auftraggeberin oder dem Auftraggeber zu übergeben oder in deren oder dessen Auftrag für sie oder ihn weiter aufzubewahren oder zu vernichten;
6. der Auftraggeberin oder 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 der Auftraggeberin oder dem Auftraggeber und der Dienstleisterin oder dem Dienstleister über die nähere Ausgestaltung der im Abs. 1 genannten Pflichten sind zum Zweck der Beweissicherung schriftlich festzuhalten.

§ 11
Genehmigungsfreie Übermittlung und Überlassung von Daten ins Ausland

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

(2) Keiner Genehmigung gemäß § 12 bedarf weiters der Datenverkehr mit Empfängerinnen und Empfängern in Drittstaaten mit angemessenem Datenschutz. Welche Drittstaaten angemessenen Datenschutz gewährleisten, wird durch Verordnung der Landesregierung festgestellt. Diese Verordnung hat Entscheidungen der Europäischen Kommission nach Art. 25 Abs. 6 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Da-

ten und zum freien Warenverkehr, ABl. Nr. L 281 vom 23.11.1995 S. 31, zu beachten und sich – ohne Bindung an diese - an der gemäß § 12 Abs. 2 DSG 2000 erlassenen Verordnung des Bundeskanzlers zu orientieren. Maßgebend für die Angemessenheit des Schutzes sind 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 die Empfängerin oder 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. die oder der Betroffene ohne jeden Zweifel ihre oder seine Zustimmung zur Übermittlung oder Überlassung ihrer oder seiner Daten ins Ausland gegeben hat oder
5. ein von der Auftraggeberin oder vom Auftraggeber mit der oder dem Betroffenen oder mit einer oder einem Dritten eindeutig im Interesse der oder 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) Wenn eine Übermittlung oder Überlassung von Daten ins Ausland in Fällen, die von den vorstehenden Absätzen nicht erfasst sind,

1. zur Wahrung eines wichtigen öffentlichen Interesses oder

2. zur Wahrung eines lebenswichtigen Interesses einer Person

notwendig und so dringlich ist, dass die gemäß § 12 erforderliche Genehmigung der Datenschutzkommission nicht eingeholt werden kann, ohne die genannten Interessen zu gefährden, so darf sie ohne Genehmigung vorgenommen werden, muss aber der Datenschutzkommission umgehend mitgeteilt werden.

(5) Voraussetzung für die Zulässigkeit jeder Übermittlung oder Überlassung ins Ausland ist die Rechtmäßigkeit der Datenanwendung im Inland gemäß § 6. Bei Überlassungen ins Ausland muss darüber hinaus die schriftliche Zusage der ausländischen Dienstleisterin oder des ausländischen Dienstleisters an die inländische Auftraggeberin oder den inländischen Auftraggeber - oder in den Fällen des § 12 Abs. 4 an die inländische Dienstleisterin oder den inländischen Dienstleister - vorliegen, dass sie oder er die Dienstleisterpflichten gemäß § 10 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.

§ 12
Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland

(1) Soweit der Datenverkehr mit dem Ausland nicht gemäß § 11 genehmigungsfrei ist, hat die Auftraggeberin oder der Auftraggeber vor der Übermittlung oder Überlassung von Daten ins 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 zu erteilen, wenn die Voraussetzungen des § 11

Abs. 5 vorliegen und wenn, ungeachtet des Fehlens eines im Empfängerstaat generell geltenden angemessenen Datenschutzniveaus,

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

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

(4) Abweichend von Abs. 1 kann auch eine inländische Dienstleisterin oder ein inländischer Dienstleister die Genehmigung beantragen, wenn sie oder er zur Erfüllung ihrer oder seiner vertraglichen Verpflichtungen gegenüber mehreren Auftraggeberinnen oder Auftraggebern jeweils eine bestimmte weitere Dienstleisterin oder einen bestimmten weiteren Dienstleister im Ausland heranziehen will. Die tatsächliche Überlassung darf jeweils nur mit Zustimmung der Auftraggeberin oder 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 § 11 Abs. 5 nicht entspricht; andernfalls ist die Übermittlung oder Überlassung der Daten ins Ausland zulässig.

3. Abschnitt
Datensicherheit

§ 13
Datensicherheitsmaßnahmen

(1) Für alle Organisationseinheiten

a) einer Auftraggeberin oder eines Auftraggebers oder

b) einer Dienstleisterin oder eines Dienstleisters,

die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der

technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass

1. die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind und
2. ihre Verwendung ordnungsgemäß erfolgt und
3. 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 sowie zwischen den Mitarbeiterinnen und Mitarbeitern ausdrücklich festzulegen;
2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten sowie Mitarbeiterinnen und Mitarbeiter zu binden;
3. alle Mitarbeiterinnen und Mitarbeiter über ihre nach diesem Gesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren;
4. die Zutrittsberechtigung zu den Räumlichkeiten der Auftraggeberin oder des Auftraggebers oder der Dienstleisterin oder des Dienstleisters zu regeln;
5. die Zugriffsberechtigung auf Daten und den Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln;
6. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können;
7. eine Dokumentation über die nach Z 1 bis 6 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleis-

ten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(3) Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck - das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestands - unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, dass es sich um die Verwendung zum Zweck der Verhinderung oder Verfolgung eines Verbrechens nach § 278a des Strafgesetzbuchs, BGBl. Nr. 60/1974, zuletzt geändert durch das Gesetz BGBl. I Nr. 152/2004, (kriminelle Organisation) oder eines Verbrechens mit einer angedrohten Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, handelt.

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

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

§ 14
Datengeheimnis

(1) Auftraggeberinnen und Auftraggeber, Dienstleisterinnen und Dienstleister sowie ihre Mitarbeiterinnen und Mitarbeiter - das sind Arbeitnehmerinnen und Arbeitnehmer (Dienstnehmerinnen und Dienstnehmer) sowie 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) Mitarbeiterinnen und Mitarbeiter dürfen Daten nur auf Grund einer ausdrücklichen Anordnung ihrer Arbeitgeberin oder ihres Arbeitgebers (ihrer Dienstgeberin oder ihres Dienstgebers) übermitteln. Auftraggeberinnen und Auftraggeber (Dienstleisterinnen und Dienstleister) haben, sofern eine solche Verpflichtung ihrer Mitarbeiterinnen und 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 zur Auftraggeberin oder zum Auftraggeber (zur Dienstleisterin oder zum Dienstleister) einhalten werden.

(3) Auftraggeberinnen und Auftraggeber (Dienstleisterinnen 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 Mitarbeiterinnen und Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einer Mitarbeiterin oder 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

§ 15
Vorabkontrolle

(1) Datenanwendungen, die

1. sensible Daten oder
2. strafrechtlich relevante Daten im Sinne des § 7 Abs. 4 enthalten oder
3. die Auskunftserteilung über die Kreditwürdigkeit der oder des 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.

(3) Soweit in diesem Abschnitt nicht ausdrücklich anderes bestimmt wird, sind die Bestimmungen des 4. Abschnitts des DSG 2000 sinngemäß anzuwenden.

§ 16
Verfahren der Vorabkontrolle

(1) Die Auftraggeberin oder der Auftraggeber hat der Datenschutzkommission folgende Angaben über die Datenanwendung zu melden:

1. den Namen (oder die sonstige Bezeichnung) und die Anschrift der Auftraggeberin oder des Auftraggebers sowie einer allfälligen Vertreterin oder eines allfälligen Vertreters gemäß § 5 Abs. 3, weiters die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde;
2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit der Auftraggeberin oder des Auftraggebers, soweit dies erforderlich ist;
3. den Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z 2 ergeben;
4. die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten;
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;
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 § 13, 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 ihre oder seine schutzwürdigen Geheimhaltungsinteressen verletzt sein könnten. Unstimmigkeit liegt insbesondere auch dann vor, wenn der Inhalt einer gemeldeten Datenanwendung durch die gemeldeten 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 der Auftraggeberin oder dem Auftraggeber längstens innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung des Mangels unter Setzung einer angemessenen 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 der Auftraggeberin oder dem Auftraggeber Auflagen für die Vornahme der Datenanwendung mit 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, die sie in Vollziehung der Gesetze durchführen, Parteistellung.

§ 17
Datenverarbeitungsregister

(1) Meldungen gemäß § 16 sind in das Datenverarbeitungsregister einzutragen, wenn

1. das Prüfungsverfahren die Zulässigkeit der Registrierung ergeben hat oder
2. zwei Monate nach Einlangen der Meldung bei der Datenschutzkommission verstrichen sind, ohne dass ein Verbesserungsauftrag gemäß § 16 Abs. 3 erteilt wurde.

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

(2) Der Auftraggeberin oder dem Auftraggeber ist die Durchführung der Registrierung schriftlich in Form eines Registerauszugs mitzuteilen.

(3) Jeder Auftraggeberin und jedem Auftraggeber ist bei der erstmaligen Registrierung eine Registernummer zuzuteilen.

(4) Streichungen und Änderungen im Datenverarbeitungsregister sind auf Antrag der oder des Eingetragenen oder in den Fällen der Abs. 5 und 7 von Amts wegen durchzuführen.

(5) Gelangen der Datenschutzkommission aus amtlichen Verlautbarungen Änderungen in der Bezeichnung oder der Anschrift der Auftraggeberin oder

des Auftraggebers zur Kenntnis, so sind die Eintragungen von Amts wegen zu berichtigen. Ergibt sich aus einer amtlichen Verlautbarung der Wegfall der Rechtsgrundlage der Auftraggeberin oder des Auftraggebers, ist von Amts wegen die Streichung aus dem Register anzuordnen.

(6) Änderungen oder Streichungen nach Abs. 5 sind ohne weiteres Ermittlungsverfahren durch Bescheid zu verfügen.

(7) Werden der Datenschutzkommission andere als die im 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.

(8) Jede Person darf in das Register Einsicht nehmen. In den Registrierungsakt einschließlich darin allenfalls enthaltener Genehmigungsbescheide ist Einsicht zu gewähren, wenn die Einsichtswerberin oder der Einsichtswerber glaubhaft macht, dass sie Betroffene oder er Betroffener ist, und soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen der Auftraggeberin oder des Auftraggebers oder anderer Personen entgegenstehen.

§ 18
Offenlegungspflicht der Auftraggeberin und des Auftraggebers

Auftraggeberinnen und Auftraggeber haben jeder Person auf Anfrage folgende Angaben über ihre Datenanwendungen, die nicht der Vorabkontrolle unterliegen, bekannt zu geben:

1. den Namen (oder die sonstige Bezeichnung) und die Anschrift der Auftraggeberin oder des Auftraggebers sowie einer allfälligen Vertreterin oder eines allfälligen Vertreters gemäß § 5 Abs. 3;
2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit der Auftraggeberin oder des Auftraggebers, soweit dies erforderlich ist;
3. den Zweck der Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z 2 ergeben,
4. die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten sowie
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.

§ 19
Informationspflicht der Auftraggeberin und des Auftraggebers

(1) Auftraggeberinnen und Auftraggeber einer Datenanwendung haben aus Anlass der Ermittlung von Daten die Betroffenen in geeigneter Weise über

1. den Zweck der Datenanwendung, für die die Daten ermittelt werden, und
2. über Namen und Adresse der Auftraggeberin oder des Auftraggebers

zu informieren, sofern diese Informationen der oder 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 der oder des Betroffenen gemäß § 22 besteht oder

2. es für die oder den Betroffenen nach den Umständen des Falls nicht klar erkennbar ist, ob sie oder er zur Beantwortung der an sie oder ihn gestellten Fragen rechtlich verpflichtet ist.

(3) Werden Daten nicht durch Befragung der oder des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten derselben Auftraggeberin oder desselben Auftraggebers oder aus Anwendungen anderer Auftraggeberinnen oder Auftraggeber ermittelt, so 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 Rechte der Betroffenen einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordern würde. Dies liegt insbesondere dann vor, wenn Daten für Zwecke der wissenschaftlichen Forschung oder Statistik gemäß § 30 oder Adressdaten im Rahmen des § 31 ermittelt werden und die Information der oder des Betroffenen in diesen Bestimmungen nicht ausdrücklich vorgeschrieben ist. Die Landesregierung kann durch Verordnung weitere Fälle festlegen, in denen die Pflicht zur Information entfällt.

5. Abschnitt
Rechte der Betroffenen

§ 20
Auskunftsrecht

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

1. die verarbeiteten Daten;
2. die verfügbaren Informationen über ihre Herkunft;
3. allfällige Empfängerinnen oder Empfänger oder Empfängerkreise von Übermittlungen;
4. den Zweck der Datenverwendung sowie
5. die Rechtsgrundlagen hiefür

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

(2) Die Auskunft ist nicht zu erteilen, soweit dies zum Schutz der oder des Betroffenen aus besonderen Gründen notwendig ist oder soweit überwiegende berechtigte Interessen der Auftraggeberin oder des Auftraggebers oder einer oder eines Dritten, insbesondere auch überwiegende öffentliche Interes-

sen, der Auskunftserteilung entgegenstehen. Überwiegende öffentliche Interessen können sich hiebei aus der Notwendigkeit

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

ergeben. Die Zulässigkeit der Auskunftsverweigerung aus den Gründen der Z 1 bis 5 unterliegt der Kontrolle durch die Datenschutzkommission.

(3) Die oder der Betroffene hat am Auskunftsverfahren über Befragung in dem ihr oder ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand bei der Auftraggeberin oder beim Auftraggeber zu vermeiden.

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

(5) Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn die oder der Betroffene im laufenden Jahr noch kein Auskunftsersuchen an die Auftraggeberin oder den Auftraggeber zum selben Aufgabengebiet gestellt hat. In allen anderen Fällen kann ein pauschalierter Kostenersatz von 18,89 Euro verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprü-

che zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.

(6) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf die Auftraggeberin oder der Auftraggeber Daten über die Betroffene oder den Betroffenen innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 25 an die Datenschutzkommission bis zum rechtskräftigen Abschluss des Verfahrens nicht vernichten.

(7) Soweit Datenanwendungen von Gesetzes wegen öffentlich einsehbar sind, hat die oder 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 jeweilige öffentliche Buch oder Register einrichtenden Gesetze.

(8) Im Falle der auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 5 Abs. 4 eigenverantwortlichen Entscheidung über die Durchführung einer Datenanwendung durch eine Auftragnehmerin oder einen Auftragnehmer gemäß § 3 Z 4 dritter Satz kann die oder der Betroffene das Auskunftsbegehren zunächst auch an die Person richten, welche die Herstellung des Werks aufgetragen hat. Diese hat der oder dem Betroffenen, soweit dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse der eigenverantwortlichen Auftragnehmerin oder des eigenverantwortlichen Auftragnehmers mitzuteilen, damit die oder der Betroffene das Auskunftsrecht gegen diese Person gemäß Abs. 1 geltend machen kann.

§ 21
Recht auf Richtigstellung oder Löschung

(1) Alle Auftraggeberinnen und Auftraggeber haben unrichtige oder entgegen den Bestimmungen dieses Gesetzes verarbeitete Daten richtig zu stellen oder zu löschen, und zwar

1. aus Eigenem, sobald ihnen die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder
2. auf begründeten Antrag der oder 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 § 30.

(5) Der Beweis der Richtigkeit der Daten obliegt - sofern gesetzlich nicht ausdrücklich anderes angeordnet ist – der Auftraggeberin oder dem Auftraggeber, soweit die Daten nicht ausschließlich auf Grund von Angaben der oder 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 eines Antrags auf Richtigstellung oder Löschung ist dem Antrag zu entsprechen und der oder dem Betroffenen davon Mitteilung zu machen oder schriftlich zu begründen, warum die verlangte Löschung oder Richtigstellung nicht vorgenommen wird.

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

§ 22
Widerspruchsrecht

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

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

§ 23
Rechte der Betroffenen bei der Verwendung nur indirekt personenbezogener Daten

Die durch die §§ 20 bis 22 gewährten Rechte können nicht geltend gemacht werden, soweit nur indirekt personenbezogene Daten verwendet werden.

6. Abschnitt
Rechtsschutz

§ 24
Kontrollbefugnisse der Datenschutzkommission

(1) Jede Person kann sich wegen einer behaupteten Verletzung ihrer Rechte oder sie betreffende Pflichten einer Auftraggeberin oder eines Auftraggebers (einer Dienstleisterin oder eines Dienstleisters) nach diesem Gesetz mit einer Eingabe an die Datenschutzkommission wenden.

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

(3) Datenanwendungen, die der Vorabkontrolle gemäß § 15 unterliegen, dürfen auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden.

(4) Zum Zweck der Einschau ist die Datenschutzkommission nach Verständigung der Inhaberin oder des Inhabers der Räumlichkeiten und der Auftraggeberin oder des Auftraggebers (der Dienstleisterin oder des Dienstleisters) berechtigt, Räume, in denen Datenanwendungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzu-

stellen. Die Auftraggeberin oder der Auftraggeber (die Dienstleisterin oder der Dienstleister) hat die für die Einschau notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte der Auftraggeberin oder des Auftraggebers (der Dienstleisterin oder des 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; dies allerdings mit der Maßgabe, dass dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach § 33 dieses Gesetzes oder eines Verbrechens nach § 278a des Strafgesetzbuchs, BGBl. Nr. 60/1974, zuletzt geändert durch das Gesetz BGBl. I Nr. 152/2004, (kriminelle Organisation) oder eines Verbrechens mit einer angedrohten Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher strafbarer Handlungen auch dem Ersuchen der Strafgerichte nach § 26 der Strafprozessordnung, BGBl. Nr. 631/1975, zuletzt geändert durch das Gesetz BGBl. I Nr. 164/2004, zu entsprechen ist.

(6) Zur Herstellung des rechtmäßigen Zustands 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 § 17 Abs. 7 einleiten oder
2. Anzeige nach § 33 erstatten oder

3. bei schwerwiegenden Verstößen durch Auftraggeberinnen oder Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 26 Abs. 5 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) Die einschreitende Person ist darüber zu informieren, wie mit ihrer Eingabe verfahren wurde.

§ 25
Beschwerde an die Datenschutzkommission

(1) Die Datenschutzkommission erkennt auf Antrag der oder des Betroffenen über behauptete Verletzungen des Rechts auf Auskunft gemäß § 20 durch die Auftraggeberin oder den Auftraggeber einer Datenanwendung, soweit sich das Auskunftsbegehren nicht auf die Verwendung von Daten für Akte der Gesetzgebung oder der Gerichtsbarkeit bezieht.

(2) Zur Entscheidung über behauptete Verletzungen der Rechte einer oder eines Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung nach diesem Gesetz ist die Datenschutzkommission dann zuständig, wenn die oder der Betroffene eine 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 – der Auftraggeberin oder dem Auftraggeber die Anbringung eines Bestreitungsvermerks auftragen.

§ 26
Anrufung der Gerichte

(1) Ansprüche gegen Auftraggeberinnen oder Auftraggeber des privaten Bereichs wegen Verletzung der Rechte der oder des Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung sind von der oder dem Betroffenen auf dem Zivilrechtsweg geltend zu machen.

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

(3) Zur Sicherung der auf dieses Gesetz gestützten Ansprüche auf Unterlassung können einstweilige Verfügungen erlassen werden, auch wenn die im § 381 der Exekutionsordnung, RGBl. Nr. 79/1896, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 151/2004, bezeichneten Voraussetzungen nicht erfüllt sind. 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 Gerichts-

barkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel die oder der Betroffene den gewöhnlichen Aufenthalt oder Sitz hat. Klagen von Betroffenen können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel die Auftraggeberin oder der Auftraggeber (die Dienstleisterin oder der Dienstleister) den gewöhnlichen Aufenthalt oder Sitz hat.

(5) Die Datenschutzkommission hat in Fällen, in denen der begründete Verdacht einer schwerwiegenden Datenschutzverletzung durch eine Auftraggeberin oder einen Auftraggeber des privaten Bereichs besteht, gegen diese oder diesen eine Feststellungsklage (§ 228 der Zivilprozessordnung - ZPO, RGBl. Nr. 113/1895, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 151/2004) beim zuständigen Gericht zu erheben.

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

§ 27
Schadenersatz

(1) Auftraggeberinnen oder Auftraggeber (Dienstleisterinnen oder Dienstleister), die Daten schuldhaft entgegen den Bestimmungen dieses Gesetzes verwenden, haben dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen.

(2) Werden durch die öffentlich zugängliche Verwendung von

1. sensiblen Daten oder

2. strafrechtlich relevanten Daten im Sinne des § 7 Abs. 4 oder
3. Daten, die die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben,

schutzwürdige Geheimhaltungsinteressen einer oder eines Betroffenen in einer Weise verletzt, die einer Eignung zur Bloßstellung gemäß § 7 Abs. 1 des Mediengesetzes, BGBl. Nr. 314/1981, zuletzt geändert durch das Gesetz BGBl. I Nr. 136/2001, gleichkommt, so gilt diese Bestimmung auch in Fällen, in denen die öffentlich zugängliche Verwendung nicht in Form der Veröffentlichung in einem Medium geschieht. Der Anspruch auf angemessene Entschädigung für die erlittene Kränkung ist gegen die Auftraggeberin oder den Auftraggeber der Datenverwendung geltend zu machen.

(3) Die Auftraggeberinnen und Auftraggeber (Dienstleisterinnen und Dienstleister) haften auch für das Verschulden ihrer Leute, soweit deren Tätigkeit für den Schaden ursächlich war.

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

(5) Die Zuständigkeit für Klagen nach Abs. 1 richtet sich nach § 26 Abs. 4.

§ 28
Gemeinsame Bestimmungen

(1) Der Anspruch auf Behandlung einer Eingabe nach § 24, einer Beschwerde nach § 25 oder einer Klage nach § 26 erlischt, wenn die einschreitende Person sie nicht binnen eines Jahres, nachdem sie Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, einbringt. Dies ist der einschreitenden Person im Falle einer verspäteten Eingabe gemäß § 24 mitzuteilen; verspätete Beschwerden nach § 25 und Klagen nach § 26 sind abzuweisen.

(2) Eingaben nach § 24, Beschwerden nach § 25, Klagen nach § 26 sowie Schadenersatzansprüche nach § 27 können nicht nur auf die Verletzung der Vorschriften dieses Gesetzes, sondern auch auf die Verletzung von datenschutzrechtlichen Vorschriften eines anderen Mitgliedstaats der Europäischen Union gegründet werden, soweit solche Vorschriften gemäß § 2 im Burgenland anzuwenden sind.

(3) Ist die vermutete Verletzung schutzwürdiger Geheimhaltungsinteressen einer oder eines Betroffenen im Burgenland 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.

§ 29
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 Verwaltungsgerichtshofs durch die Parteien des Verfahrens ist zulässig. Dies gilt auch für die in Vollziehung der Gesetze tätigen Auftraggeberinnen und Auftraggeber des öffentlichen Bereichs in jenen Fällen, in denen ihnen gemäß § 12 Abs. 3 oder § 16 Abs. 8 Parteistellung zukommt oder durch Gesetz ausdrücklich ein Beschwerderecht an den Verwaltungsgerichtshof eingeräumt wurde.

(2) Bescheide, mit denen gemäß § 12 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 Verwendungszwecke von Daten

§ 30
Wissenschaftliche Forschung und Statistik

(1) Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, dürfen Auftraggeberinnen und Auftraggeber von Untersuchungen alle Daten verwenden, die

1. öffentlich zugänglich sind oder
2. die Auftraggeberin oder der Auftraggeber für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für die Auftraggeberin oder 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 der oder des Betroffenen oder
3. mit Genehmigung der Datenschutzkommission gemäß Abs. 3 verwendet werden.

(3) Eine Genehmigung der Datenschutzkommission zur 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 erfordern würde und
2. ein öffentliches Interesse an der beantragten Verwendung besteht und
3. die fachliche Eignung der Antragstellerin oder 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 bei der Empfängerin oder beim Empfänger nur von solchen Personen verwendet werden, die hinsichtlich des Gegenstands der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist. Die Datenschutzkomission 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 denen gemäß den vorstehenden Absätzen die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der direkte Personenbezug 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 Personenbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

§ 31
Zur-Verfügung-Stellung von Adressen für die 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, sofern

1. Daten derselben Auftraggeberin oder 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) die oder 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 der 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 die Antragstellerin oder der Antragsteller das Vorliegen der im 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 denen es gemäß den vorstehenden Absätzen 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.

§ 32
Verwendung von Daten im Katastrophenfall

(1) Auftraggeber des öffentlichen Bereiches sind im Katastrophenfall ermächtigt, Daten zu verwenden, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig ist. Zu diesem Zweck sind auch Hilfsorganisationen (Abs. 6) nach Maß-

gabe der ihnen zukommenden Aufgaben und rechtlichen Befugnis ermächtigt, Daten zu verwenden. Wer rechtmäßig über Daten verfügt, darf diese an Auftraggeber des öffentlichen Bereiches und Hilfsorganisationen übermitteln, sofern diese die Daten zur Bewältigung der Katastrophe für die genannten Zwecke benötigen. Die Daten sind unverzüglich zu löschen, wenn sie für die Erfüllung des konkreten Zwecks nicht mehr benötigt werden.

(2) Eine Überlassung oder Übermittlung von Daten in das Ausland ist zulässig, soweit dies für die Erfüllung der in Abs. 1 genannten Zwecke notwendig ist. Daten, die für sich allein den Betroffenen strafrechtlich belasten, dürfen nicht übermittelt werden, es sei denn, dass diese zur Identifizierung im Einzelfall unbedingt notwendig sind. Die Übermittlung von Daten Angehöriger darf nur in pseudonymisierter Form erfolgen. Daten dürfen in Staaten ohne angemessenes Datenschutzniveau nur übermittelt oder überlassen werden, wenn der Auftraggeber auf Grund schriftlicher Vereinbarungen mit der Empfängerin oder dem Empfänger oder auf Grund schriftlicher Zusagen der Empfängerin oder des Empfängers oder, wenn dies nach den Umständen nicht oder nicht in angemessener Zeit möglich ist, durch Erteilung von Auflagen an die Empfängerin oder den Empfänger davon ausgehen kann, dass die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Eine Übermittlung oder Überlassung hat dann zu unterbleiben, wenn Grund zur Annahme besteht, dass die Empfängerin oder der Empfänger nicht für den gebotenen Schutz der Geheimhaltungsinteressen der Betroffenen Sorge tragen oder ausdrückliche datenschutzrechtliche Auflagen des Auftraggebers missachten werde. Während der Dauer der Katastrophensituation entfällt im Hinblick auf § 11 Abs. 3 Z 3 die Genehmigungspflicht. Die Datenschutzkommission ist von den veranlassten Übermittlungen und Überlassungen und den näheren Umständen des Anlass gebenden Sachverhaltes jedoch unverzüglich zu verständigen. Die Datenschutzkommission kann zum Schutz der Betroffenenrechte Datenübermittlungen oder -überlassungen untersagen, wenn der durch die Datenweitergabe bewirkte Ein-

griff in das Grundrecht auf Datenschutz durch die besonderen Umstände der Katastrophensituation nicht gerechtfertigt ist.

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

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

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

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

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

(6) Eine Hilfsorganisation im Sinne dieser Bestimmung ist eine allgemein anerkannte gemeinnützige Organisation, die statuten- oder satzungsgemäß das Ziel hat, Menschen in Notsituationen zu unterstützen und von der angenommen werden kann, dass sie in wesentlichem Ausmaß eine Hilfeleistung im Katastrophenfall erbringen kann.

(7) Alle Datenverwendungen sind im Sinne des § 13 Abs. 2 Z 6 zu protokollieren.

(8) Die Zulässigkeit von Datenverwendungen auf der Grundlage anderer in den §§ 7 und 8 genannter Tatbestände bleibt unberührt.

§ 33
Datenanwendungen des Landtages

Die Präsidentin oder der Präsident des Landtages ist Auftraggeberin oder Auftraggeber jener Datenanwendungen, die für Zwecke der ihr oder ihm gemäß § 14 der Geschäftsordnung des Landtages, LGBl. Nr. 47/1981, in der jeweils geltenden Fassung, übertragenen Angelegenheiten durchgeführt werden. Übermittlungen von Daten aus solchen Datenanwendungen dürfen nur über Auftrag der Präsidentin oder des Präsidenten des Landtages vorgenommen werden. Die Präsidentin oder der Präsident hat Vorsorge dafür zu treffen,

dass im Falle eines Übermittlungsauftrags die Voraussetzungen des § 6 Abs. 2 vorliegen und insbesondere die Zustimmung der oder des Betroffenen in jenen Fällen eingeholt wird, in denen dies gemäß § 6 Abs. 2 mangels einer anderen Rechtsgrundlage für die Übermittlung notwendig ist.

8. Abschnitt
Straf-, Übergangs- und Schlussbestimmungen

§ 34
Strafbestimmungen

(1) Personen, die

3. sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschaffen oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhalten oder
4. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 14) übermitteln, insbesondere Daten, die ihnen gemäß § 30 oder § 31 anvertraut wurden, vorsätzlich für andere Zwecke verwenden, oder
5. Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwenden, zu ihnen keine Auskunft erteilen, nicht richtig stellen oder nicht löschen oder
6. Daten vorsätzlich entgegen § 20 Abs. 6 löschen oder
7. sich unter Vortäuschung falscher Tatsachen vorsätzlich Daten gemäß § 32 verschaffen

begehen eine Verwaltungsübertretung und sind, 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, mit Geldstrafe bis zu 20.000 Euro zu bestrafen.

(2) Personen, die

1. Daten ohne Vorabkontrolle gemäß § 15 ermitteln, verarbeiten oder übermitteln,
2. Daten ins Ausland übermitteln oder überlassen, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 12 eingeholt zu haben, oder
3. entgegen einer Empfehlung der Datenschutzkommission ihre Offenlegungs- oder Informationspflicht gemäß § 18 oder § 19 verletzen oder
4. die gemäß § 13 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht lassen,

begehen eine Verwaltungsübertretung und sind, 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, mit Geldstrafe bis zu 10.000 Euro zu bestrafen.

(3) Der Versuch ist strafbar.

(4) Die Strafe des Verfalls von Datenträgern und Programmen kann ausgesprochen werden (§§ 10, 17 und 18 des Verwaltungsstrafgesetzes 1991, BGBl. Nr 52/1991, zuletzt geändert durch das Gesetz BGBl. I Nr. 117/2002), 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 die Auftraggeberin oder der Auftraggeber (die Dienstleisterin oder der Dienstleister) den gewöhnlichen Aufenthalt oder Sitz hat. Falls ein solcher im Burgenland nicht gegeben ist, ist die Bezirkshauptmannschaft Eisenstadt-Umgebung 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 im Art. 8 Abs. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr, ABl. Nr. L 281 S. 31, 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 § 12 Abs. 2 Z 1 nicht als erfüllt erachtet wurden, sowie
2. der Datenverkehr in ein Drittland ohne angemessenes Datenschutzniveau genehmigt wurde, weil die Voraussetzungen des § 12 Abs. 2 Z 2 als erfüllt erachtet wurden.

§ 36

Anhörungsverfahren

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

§ 37
Befreiung von Verwaltungsabgaben

Für Amtshandlungen, die auf durch dieses Gesetz unmittelbar veranlassten Eingaben der Betroffenen zur Wahrung ihrer Interessen beruhen, sind keine Verwaltungsabgaben des Landes zu entrichten.

§ 38
Übergangsbestimmungen

(1) Die Verarbeitungen von Daten, die zum Zeitpunkt des Inkrafttretens dieses Gesetzes in manuellen Dateien vorhanden sind, sind

1. bis zum 1. Oktober 2007 mit den §§ 5 bis 8 dieses Gesetzes sowie
2. innerhalb von zwei Jahren nach In-Kraft-Treten dieses Gesetzes mit dessen übrigen Bestimmungen

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 begehren, die unvollständig oder unzutreffend sind oder auf eine Art und Weise aufbewahrt werden, die mit den rechtmäßigen Zwecken unvereinbar sind, die von dem für die Verarbeitung Verantwortlichen verfolgt werden.

§ 39
Umsetzung von Gemeinschaftsrecht

Dieses Gesetz ergeht in Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürli-

cher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr, ABl. Nr. L 281 vom 23.11.1995 S. 31.

Vorblatt

1. Problem:

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 erfordert eine Umsetzung ins innerstaatliche Recht. Kompetenzrechtlich ist zu dieser Umsetzung für den Bereich manuell (nicht automationsunterstützt) verarbeiteter Daten, soweit es sich jeweils um Sachmaterien handelt, die der Gesetzgebungszuständigkeit des Landes unterliegen, der Landesgesetzgeber zuständig.

2. Lösung:

Erlassung eines Burgenländischen Datenschutzgesetzes mit dem Inhalt der Umsetzung der genannten Richtlinie für den Bereich des Burgenlandes im Rahmen dessen Gesetzgebungskompetenz.

3. Alternativen:

Im Hinblick auf die dargestellten gemeinschaftsrechtlichen Erfordernisse und verfassungs(kompetenz)rechtlichen Rahmenbedingungen: Keine.

4. EU-Konformität:

Gegeben, da Richtlinienumsetzung.

5. Kosten:

Die durch den Vollzug des vorliegenden Gesetzentwurfs entstehenden Kosten sind ausschließlich gemeinschaftsrechtlich bedingt (s. die oben genannte Richtlinie, deren Umsetzung dieser Entwurf dient).

Im Bereich der Landes- und Gemeindeverwaltung werden die zusätzlichen Kosten, die durch die Einbeziehung der händisch geführten Dateien in das

Datenschutzrecht (Registrierung, Auskunfts-, Richtigstellungs- und Löschungspflichten) entstehen, im Hinblick auf die weitgehende Führung von Dateien in diesen Bereichen im automationsunterstützten Wege nur geringfügig sein. Es ist auch zu beachten, dass diesen (manuell geführten) Dateien in Zukunft noch geringere Bedeutung zukommen wird, als sie sie derzeit schon haben. Dies gilt auch hinsichtlich der durch allfällige Strafverfahren erwachsenden Aufwände.

Im privaten Bereich wird der zusätzliche Aufwand nur dort von größerer Bedeutung sein können, wo traditionellerweise umfangreiche personenbezogene Dateien mit sensiblen Daten geführt werden. Da jedoch allgemein die händisch geführten Dateien immer geringere Bedeutung haben werden, wird der vorliegende Gesetzentwurf auch hier keine ins Gewicht fallenden Kosten verursachen.

Was den zusätzlichen Aufwand der Registrierung von manuell geführten Datenanwendungen beim Datenverarbeitungsregister des Bundes betrifft, kann auf die Ausführungen in der Regierungsvorlage zum Datenschutzgesetz 2002 des Bundes hingewiesen werden; demnach ist in diesem Zusammenhang mit keinen nennenswerten Kosten zu rechnen. In gleicher Weise dürften nach den Ausführungen in dieser Regierungsvorlage auch der Datenschutzkommission durch die Ausdehnung ihrer Kompetenzen auf die händisch geführten Dateien keine ins Gewicht fallenden Kosten erwachsen.

6. Besonderheiten des Normsetzungsverfahrens:

Die Bestimmungen der §§ 9, 11, 12, 15 bis 17, 20, 21, 24 bis 26 sowie 28 bis 31 enthalten Regelungen über die Mitwirkung eines Bundesorgans (der Datenschutzkommission) bei der Vollziehung des vorliegenden Gesetzentwurfs und bedürfen daher (nach Beschlussfassung durch den Landtag) gemäß Art. 97 Abs. 2 B-VG der Zustimmung der Bundesregierung.

E r l ä u t e r u n g e n

A) Allgemeiner Teil:

1.

Am 24. Oktober 1995 wurde die *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* (im folgenden kurz als „Datenschutzrichtlinie“ bezeichnet) verabschiedet; die innerstaatlich umzusetzen ist.

Ziel dieser Richtlinie ist die *Harmonisierung der Datenschutzvorschriften* der Mitgliedstaaten der Europäischen Union. Dies ist die Voraussetzung dafür, dass in Hinkunft kein Mitgliedstaat mehr den grenzüberschreitenden Datenverkehr innerhalb des EU-Gebiets im Interesse des Datenschutzes besonderen Prüfungen oder Genehmigungen unterwerfen darf. Das EU-Gebiet soll auch im Hinblick auf die Kommunikation personenbezogener Daten ein Raum sein, in dem der freie Verkehr von Daten im Hinblick auf das Funktionieren des Binnenmarkts durch nationale Grenzen nicht behindert wird bei gleichzeitiger Wahrung des Schutzes der Grundrechte.

2.

Mit dem vorliegenden Gesetzentwurf soll die Datenschutzrichtlinie im Bereich der Gesetzgebungszuständigkeit des Landes umgesetzt werden. Dazu ist Folgendes zu bemerken:

Das österreichische Datenschutzrecht erstreckte sich ursprünglich lediglich auf den Schutz personenbezogener Daten im *automationsunterstützten* Datenverkehr. Diese Angelegenheit wurde bundeseinheitlich durch das Datenschutzgesetz des Bundes aus dem Jahr 1978 geregelt. Die Kompetenzgrundlage zu Gunsten des Bundes ergab sich aus der Verfassungsbestimmung des Art. 1 dieses Gesetzes. Für die *nicht automationsunterstützt* geführten Dateien (händisch geführte Karteien und Ähnliches) bestanden weder im Bundes- noch im Landesbereich konkrete gesetzli-

che Vorgaben. Hinsichtlich der Verwendung dieser Daten in der Verwaltung waren jedoch jedenfalls die Bestimmungen der Bundesverfassung (Art. 20 Abs. 3 B-VG) und der Landesverfassung (Art. 62 L-VG) sowie des Dienstrechts der Landes- und Gemeindebediensteten über die Amtsverschwiegenheit zu beachten.

Die *Datenschutzrichtlinie* bezieht nunmehr *auch* die Verarbeitung personenbezogener Daten in *händisch* geführten Dateien in den Datenschutz mit ein. Aus diesem Grund war eine Anpassung des österreichischen Datenschutzrechts erforderlich, die auf *Bundesebene* mit dem *Datenschutzgesetz 2000*, BGBl.I Nr. 165/1999, erfolgt ist. Dieses Gesetz hat an der bisherigen Kompetenzgrundlage nichts geändert: Der Bundesgesetzgeber ist demnach weiterhin für den Bereich des Schutzes der *automationsunterstützt* verarbeiteten Daten (Art. 1 § 2 Datenschutzgesetz 2000) zuständig. Im Bereich der *manuell* strukturierten Dateien ist der Bund so weit zuständig, als ihm die *Gesetzgebungskompetenz in der jeweiligen Sachmaterie* zukommt.

Eine Zuständigkeit des *Landesgesetzgebers* besteht daher zur Regelung des Datenschutzes bei *händisch* geführten Dateien *im selbständigen Wirkungsbereich gemäß Art. 15 Abs. 1 B-VG*. Schließlich besteht eine Zuständigkeit des Landes in den Angelegenheiten des *Art. 12 B-VG*, wobei jedoch der Bund von seiner Befugnis zur Grundsatzgesetzgebung Gebrauch machen kann.

3.

Mit dem vorliegenden Gesetzentwurf soll, wie dargelegt, der genannten gemeinschaftsrechtlichen Umsetzungsverpflichtung für den Bereich der Gesetzgebungszuständigkeit des Burgenlandes Rechnung getragen werden. Im Interesse einer möglichst weitgehenden Harmonisierung des Datenschutzrechts in Österreich übernimmt dieser Entwurf – wie dies auch andere Bundesländer handhaben - *weitgehend den Inhalt des Datenschutzgesetzes 2000 des Bundes*. *Abweichungen* vom Bundesrecht ergeben sich dort, wo *kein Anwendungsfall* für die Regelungen des Bundes denkbar ist (z.B. hinsichtlich der Bestimmungen des Datenschutzgesetzes 2000, die nur die automationsunterstützte Verarbeitung von Daten betreffen), eine Übernahme aus *kompetenzrechtlichen* Gründen nicht in Betracht kommt oder die Abweichung aus *anderen Gründen* geboten ist (z.B. um dem unterschiedlichen terri-

torialen Geltungsbereich Rechnung zu tragen; Ersetzung der Zuständigkeiten des. Bundeskanzlers durch diejenige der Landesregierung). Nicht übernommen wurde - dem Art. 3 Abs. 2 der Datenschutzrichtlinie entsprechend - insbesondere die Bestimmung des § 45 des Datenschutzgesetzes 2000 über die Anwendung des Gesetzes auf für *private Zwecke* verarbeitete Daten, da es fraglich wäre, ob der mit der Durchsetzung von Datenschutzregeln in diesem Bereich verbundene Aufwand den Nutzen rechtfertigen könnte.

Im vorliegenden Entwurf wurde *nicht* – wie in einigen anderen Bundesländern – der Weg eines *bloßen Verweises* auf die sinngemäß anzuwendenden Bestimmungen des Datenschutzgesetzes 2000 des Bundes (mit den jeweiligen Ausnahmen) gewählt, da diese legistische Vorgangsweise für die Leserinnen und Leser des Gesetzes das Erfordernis einer unzweckmäßigen Heranziehung sowohl des Textes des Landesgesetzes als auch des Bundesgesetzes nach sich ziehen würde. Vielmehr werden im Entwurf die für die Übernahme ins Landesrecht in Betracht kommenden Regelungen dieses Bundesgesetzes – mit den erforderlichen Anpassungen für das Landesrecht - *weitestgehend ihrem Wortlaut nach übernommen*, was im Übrigen der Gewährleistung einer korrekten Umsetzung der Datenschutzrichtlinie dienlich ist. Mag sich dadurch – im Vergleich zu bloß pauschalen Verweisen auf die bundesgesetzlichen Regelungen, was zum gleichen Norminhalt wie die hier gewählte Vorgangsweise führt – auch der Umfang des Gesetzestextes nicht unwesentlich erhöhen, so ist diesbezüglich doch dem Gesichtspunkt der *besseren Lesbarkeit und Übersichtlichkeit und somit Benutzerfreundlichkeit im Dienste eines einfacheren Zugangs zum Normtext durch ein in sich abgeschlossenes Gesetzeswerk* höheres Gewicht beizumessen.

4.

Im Interesse der Harmonisierung des Datenschutzrechts wurde darauf *verzichtet*, für die *Registrierung* der manuell geführten Datenanwendungen oder die Aufgaben des *Rechtsschutzes und der Kontrolle* *eigene Landesbehörden* einzurichten oder den *Unabhängigen Verwaltungssenat* mit diesen Aufgaben zu betrauen. Vielmehr soll – wie dies auch in anderen Landesgesetzen vorgesehen ist – die *Datenschutzkommission des Bundes* auch im Landesbereich die inhaltlich gleich gela-

gerten Aufgaben wahrnehmen, die ihr durch das Datenschutzgesetz 2000 übertragen sind. Dies gilt auch hinsichtlich der Registrierungspflichten in dem bei der Datenschutzkommission eingerichteten *Datenverarbeitungsregister*. In verfassungsrechtlicher Hinsicht handelt es sich dabei um eine Mitwirkung von Bundesorganen an der Vollziehung des Landes, die gemäß Art. 97 Abs. 2 B-VG (nach Beschlussfassung durch den Landtag) der Zustimmung der Bundesregierung bedarf; für andere Landesgesetze wurde eine solche Zustimmung erteilt.

B) Besonderer Teil:

Zu § 1 (Sachlicher Geltungsbereich):

Abs. 1 grenzt den Gegenstand der Regelungen des vorliegenden Gesetzesentwurfs im Sinne der im Allgemeinen Teil der Erläuterungen (P. 2.) dargelegten verfassungs-(kompetenz-)rechtlichen Vorgaben ab.

Die im *Abs. 2* enthaltene Ausnahme vom Geltungsbereich dieses Entwurfs betreffend für private Zwecke verarbeitete Daten beruht auf Art. 3 Abs. 2 der Datenschutzrichtlinie, wonach diese Richtlinie keine Anwendung auf die Verarbeitung personenbezogener Daten findet, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird. Die Verwendung, d.h. das Verarbeiten und auch das Übermitteln solcher Daten, unterliegt keiner Regelung und ist daher nach Maßgabe des Regelungsgegenstands des vorliegenden Gesetzesentwurfs erlaubt. *Nicht übernommen* wurde somit die Bestimmung des § 45 des Datenschutzgesetzes 2000 über die Anwendung des Gesetzes auf für *private Zwecke* verarbeitete Daten, da es fraglich wäre, ob der mit der Durchsetzung von Datenschutzregeln in diesem Bereich verbundene Aufwand den Nutzen rechtfertigen könnte.

Zu § 2 (Räumlicher Geltungsbereich):

In Entsprechung des Art. 4 der Datenschutzrichtlinie (und § 3 Abs. 1 des Datenschutzgesetzes 2000 – mit der Maßgabe der Einschränkung auf das Landesgebiet - folgend) wird der räumliche Geltungsbereich des vorliegenden Gesetzentwurfs im *Abs.* 1 so definiert, dass der Entwurf grundsätzlich auf jede Datenverwendung im Burgenland anzuwenden ist.

Ausnahmen bestehen gemäß *Abs. 2* (analog § 3 Abs. 2 des Datenschutzgesetzes 2000) zugunsten des Sitzstaatsprinzips**,** das im Gemeinschaftsrecht angesichts der Dienstleistungsfreiheit eine gerne verwendete Kollisionsregel darstellt. Diese Ausnahme gilt dann, wenn Daten in Österreich für eine Auftraggeberin oder einen Auftraggeber aus einem anderen EU-Staat verarbeitet werden, ohne dass die Auftraggeberin oder der Auftraggeber (die oder der den Sitz in einem anderen EU-Staat hat) eine feste Betriebsstätte ("Niederlassung" im Sinne des § 3 Z 14) im Burgenland hätte. Umgekehrt gilt österreichisches Datenschutzrecht in einem anderen EU-Staat dann, wenn ein österreichischer Rechtsträger Datenverarbeitung im EU-Ausland betreibt, ohne dass er für die Verfolgung seiner Interessen dort eine "Niederlassung" (im Sinne des § 3 Z 14) besitzt.

Während der Ort der Niederlassung der Auftraggeberin oder des Auftraggebers der maßgebliche Anknüpfungspunkt für die Frage des anwendbaren Rechts ist, soweit es sich um Datenanwendungen für einen Rechtsträger mit Sitz in einem EU-Mitgliedstaat handelt, gilt bei Datenanwendungen für Zwecke eines Rechtsträgers, der keinen Sitz in einem EU-Mitgliedstaat hat, immer der Ort der Datenverwendung als Anknüpfungspunkt für die Anwendbarkeit einer nationalen Rechtsordnung (Art. 4 Abs. 1 lit. c der Datenschutzrichtlinie).

Zu § 3 (Begriffsbestimmungen):

Im Interesse einer weitestgehenden Harmonisierung von Bundes- und Landesdatenschutzrecht werden die im vorliegenden Gesetzentwurf verwendeten Begriffe grundsätzlich in der im § 4 des Datenschutzgesetzes 2000 festgelegten Bedeu-

tung definiert; Abweichungen davon sind dort notwendig, wo – dem Regelungsgegenstand dieses Entwurfs entsprechend – eine Einschränkung auf nicht automationsunterstützt verarbeitete Daten zu erfolgen hatte.

Unter den Begriff „Datei“ (*Z 6*) fallen manuelle Daten in strukturierter Form, die nach mindestens einem Suchkriterium zugänglich sind. So ist z.B. eine Handkartei, die nach aufsteigenden Nummern oder Namen geordnet ist, eine Datei im Sinne des vorliegenden Entwurfs.

Nach dem Erwägungsgrund 27 der Datenschutz-Richtlinie fallen Akten und Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien strukturiert sind, nicht unter diesen Dateibegriff. Das bedeutet jedoch andererseits, dass z.B. strukturierte Deckblätter bei Personalakten, die in einer Hängeregistratur alphabetisch oder nach Personalnummer abgelegt werden, als Datei iSd Entwurfs zu betrachten sind.

Auch nach der Rechtsprechung stellt ein Papierakt an sich noch keine „Datei“ dar, da er zwar in der Regel nach einem Suchbegriff (Geschäftszahl) geordnet aufbewahrt wird, der einzelne Akt selbst hingegen keinen geordneten Inhalt hat (DSK 10.11.2000, GZ 120.707/7-DSK/00; OGH 28.6.2000, 6 Ob 148/00h; aM allerdings *Dohr/Pollirer/Weiss*, DSG^2 Anm 7 zu § 4, die zwischen Akt und strukturiertem Akt unterscheiden).

Zum Begriff „Datenanwendung“ (Z 7) kann Folgendes ausgeführt werden: § 4 Z 7 des Datenschutzgesetzes 2000 definiert eine „Datenanwendung“ als Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (§ 4 Z 8 des Datenschutzgesetzes 2000), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung).

Aus dieser Bestimmung folgt, dass eine Datenanwendung in all ihren Verwendungsschritten nicht automationsunterstützt, also manuell, zu erfolgen hat, um in den Anwendungsbereich des vorliegenden Gesetzesentwurfs zu fallen. Erfolgt auch nur

ein Verwendungsschritt automationsunterstützt, z.B. die Verwendung eines Papierausdrucks aus einer automationsunterstützten Datenverarbeitung, liegt eine automationsunterstützte Datenanwendung vor und ist das Datenschutzgesetz 2000 anzuwenden.

Zu § 4 (öffentlicher und privater Bereich):

Die hier vorgenommene, dem § 5 des Datenschutzgesetzes 2000 entsprechende Unterscheidung zwischen öffentlichem und privatem Bereich ist nicht nur im Hinblick auf die im Abs. 3 enthaltene Verwendung des Begriffs „privater Bereich“ von Bedeutung, sondern durchzieht praktisch das gesamte Datenschutzrecht. So bestehen für Auftraggeber des öffentlichen Bereichs gemäß den §§ 7 und 8 des vorliegenden Gesetzentwurfs bestimmte Ausnahmen von Verwendungsverboten, wenn der Gebrauch der Daten etwa eine wesentliche Voraussetzung für die Wahrnehmung gesetzlich übertragener Aufgaben darstellt oder im Wege der Erfüllung einer Verpflichtung zur Amtshilfe erfolgt. Eine wichtige Unterscheidung ist auch, dass Ansprüche gegen Auftraggeber wegen Verletzung der Rechte der Betroffenen auf dem Zivilrechtsweg geltend zu machen sind, vergleichbare Ansprüche gegen Auftraggeber des öffentlichen Bereichs hingegen bei der Datenschutzkommission (§§ 25 und 26 des vorliegenden Entwurfs).

Die Abgrenzung zwischen Auftraggebern des öffentlichen Bereichs (*Abs. 1*) sowie Auftraggeberinnen und Auftraggebern des privaten Bereichs (*Abs. 2*) stellt darauf ab, nach welchem Rechtsregime sie eingerichtet sind. Eine gewisse Korrektur erfährt dieses Abgrenzungskriterium nur dort, wo Rechtsträger des privaten Rechts ausnahmsweise Hoheitsverwaltung betreiben, ein Fall, der angesichts der steigenden Anzahl von Ausgliederungen von Verwaltungsbereichen besonders zu berücksichtigen war (Abs. 2 Z 2). Die Wendung “in Vollziehung der Gesetze” ist im Sinne des Art. 23 B-VG so zu verstehen, dass auch die schlichte Hoheitsverwaltung mit umfasst ist.

Zu § 5 (Grundsätze):

Wie schon die Datenschutzkonvention des Europarats enthält auch die Datenschutzrichtlinie in einem Katalog “Grundsätze für die Datenqualität”. Dieser Katalog wurde – dem § 6 Abs. 1 des Datenschutzgesetzes 2000 entsprechend - ausdrücklich (in sprachlich gekürzter Form) auch in den vorliegenden Gesetzentwurf aufgenommen.

Zu Abs. 1:

Eine Verwendung von Daten “nach Treu und Glauben” (*Z 1*) liegt nur dann vor, wenn die Betroffenen über die Umstände des Datengebrauchs und das Bestehen und die Durchsetzbarkeit ihrer Rechte nicht irregeführt oder im Unklaren gelassen werden. Wichtig für die Verwirklichung dieses Gebots sind vor allem die Bestimmungen des 4. Abschnitts des vorliegenden Entwurfs über die Publizität der Datenanwendungen. Aus dem Gebot der Verwendung “in rechtmäßiger Weise” ergibt sich u.a. auch, dass die Auftraggeberin oder der Auftraggeber eine ausreichende rechtliche Befugnis bzw. Zuständigkeit für jene Art der Benützung von Daten, die sie oder er mit der betreffenden Datenanwendung bezweckt, besitzen muss.

Das in *Z 2* statuierte Zweckbeschränkungsprinzip findet im vorliegenden Gesetzentwurf in folgenden Bestimmungen seine Umsetzung:

– Wichtig hiefür ist zunächst die Definition des Übermittlungsbegriffs in § 3 Z 12: Jeder Zweckwechsel ist eine “Übermittlung”; diese liegt nicht nur dann vor, wenn Daten an einen Dritten weitergegeben werden, sondern auch dann, wenn dieselbe Auftraggeberin oder derselbe Auftraggeber Daten selbst für ein anderes Aufgabengebiet (weiter)verwendet.
– Jede Übermittlung bedarf einer besonderen rechtlichen Grundlage; sind die Voraussetzungen des § 6 Abs. 2 und 3 nicht gegeben, ist eine Übermittlung von Daten unzulässig.

Wenn in Z 2 statuiert wird, dass eine Weiterverwendung von Daten nur zulässig sein soll, wenn dies mit dem ursprünglichen Ermittlungszweck “nicht unvereinbar” ist, so sei dazu angemerkt, dass diejenigen innerbetrieblichen Datenverwendungen, die der Aufrechterhaltung und Optimierung der Organisation (wie z.B. Rechnungswesen und Controlling) oder der Analyse und Planung dienen, jedenfalls *nicht* als eige-

ner Verwendungszweck zu sehen sind, der mit dem Zweck der ursprünglichen Datenermittlung (z.B. im Rahmen des Abschlusses eines Handelsgeschäftes) "unvereinbar" ist.

Das Gebot der sachlichen Richtigkeit (*Z 4*) ist so zu verstehen, dass Richtigkeit *im Hinblick auf den deklarierten Zweck der Datenanwendung* gefordert ist: In diesem Zusammenhang muss jedoch ausdrücklich darauf hingewiesen werden, dass bei Datensammlungen klar erkennbar sein sollte, welches Ausmaß an objektiver Richtigkeit die gespeicherten Daten voraussichtlich besitzen; handelt es sich um sogenannte "weiche" Daten, wird eine regelmäßige Überprüfung auf Aktualität besonders wichtig sein, um ungerechtfertigte Nachteile für Betroffene zu vermeiden.

Zu den Abs. 2 und 3:

Die Absätze 2 und 3 schreiben (analog § 6 Abs. 2 und 3 des Datenschutzgesetzes 2000) die Auftraggeber(innen)verantwortung für Datenanwendungen ausdrücklich fest. Abs. 3 dient der Umsetzung von Art. 4 Abs. 2 der Richtlinie.

Zu Abs. 4:

Die Datenschutzrichtlinie bezieht sich im Art. 27 auf sogenannte "Verhaltensregeln", die nicht-staatliche Institutionen, wie z.B. Berufsverbände, zur näheren Durchführung von einzelstaatlichem Datenschutzrecht für einzelne Branchen und Berufszweige ausarbeiten können. Aus der Sicht der österreichischen Rechtsordnung scheint ein sinnvoller Anwendungsbereich von derartigem "soft law" vor allem bei der näheren Umschreibung dessen zu bestehen, was in einer bestimmten Branche als Datenverwendung nach "Treu und Glauben" anzusehen wäre; weiters wären solche Verhaltensregeln z.B. auch geeignet, um die Rollenverteilung von Auftraggeberinnen und Auftraggebern (Dienstleisterinnen und Dienstleistern) bestimmter Konstellationen ausdrücklich festzuschreiben oder um das Ausmaß der Informationsverpflichtung gegenüber den Betroffenen bei bestimmten Arten von Datenanwendungen näher festzulegen. Solche Regeln haben freilich keinen verbindlichen Charakter, wären aber bei freiwilliger Befolgung durch die Mehrzahl der Beteiligten sicher ein wertvolles Mittel für die effektive Verwirklichung von Datenschutz in wichtigen Bereichen des täglichen Lebens. Um zu vermeiden, dass durch solche Verhaltensregeln rechtswidrige Handlungsanleitungen aufgestellt werden, bedarf es einer Prüfung, die jedoch nicht von der Datenschutzkommission vorgenommen werden soll, um die Un-

abhängigkeit der Entscheidungsfindung im einzelnen Beschwerdefall nicht zu präjudizieren. Abs. 4 beruft daher (anders als § 6 Abs. 4 des Datenschutzgesetzes 2000 den Bundeskanzler) die Landesregierung zu einer Begutachtung der Verhaltensregeln.

Zu § 6 (Zulässigkeit der Verwendung von Daten):

§ 6 enthält (entsprechend § 7 des Datenschutzgesetzes 2000) die generelle Regel für die Beurteilung der Zulässigkeit einer konkreten Datenverwendung. Die Zulässigkeit einer konkreten Datenanwendung hat gemäß *Abs. 1* zwei Voraussetzungen:

- die Berechtigung der Auftraggeberin oder des Auftraggebers und
- die Berücksichtigung der schutzwürdigen Interessen der Betroffenen.

Hinzu treten bei Übermittlungen die im *Abs. 2* genannten zusätzlichen Erfordernisse.

Der Grundsatz der Verhältnismäßigkeit ist im *Abs. 3* im Hinblick auf – zulässige – Eingriffe in das Grundrecht auf Datenschutz ausdrücklich nochmals festgeschrieben.

Zu § 7 (Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten):

Die Zulässigkeit einer Datenanwendung erfordert gemäß § 6 u.a., dass schutzwürdige Geheimhaltungsinteressen nicht verletzt werden.

Dieses Erfordernis bedarf näherer Festlegungen, um vollziehbar zu sein. Dies geschieht (analog den §§ 8 und 9 des Datenschutzgesetzes 2000)

- für die *nicht-sensiblen Daten* in Form einer Generalklausel *(§ 7 Abs. 1*) mit einzelnen wichtigen Beispielen *(§ 7 Abs. 2 bis 4);*

- für *sensible Daten* in Form eines taxativen Katalogs der zulässigen Verwendungsfälle (§ 8).

Durch diese Regelungstechnik wird die von der Datenschutzrichtlinie vorgegebene Kasuistik mit der in österreichischen Gesetzen üblichen Präferenz für generelle Regelungen in Einklang gebracht und überdies die von Art. 8 der Richtlinie geforderte Verbotswirkung für die im Art. 8 nicht erwähnten Fälle der Verwendung sensibler Daten erreicht.

§ 7 Abs. 2 nennt – in Durchführung der Verfassungsbestimmung des § 1 Abs. 1 letzter Satz des Datenschutzgesetzes 2000 – zwei Fälle, in denen kein Geheimhaltungsanspruch besteht. Zum ersten Fall – der Verwendung zulässigerweise veröffentlichter Daten – ist anzumerken, dass bei allen Datenanwendungen, die solche Daten enthalten, jeweils die Frage zu stellen ist, ob sie *ausschließlich* veröffentlichte Daten enthalten oder ob nicht auch zusätzliche, durch *Auswertung* der veröffentlichten Daten gewonnene Daten in der Datenanwendung enthalten sind, die ihrerseits nirgends veröffentlicht sind. Da im Übrigen auch eine andere Form der Aufbereitung veröffentlichter Daten neue – nicht veröffentlichte – Informationen liefern kann, kann nicht ausgeschlossen werden, dass in besonderen Konstellationen schutzwürdige Geheimhaltungsinteressen doch berührt werden, weshalb das Widerspruchsrecht nach § 22 ausdrücklich aufrecht erhalten wird.

Um die praktische Anwendung des vorliegenden Gesetzentwurfs zu erleichtern, werden im *§ 7 Abs. 3* einige der wichtigsten Fälle angeführt, in denen durch die Datenverwendung keine schutzwürdigen Geheimhaltungsinteressen der Betroffenen verletzt werden, weil es sich um zulässige Eingriffe im Sinne des Abs. 1 handelt. Dieser Katalog ist in keiner Weise erschöpfend und beschränkt sich im Übrigen auf Falltypen, bei denen die Verletzung schutzwürdiger Geheimhaltungsinteressen *immer* auszuschließen ist. Nicht aufgenommen in den Katalog wurden daher Verwendungskonstellationen, in denen die Verletzung schutzwürdiger Geheimhaltungsinteressen zwar unwahrscheinlich ist, aber doch nicht von vornherein ausgeschlossen werden kann, sodass eine Beurteilung von Fall zu Fall notwendig ist (ein Beispiel hiefür wäre die Datenverwendung im Rahmen vorvertraglicher Maßnahmen – vgl. Art. 7 lit. b der Datenschutzrichtlinie).

Ein gesondertes Problem stellt die Verwendung von strafrechtsbezogenen Daten dar. Solche Daten sind nach der Datenschutzrichtlinie nicht “sensible Daten”, werden aber – zu Recht – in die Nähe dieser Daten gerückt (vgl. Art. 8 Abs. 5 der Richtlinie). Die Verarbeitung strafrechtsbezogener Daten muss daher möglichst beschränkt bleiben, weshalb *§ 7 Abs. 4 Z 3* Grenzen zieht, innerhalb derer die Verwendung dieser Daten auch durch private Auftraggeberinnen oder Auftraggeber zulässig sein soll.

Zu § 8 (Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten):

Die Zulässigkeit der Verwendung sensibler Daten ist weitgehend durch die Datenschutzrichtlinie vorgegeben. § 8 gibt zunächst (wie § 9 des Datenschutzgesetzes 2000) die im Art. 8 Abs. 2 und 3 der Richtlinie statuierten Ausnahmen vom Verwendungsverbot wieder. Hinzu treten

– die Ausnahme der *Z 2*, in der kein Geheimhaltungsanspruch gemäß § 1 Abs. 1 des Datenschutzgesetzes 2000 besteht,

- die Ausnahmen nach *Z 3, 4 und 5* sowie nach *Z 10* hinsichtlich § 30 und § 31: In allen diesen Fällen ergibt sich die Zulässigkeit der Ausnahme vom Verwendungsverbot aus Art. 8 Abs. 4 der Datenschutzrichtlinie, da diese Bestimmungen des § 8 die Zulässigkeit der Verwendung von Daten “aus Gründen eines wichtigen öffentlichen Interesses” vorsehen (in Z 10 z.B. für Zwecke von wissenschaftlicher Forschung und Statistik, woran gemäß Erwägungsgrund 34 der Richtlinie ein wichtiges öffentliches Interesse besteht).

Zum Inhalt *einzelner Ziffern* des § 8 ist Folgendes ergänzend anzumerken:

Ein wichtiges öffentliches Interesse im Sinne der *Z 3* ist auch in den Interessen der Aufsicht über bestimmte Wirtschaftszweige zu erblicken: Gesetze, die die Verwendung von Daten für Zwecke einer besonderen Wirtschaftsaufsicht vorsehen, erfüllen ein wichtiges öffentliches Interesse; dies trifft etwa zu bei gesetzlichen Datenverwendungsbestimmungen im Rahmen der Banken- oder Versicherungsaufsicht.

Die Verwendung sensibler Daten zur Rechtsverteidigung gemäß *Z 9* schließt naturgemäß die Zulässigkeit der Verwendung dieser Daten im Vorfeld einer gerichtlichen – oder verwaltungsbehördlichen – Auseinandersetzung ein, also z.B. auch die Verwendung im Rahmen des Versuchs einer außergerichtlichen Streitbeilegung.

Zu § 9 (Zulässigkeit der Überlassung von Daten zur Erbringung einer Dienstleistung):

Diese Regelungen entsprechen denen des § 10 des Datenschutzgesetzes 2000.

Die Verantwortung von Auftraggeberinnen und Auftraggebern hinsichtlich einer Kontrolle der Dienstleisterinnen und Dienstleister wird durch jene Rechtsvorschriften oder Standesregeln beschränkt, die eine Einflussnahme der Auftraggeberinnen und Auftraggeber auf die Auftragsdurchführung durch die Dienstleisterinnen und Dienstleister ausschließen. In welchen Fällen aus der Pflicht zur selbständigen Aufgabenerfüllung durch die Auftragnehmerinnen und Auftragnehmer gemäß § 3 Z 4 sogar die datenschutzrechtliche Auftraggebereigenschaft abzuleiten ist, wird in Form von Verhaltensregeln im Sinne des § 5 Abs. 4 ausdrücklich darzustellen sein.

Da § 9 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 10 (Pflichten der Dienstleisterin und des Dienstleisters):

Diese Regelungen entsprechen denen des § 11 des Datenschutzgesetzes 2000.

Zu den §§ 11 und 12 (Übermittlung und Überlassung von Daten ins Ausland):

Diese Regelungen entsprechen weitestgehend denen der §§ 12 und 13 des Datenschutzgesetzes 2000.

Als Ergebnis der durch die Datenschutzrichtlinie angestrebten Harmonisierung der datenschutzrechtlichen Rechtsvorschriften der EU-Mitgliedstaaten entfällt die datenschutzrechtliche Kontrolle des Datenverkehrs zwischen EU-Staaten (*§ 11 Abs. 1 erster Satz*). Dieses Prinzip gilt allerdings *nicht* hinsichtlich der Datenverwendung für Zwecke der sogenannten "dritten Säule" (Zusammenarbeit der EU-Mitgliedstaaten im Bereich Justiz und Inneres), weil diese Bereiche von der Richtlinie nicht erfasst sind und daher nicht dem Harmonisierungsgebot unterliegen, was Voraussetzung für den unbeschränkten Datenverkehr wäre. Was die Daten juristischer Personen betrifft, besteht allerdings ebenfalls kein harmonisiertes Datenschutzniveau in den EU-Mitgliedstaaten. Dennoch scheint es gerechtfertigt, sie in den unbeschränkt zulässigen Datenverkehr zwischen EU-Mitgliedstaaten einzubeziehen, da in den anderen Mitgliedstaaten unter anderer Bezeichnung (z.B. "Schutz der Betriebsgeheimnisse") Regelungen bestehen, die dem österreichischen Schutzniveau gegenüber keine gravierenden Nachteile befürchten lassen müssen. Durch eine Regelung, die zum Entfall der Genehmigungspflicht auch beim Transfer von Daten juristischer Personen führt, wird außerdem ein wesentlicher kostensparender Effekt bei den Rechtsunterworfenen wie auch bei der Datenschutzkommission erzielt.

Über die im ersten Satz des Abs. 1 erwähnten Fälle hinaus sind auch die in *Abs. 3 und 4* geregelten Fälle des Datenverkehrs ins Ausland ohne Beschränkungen zulässig; dies entspricht den Bestimmungen des Art. 26 Abs. 1 der Richtlinie.

Für alle anderen Fälle des Datenverkehrs mit dem Ausland gilt der Grundsatz, dass der Datenexport nur zulässig ist,

– wenn beim Empfänger ein "angemessenes Datenschutzniveau" besteht (Art. 25 Abs. 1 der Richtlinie) oder
- wenn die Auftraggeberin oder der Auftraggeber der Übermittlung (Überlassung) gegenüber der Datenschutzkommission das Vorliegen ausreichender Garantien für den Schutz der Betroffenenrechte im Ausland

glaubhaft macht (Art. 26 Abs. 2 der Richtlinie).

Für die Frage, wie festgestellt wird, ob ein "angemessenes Datenschutzniveau" besteht, bietet der vorliegende Entwurf (wie auch nach den §§ 12 und 13 des Datenschutzgesetzes 2000) zwei alternative Antworten:

Wenn ein Staat generell ein angemessenes Datenschutzniveau besitzt, kann er gemäß *§ 11 Abs. 2* in die dort genannte Verordnung der Landesregierung aufgenommen werden, was bewirkt, dass der Datenverkehr mit diesem Staat zur Gänze ohne Beschränkungen zulässig ist. (Eine solche generelle Aussage ist auch hinsichtlich der Verwirklichung von Datenschutz in EU-Mitgliedstaaten betreffend die sogenannte "dritte Säule" zulässig.) In allen anderen Fällen muss die Beurteilung von Fall zu Fall geschehen, und zwar anlässlich des Genehmigungsverfahrens gemäß *§ 12 Abs. 2 Z 1*.

Die zum Zweck einer einheitlichen Beurteilung dieser Fragen in allen EU-Mitgliedstaaten vorgesehenen Mitteilungspflichten sind im § 34 umgesetzt.

Da die §§ 11 und 12 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsehen, unterliegen diese Normen insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 13 (Datensicherheitsmaßnahmen):

Diese Bestimmungen entsprechen den Regelungen des § 14 des Datenschutzgesetzes 2000.

Zu § 14 (Datengeheimnis):

Die Verpflichtung der Auftraggeberinnen und Auftraggeber (der Dienstleisterinnen und Dienstleister) – einschließlich ihrer Mitarbeiterinnen und Mitarbeiter – zur Geheimhaltung von Daten, die ihnen auf Grund ihrer berufsmäßigen Beschäftigung bekannt geworden sind, ist auch im § 15 des Datenschutzgesetzes 2000 enthalten.

§ 14 gilt sowohl für Auftraggeberinnen und Auftraggeber (Dienstleisterinnen und Dienstleister) des privaten Bereichs als auch für Auftraggeber (und Dienstleister) des öffentlichen Bereichs sowie für deren Mitarbeiterinnen und Mitarbeiter.

Die Formulierung des *Abs. 3* soll (§ 15 Abs. 3 des Datenschutzgesetzes 2000 folgend) die Verteilung der Verantwortlichkeit zwischen der anordnenden Auftraggeberin oder dem anordnenden Auftraggeber (Dienstleisterin oder Dienstleister) - dies schließt anordnungsbefugte Organe derselben mit ein - und durchführenden Mitarbeiterinnen und Mitarbeitern deutlich zum Ausdruck bringen, was insbesondere auch im Hinblick auf die Verwaltungsstrafbestimmungen des § 33 zweckmäßig ist.

Zu § 15 (Vorabkontrolle):

Bei Verarbeitungen, die "spezifische Risiken für die Rechte und Freiheiten von Personen beinhalten können", sieht Art. 20 Abs. 1 der Datenschutzrichtlinie vor, dass sie einer sogenannten "Vorabkontrolle" zu unterwerfen, d.h. dass sie vor ihrer Aufnahme durch die unabhängige Kontrollinstanz auf ihre Zulässigkeit zu prüfen sind. Dementsprechend ist im *Abs. 1* (vgl. § 18 Abs. 2 Z 1 bis 3 des Datenschutzgesetzes 2000) in Verbindung mit *Abs. 2* festgelegt, welche Kategorien von Datenanwendungen erst nach einer Vorabkontrolle durch die Datenschutzkommission aufgenommen werden dürfen.

Strafrechtsbezogene Daten (*Abs. 1 Z 2*) werden von der Richtlinie zwar nicht als sensible Daten bezeichnet, aber hinsichtlich der Schutzwürdigkeit als "sensibilitätsnah" behandelt (vgl. Art. 8 Abs. 5 Richtlinie), weshalb ihre Unterstellung unter die Vorabkontrolle sachlich geboten erscheint.

Der Vorabkontrolle sind weiters gemäß *Abs. 1 Z 3* Datenanwendungen unterworfen, die die Auskunftserteilung über die Kreditwürdigkeit von natürlichen oder juristischen Personen zum Gegenstand haben. Unter "Auskunftserteilung" ist nicht die aus den Unterlagen des Rechnungswesens in einem Unternehmen hervorgehende Information über kreditrelevantes Verhalten der eigenen Kundinnen und Kunden (potenziellen Kundinnen und Kunden) zu verstehen; von Z 3 erfasst sollen vielmehr nur

jene Datenanwendungen sein, deren ausschließlicher Zweck die Auskunftserteilung ist und zwar an Außenstehende für deren Zwecke (Vereinsmitglieder wären in diesem Sinn als Außenstehende zu betrachten, wenn etwa ein Verein ein Kreditauskunftssystem betreibt).

Die Ausnahmen nach *Abs. 2* (analog § 17 Abs. 2 Z 1 bis 3 des Datenschutzgesetzes 2000) wurden aus folgenden Erwägungen vorgesehen:

An (zulässigerweise) veröffentlichten Daten besteht gemäß § 1 Abs. 1 kein Geheimhaltungsanspruch. Es ist daher nur konsequent, wenn Datenanwendungen, die *ausschließlich* solche Daten beinhalten, mangels Eingreifens in schutzwürdige Geheimhaltungsinteressen von der Meldepflicht ausgenommen sind (*Z 1*). Es sei aber ausdrücklich darauf hingewiesen, dass diese Ausnahme nicht anwendbar ist, wenn neben veröffentlichten Daten auch andere personenbezogene Daten in einer Datenanwendung verarbeitet werden, insbesondere Bewertungen, Analysen, Verknüpfungen, usw. von veröffentlichten Daten. Diese Ausnahme ist angesichts ihrer Grundrechtsrelevanz restriktiv zu interpretieren.

Hinsichtlich der Ausnahme von der Meldepflicht für öffentliche Register (*Z 2*) ist auf die Datenschutzrichtlinie zu verweisen (vgl. Art. 21 Abs. 3 zweiter Satz), wo dies ausdrücklich als zulässig erklärt wird.

Bei der Verwendung nur indirekt personenbezogener Daten (*Z 3*) besteht nach § 1 Abs. 1 des Datenschutzgesetzes 2000 ebenfalls kein Geheimhaltungsanspruch, weshalb eine Meldepflicht sachlich gerechtfertigt entfallen kann.

Um auch im Bereich der der Vorabkontrolle unterliegenden Datenanwendungen keine unnötigen Erschwernisse für Auftraggeberinnen und Auftraggeber zu bewirken, wurde im § 16 Abs. 4 für die Datenschutzkommission die Verpflichtung geschaffen, bereits anlässlich eines allfälligen Verbesserungsauftrags darüber zu entscheiden, ob die Verarbeitung sofort aufgenommen werden darf oder bis zur Entscheidung über die Registrierung zugewartet werden muss (vgl. § 20 Abs. 3 des Datenschutzgesetzes 2000).

Da § 15 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 16 (Verfahren der Vorabkontrolle):

Abs. 1 enthält - § 19 Abs. 1 des Datenschutzgesetzes 2000 folgend – den notwendigen Inhalt einer Meldung an die Datenschutzkommission.

Hinsichtlich des Verfahrens der Vorabkontrolle ist im *Abs. 7* ausdrücklich vorgesehen, dass bei Untätigkeit der Datenschutzkommission die Verarbeitung von Daten jedenfalls zwei Monate nach Abgabe der Meldung aufgenommen werden kann. Wenn hingegen im Fall eines Verbesserungsauftrags im Vorabkontrollverfahren gemäß *Abs. 4* entschieden wird, dass die Verarbeitung noch nicht aufgenommen werden darf, gelten die Entscheidungsfristen des AVG einschließlich der Möglichkeit der Säumnisbeschwerde für die Entscheidung darüber, ob die aufgetragenen Verbesserungen vorgenommen wurden und davon abgeleitet, ob die Verarbeitung aufgenommen werden darf (vgl. § 20 Abs. 3 und 5 des Datenschutzgesetzes 2000).

Da § 16 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 17 (Datenverarbeitungsregister):

Die hier enthaltenen Bestimmungen entsprechen denjenigen des § 21 Abs. 1 Z 1 und 2, Abs. 3 und 4, § 22 sowie § 16 Abs. 2 des Datenschutzgesetzes 2000.

Aus *Abs. 1* in Verbindung mit den §§ 15 und 16 ergibt sich, dass eine Meldepflicht nur für solche Dateien besteht, deren Inhalt der Vorabkontrolle unterliegt (so – für manuelle Dateien – auch § 58 des Datenschutzgesetzes 2000).

Da § 17 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 18 (Offenlegungspflicht der Auftraggeberin und des Auftraggebers):

Mit dieser Regelung wird der Vorgabe des Art. 21 Abs. 3 der Datenschutzrichtlinie hinsichtlich der Offenlegungspflicht für nicht einer Vorabkontrolle – und somit keiner Meldepflicht - unterliegenden Angaben entsprochen (vgl. dazu § 16 Abs. 1 Z 1 bis 5).

Zu § 19 (Informationspflicht der Auftraggeberin und des Auftraggebers):

Die hier vorgesehenen Regelungen entsprechen den Bestimmungen des § 24 Abs. 1 bis 3 des Datenschutzgesetzes 2000.

Die Informationspflicht der Auftraggeberinnen und Auftraggeber ist eine der wesentlichsten Neuerungen der Datenschutzrichtlinie gegenüber der bis zur Erlassung des Datenschutzgesetzes 2000 geltenden österreichischen Rechtslage. Sie soll es den Betroffenen erleichtern ihre Rechte zu wahren. Datenverarbeitung nach Treu und Glauben (vgl. § 5 Abs. 1 Z 1 des vorliegenden Gesetzentwurfs) setzt voraus, dass die Betroffenen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden (so Erwägungsgrund 38 zur Datenschutzrichtlinie).

Der vorliegende Gesetzentwurf sieht als Instrumente für diesen Zweck die Informationspflicht nach *§ 19*, das Datenverarbeitungsregister (*§ 17*), die Offenlegungspflicht nach *§ 18* und schließlich das Auskunftsrecht gemäß *§ 20* vor. Schon aus dem allgemeinen Sachlichkeitsgebot (Art. 7 Abs. 1 B-VG) ergibt sich, dass es sich hier nicht um Pflichten handeln kann, die alle denselben Inhalt haben. Diese Instrumente haben einander vielmehr so zu ergänzen, dass die Betroffenen verlässlich jene Informationen erhalten, die sie zur Durchsetzung ihrer Datenschutzrechte brauchen, und zwar ohne unzumutbare Anstrengungen ihrerseits, aber auch ohne unzumutbare und unnötige Belastung der Auftraggeberinnen und Auftraggeber. Deshalb kann diese Verpflichtung vorzusorgen, dass die Betroffenen in der Lage sind, das

Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden (s. die oben zitierte Richtlinienstelle), nicht so verstanden werden, dass sich daraus ein Zwang zur Verdoppelung der Meldepflicht (an das Register) in Form einer zusätzlichen Pflicht zur "Meldung an die Betroffenen" ergibt; diesfalls müsste die Führung eines Registers als überflüssiger und daher unverhältnismäßiger Aufwand betrachtet werden. Vor dem Hintergrund des Bestehens einer Registrierungspflicht muss vielmehr der Sinn einer zusätzlichen Informationspflicht darin gesehen werden, dass den Betroffenen immer dann, "wenn ihnen diese Information nicht bereits vorliegt", der Hinweis darauf gegeben wird, dass ihre Daten von einer bestimmten Auftraggeberin oder einem bestimmten Auftraggeber für einen bestimmten Zweck verarbeitet werden sollen. Dadurch werden sie in die Lage versetzt, sich – falls sie das wünschen – aller Hilfsmittel zu bedienen, um "ordnungsgemäß und umfassend informiert zu werden".

Aus diesen Darlegungen folgt, dass die Frage, ob Informationen mit dem Inhalt des § 19 *Abs. 1* "bereits vorliegen", nach der jeweiligen Situation zu beurteilen ist. Es ist dabei durchaus denkbar, dass z.B. die Umstände, unter welchen Daten bei der oder beim Betroffenen erhoben werden, jeden Zweifel darüber ausschließen, dass die Daten von der Datenermittlerin oder vom Datenermittler für einen der oder dem Betroffenen unmittelbar einsichtigen Zweck verarbeitet werden. Diesfalls ist eine ausdrückliche Information der oder des Betroffenen unnötig und würde wahrscheinlich bei ihr oder ihm auch nur Befremden hervorrufen.

Andererseits werden bestimmte Situationen entsprechend dem Gebot der Verarbeitung nach "Treu und Glauben" über Abs. 1 hinausgehende Informationen erfordern. Diesem Umstand trägt *Abs. 2* Rechnung. Diese Information hat nicht den Charakter einer umfassenden Rechtsbelehrung für den konkreten Einzelfall; vielmehr wäre etwa bei einer Information gemäß Z 1 auf das Bestehen des Widerspruchsrechts gemäß § 22 – allenfalls unter Zitierung dieser Bestimmung – hinzuweisen. Da die richtige Information somit unter Umständen die Beurteilung eines komplexen Sachverhalts voraussetzt, kann es sinnvoll sein, das Ausmaß der Informationspflicht in einzelnen typischen Situationen durch Verhaltensregeln nach § 5 Abs. 4 zu klären. Die Befolgung solcher Verhaltensregeln kann im Hinblick auf eine etwaige Strafbarkeit nach § 33 von wesentlicher Bedeutung sein.

Zu § 20 (Auskunftsrecht):

Diese Regelungen entsprechen den Bestimmungen des § 26 Abs. 1 bis 4, 6 bis 8 und 10 des Datenschutzgesetzes 2000.

Abs. 2 regelt insbesondere, in welchen Fällen im öffentlichen Interesse oder im Interesse Dritter keine Auskunft zu geben ist. Die Zulässigkeit dieser Ausnahmen stützt sich auf Art. 13 der Datenschutzrichtlinie. Im Übrigen wird – in Übereinstimmung mit Art. 13 der Richtlinie – auch der Fall einbezogen, dass das Auskunftsrecht zum Schutz der Betroffenen einzuschränken ist; dies wird freilich nur in wenigen Ausnahmefällen gerechtfertigt sein (z.B. im medizinischen Bereich).

Zur Verpflichtung der Betroffenen, im Rahmen des Auskunftsverfahrens mitzuwirken (*Abs. 3*) ist Folgendes zu bemerken: In der Datenschutzrichtlinie finden sich mehrfach Bestimmungen, die der Ausübung von Betroffenenrechten Grenzen setzen, und zwar dort, wo die Rechtsausübung der Betroffenen einen unverhältnismäßigen Aufwand bei der Auftraggeberin oder beim Auftraggeber verursachen würde (vgl. die Informationspflicht nach Art. 11 oder die Verständigungspflicht an Datenempfängerinnen und Datenempfänger gemäß Art. 12). Dieser Grundsatz ist aus der Verpflichtung zur entsprechenden Berücksichtigung der Rechte und Freiheiten Dritter abzuleiten und wird auch beim Auskunftsrecht Geltung beanspruchen dürfen. Gerade bei Auftraggeberinnen und Auftraggebern mit sehr vielen Datenverarbeitungen kann die Verpflichtung der Auftraggeberin oder des Auftraggebers, alle ihre oder seine Datenverarbeitungen zu durchsuchen, wenn die oder der Betroffene nicht den mindesten Hinweis darauf gibt oder geben will, in welchem Zusammenhang sie oder er in den Datenanwendungen der Auftraggeberin oder des Auftraggebers vorhanden sein könnte, eine beträchtliche Belastung der Auftraggeberin oder des Auftraggebers (unter Umständen sogar Stilllegung der Datenverarbeitung für einige Zeit) bewirken. In dem Bestreben, einen Interessenausgleich zwischen den Betroffenen einerseits sowie den Auftraggeberinnen und Auftraggebern andererseits zu erzielen, statuiert daher Abs. 3, dass die Betroffenen in dem ihnen zumutbaren Ausmaß mitwirken müssen, und *Abs. 5*, dass die Auskunft dann unentgeltlich zu er-

teilen ist, wenn die Auffindung der der Auskunft unterliegenden Daten für die Auftraggeberin oder den Auftraggeber keine besondere Belastung darstellt ("wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft"). In allen anderen Fällen ist die Auskunft kostenpflichtig, wobei ein niedriger Grundtarif (aus Gründen der Gleichbehandlung der Kostenersatzpflichtigen exakt gleich wie der im § 26 Abs. 6 des Datenschutzgesetzes 2000 vorgesehene Betrag) im Gesetz festgelegt ist, von dem bei tatsächlich erwachsenden höheren Kosten abgewichen werden darf. Auch Portokosten sind den tatsächlich erwachsenden Kosten zuzuzählen. Ob derartige Abweichungen gerechtfertigt sind, wäre in einem Verfahren vor der Datenschutzkommission gemäß § 25 Abs. 1 überprüfbar.

Da § 20 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 21 (Recht auf Richtigstellung oder Löschung):

Die hier enthaltenen Regelungen entsprechen den Bestimmungen des § 27 Abs. 1 bis 4 sowie 7 und 8 des Datenschutzgesetzes 2000.

In den *Abs. 1 bis 4* wird zunächst klargestellt, dass die Verpflichtung zur Richtigstellung oder Löschung von Daten die Auftraggeberinnen und Auftraggeber auch dann trifft, wenn die oder der Betroffene dies nicht eigens beantragt hat. Weiters werden Klarstellungen gegeben, wann Unvollständigkeit und wann Unzulässigkeit der Verarbeitung in bestimmten Konstellationen vorliegt.

Abs. 6 trägt dem Umstand Rechnung, dass manche Datenanwendungen nach ihrem besonderen Zweck eine Löschung von Daten in der Form, dass Daten nicht mehr sichtbar sind, nicht gestatten. Dies wird überall dort der Fall sein, wo die lückenlose Dokumentation eines Geschehens Gegenstand der Datenverarbeitung ist (z.B. bei der Führung von Krankengeschichten, sofern sie manuell erfolgt).

Da § 21 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 22 (Widerspruchsrecht):

Die Datenschutzrichtlinie sieht ein Widerspruchsrecht im Art. 14, das Datenschutzgesetz 2000 im § 28 (dessen Regelungen der vorliegende Gesetzesentwurf folgt) vor.

Ausgehend von der zum Teil sehr allgemeinen Formulierung der Zulässigkeitsvoraussetzung für Datenverarbeitungen im Art. 7 der Datenschutzrichtlinie (insbesondere lit. e und f) enthält die Richtlinie als Korrekturmöglichkeit ein Widerspruchsrecht, wonach die Betroffenen verlangen können, dass sie aus "sich aus ihrer besonderen Situation ergebenden Gründen" aus einer Datenanwendung, gegenüber der sie ein Widerspruchsrecht geltend machen, gelöscht werden.

Zur Frage, wo der Unterschied zwischen einer Beschwerde (Klage) wegen unzulässiger Verarbeitung von Daten nach den §§ 25 oder 26 und der Ausübung des Widerspruchrechts nach § 22 *Abs. 1* liegt, ist Folgendes auszuführen:

Die Datenschutzrichtlinie enthält im Art. 14 keine klare Aussage über diese Frage und gibt auch keinen Hinweis auf möglicherweise unterschiedliche Folgen. Daraus, dass im Art. 14 aber auch auf das Widerspruchsrecht im Bereich der Verwendung von Daten für Marketingzwecke Bezug genommen wird, könnte folgender Schluss gezogen werden:

Die Ausübung des Widerspruchsrechts hat keinen Einfluss auf die rechtliche Zulässigkeit der Datenanwendung an sich. Sie bewirkt nur eine individuell auf die (erfolgreich) Widersprechenden begrenzte Löschungspflicht, bedeutet aber nicht, dass die gesamte Datenanwendung wegen Rechtswidrigkeit einzustellen wäre. Die erfolgreiche Ausübung des Widerspruchsrechts wird daher – zumindest grundsätzlich – auch keinen Schadenersatzanspruch begründen können.

Im *Abs. 2* wird eine zusätzliche Spielart des Widerspruchsrechts ausdrücklich geregelt, die in der Praxis nach den bisherigen Erfahrungen im Bundesbereich bedeutsam sein könnte und nur die Nutzanwendung des bereits zu Abs. 1 Gesagten auf eine besondere Konstellation darstellt: Es kann Anwendungsfälle geben (wenngleich im Bereich manueller Datenverarbeitung wohl nur in relativ geringfügigem Ausmaß), in denen bei einer Durchschnittsbetrachtung eine Verletzung schutzwürdiger Geheimhaltungsinteressen infolge des Zwecks der Datenverarbeitung und der verwendeten Datenarten unwahrscheinlich ist. Derartige öffentlich zugängliche Verzeichnisse beruhen zum größten Teil nicht auf ausdrücklichen gesetzlichen Regelungen. Um einen fairen Interessenausgleich zu gewährleisten, scheint es sinnvoll, Personen ein Widerspruchsrecht gegen die Aufnahme in solche Verzeichnisse einzuräumen, wenn sie in Abweichung von der durchschnittlichen Einschätzung der Geheimhaltungsinteressen eine Verletzung ihrer Interessen durch Aufnahme ihrer Daten in ein solches Verzeichnis befürchten. Durch die Möglichkeit des Widerspruchs wäre gewährleistet, dass einerseits Verzeichnisse dieser Art, die von der großen Mehrheit der Bevölkerung als sinnvoll und nützlich empfunden werden, legalerweise existieren können und andererseits Interessenlagen, die vom Durchschnitt abweichen, entsprechend berücksichtigt werden können und diese Berücksichtigung auch einfach durchzusetzen ist.

Zu § 24 (Kontrollbefugnisse der Datenschutzkommission):

Diese Bestimmungen entsprechen den Regelungen des § 30 des Datenschutzgesetzes 2000.

Die Datenschutzrichtlinie misst der Kontrolle von Datenanwendungen außerhalb förmlicher Beschwerdeverfahren große Bedeutung zu. Diese Kontrolle muss gemäß der Richtlinie auch im privaten Bereich möglich sein. Sie ist von einer unabhängigen Kontrollstelle wahrzunehmen und hat das Recht der Kontrollstelle zu beinhalten, Einschau in Datenverarbeitungen und Unterlagen zu nehmen, Auskünfte zu verlangen und den Auftraggeberinnen und Auftraggebern Empfehlungen und Ermahnungen zu erteilen; sie kann bis zu einem gewissen Grad auch rechtsförmliche

Akte umfassen, soweit z.B. eine Kompetenz zur vorläufigen Untersagung der Weiterführung von Datenverarbeitungen besteht.

Im vorliegenden Entwurf sind nun – wie auch im § 30 des Datenschutzgesetzes 2000 - die Kontrollbefugnisse in der Weise umgesetzt, dass die ***Datenschutzkommission*** als unabhängige Kontrollstelle den öffentlichen und den privaten Bereich zu kontrollieren hat, und zwar entweder aus Anlass eines Anbringens einer Bürgerin oder eines Bürgers oder auch in Fällen, die ein erhöhtes Gefährdungspotenzial besitzen, ohne einen solchen Anlass. Rechtsförmliche Entscheidungen über behauptete Datenschutzverletzungen werden hingegen so wie bisher von der Datenschutzkommission zu erlassen sein, wenn sie Auftraggeber des öffentlichen Bereichs betreffen, und von den ordentlichen Gerichten, wenn sie Auftraggeberinnen oder Auftraggeber des privaten Bereichs betreffen.

Die Verpflichtung zur möglichsten Schonung der Rechte der Auftraggeberinnen und Auftraggeber (Dienstleisterinnen und Dienstleister) im Rahmen einer Einschau (*Abs. 4 letzter* Satz) bedeutet auch, dass eine Einschau grundsätzlich nur innerhalb der Betriebszeiten vorgenommen werden darf.

Die Konsequenzen der Nichtbefolgung einer Empfehlung der Kontrollstelle sind im *Abs. 6* näher geregelt.

Da § 24 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 25 (Beschwerde an die Datenschutzkommission):

Diese Bestimmungen entsprechen den Regelungen des § 31 Abs. 1 bis 3 des Datenschutzgesetzes 2000.

Die Datenschutzkommission übt neben ihrer Kontrolltätigkeit auch eine quasirichterliche Entscheidungsfunktion in ihrer Rolle als Behörde gemäß Art. 133 Z 4

B-VG aus. Sie erkennt in rechtsförmlichen Verfahren mit Bescheid über Beschwerden wegen behaupteter Verletzungen des vorliegenden Gesetzentwurfs durch einen Auftraggeber des öffentlichen Bereichs. Es besteht eine umfassende Zuständigkeit für Verletzungen des Auskunftsrechts (*Abs. 1*), gleichgültig, ob diese einem Auftraggeber des öffentlichen Bereichs oder einer Auftraggeberin oder einem Auftraggeber des privaten Bereichs zur Last gelegt werden. Hinsichtlich aller anderen behaupteten Verletzungen ist die Datenschutzkommission nur dann zuständig, wenn sie einen Auftraggeber des öffentlichen Bereichs betreffen (*Abs. 2*), insgesamt aber immer nur im Hinblick auf die Prüfung von Handlungen, die weder der Gerichtsbarkeit noch der Gesetzgebung zuzurechnen sind, wobei die Zurechnung nach funktionalen Gesichtspunkten vorzunehmen ist.

Da § 25 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 26 (Anrufung der Gerichte):

Diese Regelung entspricht den Bestimmungen des § 32 des Datenschutzgesetzes 2000.

Die Betroffenen haben Anspruch auf Unterlassung und Beseitigung eines dem vorliegenden Gesetzentwurf widerstreitenden Zustands. Ist Verursacher eine Auftraggeberin oder ein Auftraggeber des privaten Bereichs, so sind diese Ansprüche vor den ordentlichen Gerichten durchzusetzen. Einzige Ausnahme hievon ist die Durchsetzung des Auskunftsrechts, für die immer die Datenschutzkommission zuständig ist.

Gemäß *Abs. 5* kann die Datenschutzkommission anstelle der oder des Betroffenen beim zuständigen ordentlichen Gericht Klage zur Feststellung der Rechtmäßigkeit einer Datenverwendung erheben. Diese Möglichkeit ist auf vermutete schwerwiegende Datenschutzverletzungen beschränkt und soll für solche Fälle, an deren Klärung somit auch ein öffentliches Interesse besteht, das Prozessrisiko der

oder des Betroffenen vermeiden. Auf der Grundlage des gerichtlichen Feststellungsurteils kann die oder der Betroffene sodann entscheiden, ob er ihre oder seine Unterlassungs- und Schadenersatzansprüche selbst weiterverfolgen will.

Da § 26 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG. Im Übrigen ist im Hinblick darauf, dass die vorliegende Regelung ausschließlich der Umsetzung von Gemeinschaftsrecht dient, davon auszugehen, dass sie – soweit sie Bestimmungen zivilrechtlichen Inhalts aufweist - im Sinne des Art. 15 Abs. 9 B-VG „erforderlich“ und somit verfassungsrechtlich zulässig ist.

Zu § 27 (Schadenersatz):

In Umsetzung von Art. 23 Abs. 1 der Datenschutzrichtlinie enthält § 27 (gleich § 33 des Datenschutzgesetzes 2000) ausdrückliche Bestimmungen über den Ersatz erlittenen Schadens. Dafür gelten zunächst die allgemeinen Bestimmungen des Schadenersatzrechts; gehaftet wird nur bei Verschulden (*Abs. 1*).

Für Fälle schwerwiegender rechtswidriger Datenverwendung, die ihrem Wesen nach Tatbeständen vergleichbar sind, die nach Mediengesetz zum Schadenersatz verpflichten, sieht *Abs. 2* den Ersatz immaterieller Schäden vor, wobei sich die näheren Voraussetzungen und die Höhe der Entschädigung aus den §§ 6 und 7 des Mediengesetzes ergeben. Daraus folgt, dass die Höhe der Entschädigung derzeit mit 14.535 Euro begrenzt ist. Da nur Fälle besonders schwerwiegender Datenschutzverletzungen zum immateriellen Schadenersatz berechtigen sollten, wurden die hier relevanten Fälle auf die Verwendung von Daten im Sinne des § 15 Abs. 1 des vorliegenden Entwurfs beschränkt; hiebei ist neben der fehlerhaften insbesondere auch die rechtsmissbräuchliche Datenverwendung Regelungsgegenstand.

Klargestellt sei, dass die Bestimmungen des vorliegenden Gesetzesentwurfs im Einzelfall auch als Schutzgesetz im Sinne des § 1311 ABGB greifen können. Das Grundrecht auf Datenschutz gemäß § 1 des Datenschutzgesetzes 2000 wird im Üb-

rigen auch zu den – absolut geschützten – Persönlichkeitsrechten im Sinne des § 16 ABGB zu zählen sein.

Verletzungen von Datenschutzbestimmungen erfolgen häufig außerhalb von Vertragsverhältnissen zur oder zum Geschädigten, sodass die Regelung des § 1313a ABGB nicht zur Anwendung kommt. Auf Grund des Umstands, dass es für die Betroffenen jedoch oft nicht möglich ist, die Arbeitsaufteilung und die daraus resultierende Verantwortlichkeit bei Datenverarbeitungsvorgängen nachzuvollziehen, erscheint es dennoch sachgemäß, im *Abs. 3* die Regelung des § 1313a ABGB sinngemäß für sämtliche Haftungen aus rechtswidrigen Datenverwendungen zu übernehmen: Den Auftraggeberinnen und Auftraggebern (Dienstleisterinnen und Dienstleistern) ist daher jeweils das Verhalten ihrer Leute zuzurechnen, wobei die Dienstleisterinnen und Dienstleister und ihre Leute gleichzeitig "Leute der Auftraggeberin oder des Auftraggebers" sind, sodass die Haftung gegenüber der oder dem Betroffenen zunächst bei der Auftraggeberin oder beim Auftraggeber konzentriert wird. Allerdings kann sich die Auftraggeberin oder der Auftraggeber von ihrer oder seiner Haftung gegenüber der oder dem Betroffenen befreien, wenn sie oder er nachweist, dass der Umstand, durch den der Schaden verursacht wurde, ihr oder ihm bzw. ihren oder seinen Leuten nicht zur Last gelegt werden kann. Diese, im *Abs. 4* vorgesehene Beweislastumkehr zu Gunsten der Betroffenen setzt die zwingende Bestimmung des Art. 23 Abs. 2 der Datenschutzrichtlinie um.

Im Übrigen gelten, etwa was Rückersatzansprüche oder die Haftung für Handlungen in Vollziehung der Gesetze betrifft, die allgemeinen Bestimmungen des bürgerlichen Rechts und des Amtshaftungsgesetzes.

Im Hinblick darauf, dass die vorliegende Regelung ausschließlich der Umsetzung von Gemeinschaftsrecht dient, ist davon auszugehen, dass sie – soweit sie Bestimmungen zivilrechtlichen Inhalts aufweist - im Sinne des Art. 15 Abs. 9 B-VG „erforderlich" und somit verfassungsrechtlich zulässig ist.

Zu § 28 (Gemeinsame Bestimmungen):

Diese Regelungen entsprechen den im § 34 des Datenschutzgesetzes 2000 enthaltenen Bestimmungen.

Die Anwendungserfahrung, insbesondere vor der Datenschutzkommission, hat ergeben, dass die Statuierung von Verjährungsfristen (*Abs. 1*) für die Geltendmachung der Interessen der Betroffenen nach dem vorliegenden Gesetzentwurf sachlich geboten ist: Die Ermittlung von Sachverhalten, die lange zurückliegen, stößt erfahrungsgemäß auf erhebliche Schwierigkeiten und verhindert eine verlässliche Beurteilung des Vorliegens von Datenschutzverletzungen. Auch im eigenen Interesse sollten die Betroffenen daher dazu angehalten werden, behauptete Datenschutzverletzungen möglichst frühzeitig bei der Datenschutzkommission oder bei Gericht anhängig zu machen. Festzuhalten ist, dass diese besonderen Verjährungsfristen für Schadenersatzansprüche nach § 27 nicht gelten; diesbezüglich gelten die Verjährungsfristen des § 1489 ABGB, das sind drei bzw. 30 Jahre.

Gemäß § 2 des vorliegenden Entwurfs finden – in Umsetzung des Art. 4 der Datenschutzrichtlinie – in Österreich unter Umständen die Datenschutzregelungen eines anderen EU-Mitgliedstaats Anwendung. § 28 *Abs. 2* weist ausdrücklich darauf hin, dass auch die Verletzung ausländischen Datenschutzrechts vor den in Österreich zuständigen Stellen anhängig gemacht werden kann, und zwar insbesondere auch im Rahmen der Kontrolltätigkeit der Datenschutzkommission nach § 24 des Entwurfs.

Durch die Statuierung der Verpflichtung zur Amtshilfe an ausländische Kontrollstellen (*Abs. 4*) – eine Verpflichtung, die in den Rechtsordnungen aller EU-Mitgliedstaaten vorzusehen ist – sollen die Vollziehungsprobleme, die sich aus der Anwendung ausländischen Rechts ergeben, verringert werden.

Da § 28 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 29 (Wirkung von Bescheiden der Datenschutzkommission):

Diese Regelungen entsprechen den in § 40 Abs. 2 bis 4 des Datenschutzgesetzes 2000 enthaltenen Bestimmungen.

Hinsichtlich der bescheidmäßigen Erledigungen der Datenschutzkommission wird die generelle Möglichkeit den Verwaltungsgerichtshof anzurufen, für die Parteien des Verfahrens durch ausdrückliche Anordnung geschaffen (*Abs. 1*).

Was die Stellung der in Vollziehung der Gesetze tätigen Auftraggeber des öffentlichen Bereichs betrifft, haben sie mangels subjektiver Rechte in Verwaltungsverfahren an sich weder Parteistellung noch ein Beschwerderecht an den Verwaltungsgerichtshof (vgl. etwa sogar für den Fall der Formalpartei VwSlg 12.662 A). In jenen Konstellationen, in welchen jedoch im Datenschutzgesetz bei Auftraggebern des öffentlichen Bereichs die Eigenschaft als “belangte Behörde” nicht im Vordergrund steht, wie im Registrierungsverfahren und im Genehmigungsverfahren im internationalen Datenverkehr, scheint es sachgerecht zu sein, auch den in Vollziehung der Gesetze tätigen Auftraggebern des öffentlichen Bereichs Parteistellung und, daran anknüpfend, das Beschwerderecht an den Verwaltungsgerichtshof einzuräumen. Die Beschränkung des Beschwerderechts an den Verwaltungsgerichthof auf diese Fälle ist insoweit systemkonform, als auch im Verfahren vor dem Unabhängigen Verwaltungssenat in Beschwerden über faktische Amtshandlungen – das am ehesten mit dem Beschwerdeverfahren vor der Datenschutzkommission vergleichbar ist – kein Beschwerderecht der belangten Behörde an den Verwaltungsgerichtshof besteht. Neben diesen rechtssystematischen Erwägungen spricht im Übrigen auch das Faktum der bekannten Überlastung des Verwaltungsgerichtshofs gegen eine wesentliche Ausdehnung der Beschwerderechte an dieses Höchstgericht.

Abs. 2 enthält eine sowohl im Hinblick auf § 68 AVG als auch im Hinblick auf den Vorrang des Gemeinschaftsrechts notwendige Regelung, nach der erteilte Genehmigungen im internationalen Datenverkehr widerrufen werden können, wenn die Voraussetzungen der Genehmigung tatsächlich weggefallen sind oder die Kommission der EU die Frage hinreichenden Schutzes bei einem konkreten Datentransfer

ins Ausland nachträglich im Verfahren gemäß Art. 26 Abs. 3 Richtlinie anders beurteilt als die österreichische Datenschutzkommission.

Da § 29 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 30 (Wissenschaftliche Forschung und Statistik):

Diese Bestimmungen entsprechen den Regelungen des § 46 des Datenschutzgesetzes 2000.

Die Datenschutzrichtlinie spricht an mehreren Stellen deutlich aus, dass eine besondere, privilegierende Stellung von wissenschaftlicher Forschung und Statistik bei der Verwendung personenbezogener Daten als sachlich gerechtfertigt angesehen wird. Dementsprechend enthält der vorliegende Entwurf eingehende datenschutzrechtliche Regelungen für diesen Bereich der Verwendung personenbezogener Daten.

Zunächst ist festzuhalten, dass § 30 nur gilt, sofern eine Gesetzgebungszuständigkeit des Landes besteht (s. Art. 10 Abs. 1 Z 13 iVm Art. 15 Abs. 1 B-VG; s. auch die Ausführungen im Allgemeinen Teil zur Kompetenzlage). Auf dieser Grundlage gilt Folgendes, wobei zwei grundsätzlich verschiedene Gebrauchssituationen zu unterscheiden sind:

- Daten werden erhoben für eine “Untersuchung”, das ist ein konkretes Forschungsprojekt oder eine konkrete statistische Erhebung, bei der als Ergebnis Aussagen *in nicht personenbezogener Form* gewonnen werden sollen. Für diese Fälle sieht *Abs. 1* eine privilegierte Verwendungsmöglichkeit bestimmter Daten vor (dies betrifft insbesondere auch Daten, die bei derselben Auftraggeberin oder beim selben Auftraggeber bereits für andere Zwecke vorhanden sind).
- Für alle anderen Fälle gilt *Abs. 2*: Die “anderen Fälle” im Sinne dieser Bestimmung sind entweder Untersuchungen mit *personenbezogenen*

Ergebnissen (z.B. Publikationen aus dem Wissenschaftsbereich der [zeitgenössischen] Geschichtsforschung) oder wissenschaftliche oder statistische Aktivitäten, die ***keine konkrete Untersuchung*** (Erhebung) darstellen (das wäre z.B. die Führung von personenbezogenen Hilfsregistern für statistische Zwecke oder andere personenbezogene permanente Datensammlungen im Umfeld von Forschung und Statistik).

Was die Begriffe "wissenschaftliche Forschung" und "Statistik" betrifft, geht die vorliegende Regelung in Beachtung der Terminologie der Datenschutzrichtlinie von folgendem Begriffsverständnis aus:

"***Wissenschaftliche Forschung***" soll nicht einen inhaltlich abgegrenzten Bereich bezeichnen – etwa in der Richtung, dass nur Grundlagenforschung erfasst und angewandte Forschung ausgeschlossen wäre –, sondern als Gebiet verstanden werden, in dem eine bestimmte Methode der Vorgangsweise, nämlich eine "wissenschaftliche", angewendet wird. Dass hiefür nicht der Ausdruck "Forschung" allein verwendet wird, ist in der Terminologie der Richtlinie begründet: Eine abweichende Begriffsbildung könnte zu Interpretationsschwierigkeiten führen.

Auch der Begriff "***Statistik***" wird dahingehend verstanden, dass es sich um methodologisch "***wissenschaftliche*** Statistik" handelt, da nur unter dieser Voraussetzung eine Privilegierung sachlich zu rechtfertigen ist. Abgesehen davon soll aber dieser Begriff sowohl die sogenannte "amtliche Statistik" als auch sonstige (mit wissenschaftlichen Methoden durchgeführte) Statistik umfassen.

Da § 30 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 31 (Zur-Verfügung-Stellung von Adressen für die Benachrichtigung und Befragung von Betroffenen):

Diese Bestimmung (analog § 47 des Datenschutzgesetzes 2000) entspricht den bisherigen Erfahrungen im Bereich des Datenschutzrechts des Bundes, wonach sich ergeben hat, dass dieses Problem ohne ausdrückliche Regelung unlösbar ist.

Wiederholt wurde das Bundeskanzleramt damit befasst, dass bestimmte Betroffenenkreise aus Gründen, die durchaus im Interesse der Betroffenen oder sogar auch der Öffentlichkeit lagen, informiert oder befragt werden sollten, die Adressdaten dieser Betroffenenkreise jedoch von jenen Stellen, die sie auf Grund anderer Datenanwendungen besaßen, nicht übermittelt werden durften, weil die Tatbestände des § 6 Abs. 2 und 3 jeweils nicht verwirklicht waren. Dasselbe gilt für jene Fälle, in denen für Zwecke wissenschaftlicher Forschung die Adressdaten von bestimmten Betroffenenkreisen benötigt werden, um mit ihnen in Kontakt treten zu können. Um in dieser Situation berechtigten Informationsinteressen gerecht zu werden, wird im vorliegenden § 31 einerseits in unbedenklichen Fällen die Verwendung von Daten gestattet, andererseits in komplizierter gelagerten Fällen die Datenschutzkommission mit der Aufgabe betraut im Einzelfall zu prüfen, ob eine konkrete Übermittlung von Adressdaten eines bestimmten Betroffenenkreises die schutzwürdigen Geheimhaltungsinteressen dieser Betroffenen gefährden würde.

Da § 31 die Mitwirkung eines Bundesorgans (Datenschutzkommission) bei der Landesvollziehung vorsieht, unterliegt diese Norm insoweit dem Zustimmungsrecht durch die Bundesregierung gemäß Art. 97 Abs. 2 B-VG.

Zu § 32 (Verwendung von Daten im Katastrophenfall):

Diese Bestimmung ist weitgehend mit dem durch die 2. Novelle zum DSG 2000, BGBl. I Nr. 13/2005, in das DSG 2000 eingefügten § 48a DSG 2000 ident.

Zu § 33 (Datenanwendungen des Landtages):

Mit dieser Regelung werden zweckmäßige Klarstellungen hinsichtlich der Stellung der Präsidentin oder des Präsidenten des Landtages bei Datenanwendungen für Zwecke der ihr oder ihm durch die Geschäftsordnung des Landtages übertragenen Angelegenheiten getroffen.

Zu § 34 (Strafbestimmungen):

Die Datenschutzrichtlinie verlangt von der nationalen Rechtsordnung, dass sie entsprechende Sanktionen für Verstöße gegen die Bestimmungen der Richtlinie vorsieht (Art. 24 der Richtlinie). § 33 enthält daher einen Katalog von Verwaltungsstraftatbeständen. Im Hinblick auf das Verletzungspotenzial der Straftatbestände wird eine Abstufung des Strafrahmens vorgenommen:

- *Abs. 1* enthält (wie § 52 Abs. 1 des Datenschutzgesetzes 2000) Tatbestände, in denen eine Verletzung von Rechten tatsächlich stattgefunden hat;
- *Abs. 2* zählt (wie § 52 Abs. 2 des Datenschutzgesetzes 2000) Tatbestände auf, in denen zwar noch keine Verletzung von Rechten der Betroffenen manifest ist, aber Unterlassungen begangen wurden, die eine Gefährdung der Rechte der Betroffenen oder zumindest eine Gefährdung der Durchsetzbarkeit dieser Rechte zur Folge haben.

Die in Abs. 1 und 2 vorgesehenen *Strafsätze* orientieren sich an den jeweiligen, in § 52 Abs. 1 und 2 des Datenschutzgesetzes 2000 enthaltenen Beträgen.

Die Zurechnung der Verantwortlichkeit für Tathandlungen zu den einzelnen Organen (Mitarbeiterinnen und Mitarbeitern) von Auftraggeberinnen oder Auftraggebern (Dienstleisterinnen oder Dienstleister) ist durch § 9 VStG geregelt. Für Auftraggeber des öffentlichen Bereichs bedeutet dies, dass auch interne Organisationsvorschriften wie die jeweiligen Geschäftseinteilungen, Geschäftsordnungen oder Vergleichbares zur Beurteilung dieser Frage heranzuziehen sein werden.

Zu § 35 (Mitteilungen an die Europäische Kommission und an die anderen Mitgliedstaaten der Europäischen Union):

Die Bestimmungen des § 34 sind in Umsetzung der Datenschutzrichtlinie notwendig (s. Art. 8 Abs. 6 und Art. 25 Abs. 3). Sie dienen einer gleichmäßigen Entscheidungspraxis in den Fällen des Datenverkehrs mit Drittstaaten durch die Behörden aller EU-Mitgliedstaaten.

Zu § 36 (Anhörungsverfahren):

Diese Regelung entspricht § 38 Abs. 3 des Datenschutzgesetzes 2000.

Zu § 37 (Befreiung von Verwaltungsabgaben):

Hier wird im Sinne eines möglichst ungehinderten Zugangs von Betroffenen zur Wahrnehmung ihrer Rechte nach dem vorliegenden Gesetzentwurf eine Befreiung der Entrichtung von Verwaltungsabgaben des Landes für Eingaben normiert.

Zu § 38 (Übergangsbestimmungen):

Abs. 1 Z 1 entspricht der Vorgabe des Art. 32 Abs. 2 zweiter Satz der Datenschutzrichtlinie, wonach es dem zuständigen Normsetzer freisteht zu normieren, dass die Verarbeitungen von Daten, die zum Zeitpunkt des In-Kraft-Tretens der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie bereits in manuellen Dateien enthalten sind, binnen zwölf Jahren nach Annahme dieser Richtlinie (das war der 24. Oktober 1995) mit deren Artikeln 6, 7 und 8 in Einklang zu bringen sind.

Abs. 1 Z 2 stützt sich auf Art. 32 Abs. 2 erster Satz der Richtlinie.

Abs. 2 setzt Art. 32 Abs. 2 letzter Satz der Richtlinie um.

Zu § 39 (Umsetzung von Gemeinschaftsrecht):

Damit wird der Vorgabe des Art. 32 Abs. 1 zweiter Satz der Datenschutzrichtlinie entsprochen.