Der Landtag von Niederösterreich hat am 5. Okt. 2000 beschlossen:

NÖ Datenschutzgesetz (NÖ DSG)

Inhaltsverzeichnis

4. Abschnitt: Publizität der Datenanwendungen

5. Abschnitt: Aufnahme der Datenanwendung

6. Abschnitt: Die Rechte des Betroffenen

7. Abschnitt: Rechtsschutz

8. Abschnitt: Strafbestimmungen

9. Abschnitt: Schluss- und Übergangsbestimmungen

1. Abschnitt
Allgemeines, Geltungsbereich, Begriffsbestimmungen

§ 1
Allgemeines

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

(2) Dieses Gesetz gilt nicht für Angelegenheiten, in denen die Gesetzgebung Bundessache ist.

(3) Soweit in diesem Gesetz personenbezogene Bezeichnungen nur in männlicher oder weiblicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise.

§ 2
Geltungsbereich

(1) Dieses Gesetz ist auf die im Rahmen des § 1 erfolgende Verwendung personenbezogener Daten in Niederösterreich anzuwenden. Dies gilt nicht für die Fälle des Abs. 3.

(2) Auf die Verwendung personenbezogener Daten im Ausland ist dieses Gesetz anzuwenden, wenn die Verwendung

- in anderen Mitgliedstaaten der Europäischen Union
- für Zwecke einer in Niederösterreich gelegenen Haupt- oder Zweigniederlassung eines Auftraggebers

geschieht.

(3) Das Recht des Sitzstaates des Auftraggebers ist auf eine Datenanwendung in Niederösterreich anzuwenden, wenn

- ein Auftraggeber des privaten Bereichs
- mit Sitz in einem anderen Mitgliedstaat der Europäischen Union
- personenbezogene Daten in Niederösterreich zu einem Zweck verwendet, der keiner in Niederösterreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.

(4) Dieses Gesetz ist nicht anzuwenden auf

- die Verwendung personenbezogener Daten durch natürliche Personen für ausschließlich persönliche oder familiäre Tätigkeiten;
- die ausschließliche Durchfuhr personenbezogener Daten.

§ 3
Begriffsbestimmungen

Im Sinne dieses Gesetzes gelten als:

1. **Daten (personenbezogene Daten)**: Angaben über Betroffene (Z. 4), deren Identität bestimmt oder bestimmbar ist;
2. **nur indirekt personenbezogene Daten:** Daten für einen Auftraggeber (Z. 5), Dienstleister (Z. 6) oder Empfänger einer Übermittlung (Z. 15), deren Personenbezug derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;
3. **sensible Daten (besonders schutzwürdige Daten):** Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;
4. **Betroffener:** jede vom Auftraggeber (Z. 5) verschiedene **natürliche Person**, deren Daten verwendet werden (Z. 11);
5. **Auftraggeber:**
   - natürliche oder juristische Personen,
   - Personengemeinschaften oder
   - Organe einer Gebietskörperschaft und die Geschäftsapparate solcher Organe,

   wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten

für einen bestimmten Zweck zu verarbeiten (Z. 12). Dies unabhängig davon, ob sie die Verarbeitung selbst durchführen oder dazu einen anderen heranziehen.
Als Auftraggeber gelten sie auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen, und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten.

Der Auftragnehmer gilt jedoch als Auftraggeber, wenn

- ihm anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt wurde oder
- er 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 eigenverantwortlich zu treffen hat;

6. **Dienstleister:**
   - natürliche oder juristische Personen,
   - Personengemeinschaften oder
   - Organe einer Gebietskörperschaft und die Geschäftsapparate solcher Organe,

   wenn sie Daten im Auftrag verwenden (Z. 11);
7. **Datei:** strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;
8. **Datenanwendung:** die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z. 11), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind;
9. **Datenanwendung des öffentlichen Bereichs:** Datenanwendungen, die für
   - Auftraggeber, die in Formen des öffentlichen Rechts eingerichtet sind oder
   - Auftraggeber, die in Formen des Privatrechts eingerichtet aber in Vollziehung der Gesetze tätig sind

   durchgeführt werden;
10. **Datenanwendung des privaten Bereichs:** Datenanwendungen, die nicht für Auftraggeber im Sinne der Z. 9 durchgeführt werden;
11. **Verwenden von Daten:** jede nicht automationsunterstützte Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten (Z. 12) als auch das Übermitteln (Z. 15) von Daten;

12. **Verarbeiten von Daten:** das Ermitteln, Erfassen, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Benützen, Überlassen (Z. 14), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittelns (Z. 15) von Daten, soweit diese Schritte nicht automationsunterstützt erfolgen;
13. **Ermitteln von Daten:** das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden;
14. **Überlassen von Daten:** die Weitergabe von Daten vom Auftraggeber an einen Dienstleister;
15. **Übermitteln von Daten:** die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;
16. **Zustimmung:** die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;
17. **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;
18. **Datenschutzkommission:** die nach dem 7. Abschnitt des DSG 2000 eingerichtete Datenschutzkommission;
19. **DSG 2000:** Datenschutzgesetz 2000 – DSG 2000, BGBl. I Nr. 165/1999.

2. Abschnitt
Verwendung von Daten

§ 4
Grundsätze

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 § 16 Abs. 1 zulässig;

3. verwendet werden, soweit sie für den Zweck der Datenanwendung wesentlich sind und über diesen Zweck nicht hinausgehen;
4. so verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig sind. Erforderlichenfalls sind sie auf den neuesten Stand zu bringen;
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.

§ 5
Festlegung von Treu und Glauben

(1) Für den privaten Bereich können

- die gesetzlichen Interessenvertretungen,
- die sonstigen Berufsverbände und
- vergleichbare Einrichtungen

mit Verhaltensregeln festlegen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist.

(2) Solche Verhaltensregeln müssen vor ihrer Veröffentlichung

- der Landesregierung zur Begutachtung vorgelegt werden und
- von der Landesregierung als mit den Bestimmungen dieses Gesetzes übereinstimmend erachtet werden.

§ 6
Pflichten des Auftraggebers

(1) Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der in § 4 genannten Grundsätze. Dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.

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

§ 7
Zulässigkeit der Verwendung von Daten

(1) Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung

1. von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und
2. die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzen.

(2) Daten dürfen nur übermittelt werden, wenn

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

(3) Die Zulässigkeit einer Datenverwendung setzt voraus, dass

1. die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und
2. dass die Grundsätze des § 4 eingehalten werden.

§ 8
Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten

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

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder

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

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

(3) Schutzwürdige Geheimhaltungsinteressen sind aus dem Grunde des Abs. 1 Z. 4 insbesondere dann nicht verletzt, wenn die Verwendung der Daten
1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder
2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder
3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder
4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich ist oder
5. zur Geltendmachung , Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat.

(4) Die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verstößt – unbeschadet der Bestimmungen des Abs. 2 – nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn
1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht oder

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

§ 9

Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

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

1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder
2. die Daten in nur indirekt personenbezogener Form verwendet werden oder
3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen, oder
4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht oder
5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben, oder
6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder
8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder

9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
10. Daten für private Zwecke oder für wissenschaftliche Forschung oder Statistik gemäß § 16 Abs. 1 oder zur Benachrichtigung oder Befragung des Betroffenen gemäß § 16 Abs. 2 verwendet werden oder
11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz, BGBl. Nr. 22/1974 in der Fassung BGBl. I Nr. 14/2000, zustehenden Befugnisse zur Datenverwendung unberührt bleiben, oder
12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich sind, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder
13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten und es sich hiebei um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben; diese Daten dürfen, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden.

§ 10

Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen

(1) Auftraggeber dürfen bei ihren Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten.

(2) Der Auftraggeber hat mit dem Dienstleister die dafür notwendigen Vereinbarungen zu treffen. Er hat sich von ihrer Einhaltung zu überzeugen, indem er die erforderlichen Informationen über die vom Dienstleister tatsächlich getroffenen Maßnahmen einholt.

(3) Beabsichtigt ein Auftraggeber des öffentlichen Bereichs, einen Dienstleister im Rahmen einer Datenanwendung heranzuziehen, die der Vorabkontrolle gemäß § 18 unterliegt, hat er dies der Datenschutzkommission mitzuteilen.
Dies gilt nicht, wenn

- der Auftraggeber den Dienstleister auf Grund ausdrücklicher gesetzlicher Ermächtigung in Anspruch nimmt oder
- als Dienstleister eine Organisationseinheit tätig wird, die mit dem Auftraggeber oder einem diesem übergeordneten Organ in einem Über- oder Unterordnungsverhältnis steht.

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

§ 11
Pflichten des Dienstleisters

Der Dienstleister hat unabhängig allfälliger vertraglicher Vereinbarungen die Pflichten im Sinne des § 11 des DSG 2000.

§ 12
Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland

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

(2) Keiner Genehmigung gemäß § 13 bedarf weiters der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutz. Die Landesregierung stellt mit Verordnung fest, welche Drittstaaten angemessenen Datenschutz gewährleisten.

Maßgebend für die Angemessenheit des Schutzes ist

- die Ausgestaltung der Grundsätze des § 4 in der ausländischen Rechtsordnung und
- das Vorhandensein wirksamer Garantien für ihre Durchsetzung.

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

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

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

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

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

(5) Voraussetzung für die Zulässigkeit jeder Übermittlung oder Überlassung in das Ausland ist die Zulässigkeit der Datenanwendung im Inland gemäß § 7. Bei Überlassungen ins Ausland muss darüber hinaus die schriftliche Zusage des ausländischen Dienstleisters an den inländischen Auftraggeber – oder in den Fällen des § 13 Abs. 4

an den inländischen Dienstleister – vorliegen, dass er die Dienstleisterpflichten gemäß § 11 einhalten werde. Dies entfällt, wenn die Dienstleistung im Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind.

§ 13

Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland

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

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

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

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

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

(5) Die Übermittlung von Daten an ausländische Vertretungsbehörden oder zwischenstaatliche Einrichtungen in Niederösterreich 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.

(7) Die Datenschutzkommission hat binnen sechs Wochen ab Einlangen der Anzeige gemäß Abs. 6 mit Bescheid den angezeigten Datenverkehr zu untersagen, wenn er

- keiner der in der Verordnung geregelten Kategorien zuzurechnen ist oder
- den Voraussetzungen gemäß § 12 Abs. 5 nicht entspricht;

andernfalls ist die Übermittlung oder Überlassung der Daten in das Ausland zulässig.

3. Abschnitt
Datensicherheit

§ 14
Datensicherheitsmaßnahmen

Der Auftraggeber oder Dienstleister hat für alle Organisationseinheiten zur Gewährleistung der Datensicherheit Maßnahmen zu treffen. § 14 Abs.1 und 2 sowie Abs. 4 bis 6 des DSG 2000 gelten sinngemäß.

§ 15
Datengeheimnis

Daten sind im Sinne des § 15 des DSG 2000 geheim zu halten.

§ 16
Besondere Verwendungszwecke

(1) Die Verwendung von Daten für wissenschaftliche oder statistische Untersuchungen ist nach den Bestimmungen des § 46 des DSG 2000 zulässig.

(2) Die Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen ist nach den Bestimmungen des § 47 des DSG 2000 zulässig.

4. Abschnitt
Publizität der Datenanwendungen

§ 17
Auskunftspflicht

Der Auftraggeber hat jedermann auf Anfrage folgende Angaben über seine Datenanwendungen bekannt zu geben:

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

5. Abschnitt
Aufnahme der Datenanwendung

§ 18
Vorabkontrolle

(1) Datenanwendungen, die

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

dürfen erst nach einer Vorabkontrolle durch die Datenschutzkommission aufgenommen werden.

(2) Dies gilt nicht für Datenanwendungen, die

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

§ 19
Verfahren zur Vorabkontrolle

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

1. den Namen (die sonstige Bezeichnung) und die Anschrift sowie eines allfälligen Vertreters gemäß § 6 Abs. 2, und
2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit, soweit dies erforderlich ist, und
3. den Zweck der Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z. 2 ergeben, und

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

(2) Eine Mitteilung 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 hinreichenden Informationen darüber gewinnen kann, ob durch die Datenanwendung seine schutzwürdigen Geheimhaltungsinteressen verletzt sein könnten. Unstimmigkeit liegt insbesondere auch dann vor, wenn der Inhalt einer Datenanwendung nicht durch die angegebenen Rechtsgrundlagen gedeckt ist.

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

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

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

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

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

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

6. Abschnitt
Die Rechte des Betroffenen

§ 20
Auskunftsrecht

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

(2) Die Auskunft hat

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

in allgemein verständlicher Form anzuführen.
Auf Verlangen des Betroffenen sind auch Namen und Adresse von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Mit Zustimmung des Betroffenen kann an Stelle der schriftlichen Auskunft auch eine mündliche

Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.

(3) Die Auskunft ist nicht zu erteilen,

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

Überwiegende öffentliche Interessen können sich hiebei aus der Notwendigkeit

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

§ 21
Auskunftsverfahren

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

(2) Innerhalb von acht Wochen nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Betroffene am Verfahren nicht gemäß Abs. 1 mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.

(3) Die Auskunft ist unentgeltlich zu erteilen, wenn

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

In allen anderen Fällen kann ein pauschalierter Kostenersatz von 260 S verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.

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

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

(6) Im Falle der auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 5 eigenverantwortlichen Entscheidung über die Durchführung einer Datenanwendung durch einen Auftragnehmer gemäß § 3 Z. 5, vierter Satz, kann der Betroffene sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Betroffenen, soweit dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des eigenverantwortlichen Auftragnehmers mitzuteilen, damit der Betroffene sein Auskunftsrecht gemäß § 20 Abs. 1 gegen diesen geltend machen kann.

§ 22

Recht auf Richtigstellung oder Löschung

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

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

(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. Dies gilt nicht, wenn ihre Archivierung rechtlich zulässig ist und wenn 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 § 16 Abs. 1.

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

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

(7) Dem Antrag ist innerhalb von acht Wochen nach Einlangen zu entsprechen und 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 der Betroffene bestreitet, und lässt sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen, so ist auf Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. Der Bestreitungsvermerk darf nur mit Zustimmung des Betroffenen oder auf Grund einer Entscheidung des zuständigen Gerichtes oder der Datenschutzkommission gelöscht werden.

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

§ 23
Widerspruchsrecht

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

(2) Abs. 1 gilt nicht für die gesetzlich vorgesehene Verwendung von Daten.

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

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

Die durch die §§ 20 bis 23 gewährten Rechte können nicht geltend gemacht werden, soweit nur indirekt personenbezogene Daten verwendet werden.

7. Abschnitt
Rechtsschutz

§ 25
Kontrollbefugnisse der Datenschutzkommission

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

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

(3) Datenanwendungen, die der Vorabkontrolle gemäß § 18 unterliegen, dürfen auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden.

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

- Räume, in welchen Datenanwendungen vorgenommen werden, zu betreten,
- die zu überprüfenden Verarbeitungen durchzuführen sowie
- Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen.

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

(5) Informationen, die der Datenschutzkommission oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Die Pflicht zur Verschwiegenheit besteht auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden.

(6) Ergibt die Einschau den Verdacht

- einer strafbaren Handlung nach § 30 dieses Gesetzes oder
- eines Verbrechens nach § 278a StGB (kriminelle Organisation), BGBl. Nr. 60/1974 in der Fassung BGBl. I Nr. 146/1999, oder
- eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt,

ist jedoch Anzeige zu erstatten und hinsichtlich solcher Verbrechen und Vergehen auch dem Ersuchen der Strafgerichte nach § 26 StPO, BGBl. Nr. 631/1975 in der Fassung BGBl. I Nr. 191/1999, zu entsprechen.

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

1. Anzeige nach § 30 erstatten, oder
2. bei schwer wiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 27 Abs. 2 erheben, oder
3. bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, dass der Empfehlung der Datenschutzkommission entsprochen wird, oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen

wurde. Die Begründung darf von der Datenschutzkommission der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.

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

§ 26
Beschwerde an die Datenschutzkommission

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

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

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

§ 27
Anrufung der Gerichte

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

(2) Die Datenschutzkommission hat in Fällen, in welchen der begründete Verdacht einer schwer wiegenden Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs besteht, gegen diesen eine Feststellungsklage (§ 228 ZPO), RGBl. Nr. 113/1885 in der Fassung BGBl. I Nr. 125/1999, beim zuständigen Gericht zu erheben.

§ 28
Schadenersatz

Ein Auftraggeber oder Dienstleister, der Daten schuldhaft entgegen den Bestimmungen dieses Gesetzes verwendet, hat dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. Im Übrigen gilt § 33 DSG 2000.

§ 29
Gemeinsame Bestimmungen

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

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

(3) Ist die vermutete Verletzung schutzwürdiger Geheimhaltungsinteressen eines Betroffenen im Inland 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.

8. Abschnitt
Verwaltungsstrafbestimmung

§ 30

(1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 100.000 S zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält oder
2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 15) übermittelt, insbesondere Daten, die ihm gemäß § 16 anvertraut wurden, vorsätzlich für andere Zwecke verwendet oder
3. Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtigstellt oder nicht löscht oder
4. Daten vorsätzlich entgegen § 21 Abs. 4 vernichtet.

(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 50.000 S zu ahnden ist, wer

1. Daten ermittelt, verarbeitet oder übermittelt, ohne eine Mitteilungspflicht gemäß § 19 erfüllt zu haben oder

2. Daten ins Ausland übermittelt oder überläßt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 eingeholt zu haben oder
3. trotz einer Empfehlung der Datenschutzkommission die Auskunftsspflicht gemäß § 17 verletzt oder
4. die gemäß § 14 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht läßt.

(3) Der Versuch ist strafbar.

(4) Die Strafe des Verfalls von Datenträgern kann ausgesprochen werden (§§ 10, 17 und 18 VStG, BGBl. Nr. 52/1991 in der Fassung BGBl. I Nr. 191/1999), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 oder 2 in Zusammenhang stehen.

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

9. Abschnitt
Schluss- und Übergangsbestimmungen

§ 31
Mitteilungen an die Europäische Kommission und an die anderen Mitgliedstaaten der Europäischen Union

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

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

§ 32
Anhörungsverfahren, Berichtspflicht

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

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

§ 33
Datenanwendungen des Landtages

Der Präsident des Landtages ist Auftraggeber jener Datenanwendungen, die für Zwecke der ihm gemäß § 22 der Geschäftsordnung – LGO 1979, LGBl. 0010, übertragenen Angelegenheiten durchgeführt werden. Übermittlungen von Daten aus solchen Datenanwendungen dürfen nur über Auftrag des Präsidenten des Landtags vorgenommen werden. Der Präsident trifft Vorsorge dafür, daß im Falle eines Übermittlungsauftrags die Voraussetzungen des § 7 Abs. 2 vorliegen und insbesondere die Zustimmung des Betroffenen in jenen Fällen eingeholt wird, in welchen dies gemäß § 7 Abs. 2 mangels einer anderen Rechtsgrundlage für die Übermittlung notwendig ist.

§ 34
Umgesetzte EG-Richtlinien

Durch dieses Gesetz wird folgende Richtlinie der Europäischen Gemeinschaften umgesetzt:
Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl.Nr. L 281, vom 23.11.1995, S. 31

§ 35
Inkrafttreten

Dieses Gesetz tritt am 1. Jänner 2001 in Kraft.

§ 36
Übergangsbestimmungen

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

1. bis zum 1. Oktober 2007 mit den §§ 4, 5, 6, 7,8 und 9
2. bis zum 1. Jänner 2003 mit den übrigen Bestimmungen dieses Gesetzes

in Einklang zu bringen.

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