

Rahmenbedingungen für ein logisches österreichisches Gesundheitsdatennetz („MAGDA-LENA“)

**STRING-Kommission beim Bundesministerium
für soziale Sicherheit und Generationen**

Teil 4: Relevante Gesetzesstellen

Version 2.0 vom 21. 6. 2000

Die aktuelle Version im Internet:

www.bmsg.gv.at

bzw.

www.akh-wien.ac.at/STRING/

3. Relevante Gesetzesstellen im Einzelnen

3.1. Datenschutzgesetz 2000 (DSG 2000, BGBl I Nr. 165/1999) - Rechtsnormen im Einzelnen

Datenschutzgesetz 2000 – Angeführte Rechtsnormen

- § 1 Grundrecht auf Datenschutz
- § 2 Zuständigkeit
- § 3 Räumlicher Anwendungsbereich
- § 4 Definitionen
- § 5 Öffentlicher und privater Bereich
- § 6 Grundsätze
- § 7 Zulässigkeit der Verwendung von Daten
- § 8 Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten
- § 9 Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten
- § 10 Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen
- § 14 Datensicherheitsmaßnahmen
- § 15 Datengeheimnis
- § 26 Auskunftsrecht
- § 27 Recht auf Richtigstellung oder Löschung
- § 28 Widerspruchsrecht
- § 29 Die Rechte des Betroffenen bei Verwendung nur indirekt
- § 45 Private Zwecke
- § 46 Wissenschaftliche Forschung und Statistik
- § 47 Zurverfügungstellung von Adressen zur Benachrichtigung und
- § 51 Datenverwendung in Gewinn- oder Schädigungsabsicht
- § 52 Verwaltungsstrafbestimmung

Datenschutzgesetz 2000 (DSG 2000, BGBl I Nr. 165/1999) - Rechtsnormen im Einzelnen

Artikel 1: (Verfassungsbestimmung)

§ 1 Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter

Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, d.h. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

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

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

§ 2 Zuständigkeit

§ 2. (1) Bundessache ist die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr.

(2) Die Vollziehung solcher Bundesgesetze steht dem Bund zu. Soweit solche Daten von einem Land, im Auftrag eines Landes, von oder im Auftrag von juristischen Personen, die durch Gesetz eingerichtet sind und deren Einrichtung hinsichtlich der Vollziehung in die Zuständigkeit der Länder fällt, verwendet werden, sind diese Bundesgesetze von den Ländern zu vollziehen, soweit nicht durch Bundesgesetz die Datenschutzkommission, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden.

§ 3 Räumlicher Anwendungsbereich

§ 3. (1) Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von personenbezogenen Daten im Inland anzuwenden. Darüber hinaus ist dieses Bundesgesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung (§ 4 Z 15) eines Auftraggebers (§ 4 Z 4) geschieht.

(2) Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.

(3) Weiters ist dieses Bundesgesetz nicht anzuwenden, soweit personenbezogene Daten durch das Inland nur durchgeführt werden.

(4) Von den Abs. 1 bis 3 abweichende gesetzliche Regelungen sind nur in Angelegenheiten zulässig, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

1. Abschnitt: Allgemeines

§ 4 Definitionen

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

- 1 „Daten“ („personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;
2. „sensible Daten“ („besonders schutzwürdige Daten“): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;
3. „Betroffener“: jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;
4. „Auftraggeber“: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Z 9), und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem anderen

- Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten. Wurde jedoch dem Auftragnehmer anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt oder hat der Auftragnehmer die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten, auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 6 Abs. 4 eigenverantwortlich zu treffen, so gilt der mit der Herstellung des Werkes Betraute als datenschutzrechtlicher Auftraggeber;
5. „Dienstleister“: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden (Z 8);
 6. „Datei“: strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;
 7. „Datenanwendung“ (früher: „Datenverarbeitung“): die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);
 8. „Verwenden von Daten“: jede Art der Handhabung von Daten 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 den Auftraggeber oder Dienstleister mit Ausnahme des Übermittels (Z 12) von Daten;
 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 vom Auftraggeber an einen Dienstleister;
 12. „Übermitteln von Daten“: die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichende solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;
 13. „Informationsverbundsystem“: die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, dass jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden;
 14. „Zustimmung“: die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;
 15. „Niederlassung“: jede durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne

Rechtspersönlichkeit, die am Ort ihrer Einrichtung auch tatsächlich Tätigkeiten ausübt.

§ 5 Öffentlicher und privater Bereich

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

(2) Auftraggeber des öffentlichen Bereichs sind alle Auftraggeber,

1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder
2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

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

2. Abschnitt: Verwendung von Daten

§ 6 Grundsätze

§ 6. (1) Daten dürfen nur

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

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

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

(4) Zur näheren Festlegung dessen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist, können für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten. Solche Verhaltensregeln dürfen nur veröffentlicht werden, nachdem sie dem Bundeskanzler zur Begutachtung vorgelegt wurden und dieser ihre Übereinstimmung mit den Bestimmungen dieses Bundesgesetzes begutachtet und als gegeben erachtet hat.

§ 7 Zulässigkeit der Verwendung von Daten

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

(2) Daten dürfen nur übermittelt werden, wenn

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

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

§ 8 Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten

§ 8. (1) Gemäß § 1 Abs. 1 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. 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 berechnete 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 § 28 Widerspruch zu erheben, bleibt unberührt.

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

1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche 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 Bundesgesetz gewährleistet.

§ 9 Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

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

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

5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben, oder
6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder
8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist oder
9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
10. Daten für private Zwecke gemäß § 45 oder für wissenschaftliche Forschung oder Statistik gemäß § 46 oder zur Benachrichtigung oder Befragung des Betroffenen gemäß § 47 verwendet werden oder
11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse im Hinblick auf die Datenverwendung unberührt bleiben, oder
12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder
13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten und es sich hierbei 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

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

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

3. Abschnitt: Datensicherheit

§ 14 Datensicherheitsmaßnahmen

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

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

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

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

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

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

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

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

§ 15 Datengeheimnis

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

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

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

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

5. Abschnitt: Die Rechte des Betroffenen

§ 26 Auskunftsrecht

§ 26. (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. 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 hierfür 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 anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.

(2) Die Auskunft ist nicht zu erteilen, soweit dies zum Schutz des 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 hierbei aus der Notwendigkeit

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
3. der Sicherung der Interessen der umfassenden Landesverteidigung oder
4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten ergeben. Die Zulässigkeit der Auskunftsverweigerung aus den Gründen der Z 1 bis 5 unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission gemäß § 31 Abs. 4.

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

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

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Auskunftsverweigerung erfordert, folgendermaßen vorzugehen: Es ist in allen Fällen, in welchen keine Auskunft erteilt wird - also auch weil tatsächlich keine Daten verwendet werden -, anstelle einer inhaltlichen Begründung der Hinweis zu geben, dass keine der Auskunftspflicht unterliegenden Daten über den Betroffenen verwendet werden. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.

(6) Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Betroffene im laufenden Jahr noch kein Auskunftersuchen 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 erwachsener höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.

(7) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Betroffenen innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die Datenschutzkommission bis zum rechtskräftigen Abschluss des Verfahrens nicht vernichten.

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

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

(10) Im Falle der auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 6 Abs. 4 eigenverantwortlichen Entscheidung über die Durchführung einer Datenanwendung durch einen Auftragnehmer gemäß § 4 Z 4, dritter Satz, kann der Betroffene sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Betroffenen, soweit dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des eigenverantwortlichen Auftragnehmers mitzuteilen, damit der Betroffene sein Auskunftsrecht gemäß Abs. 1 gegen diesen geltend machen kann.

§ 27 Recht auf Richtigstellung oder Löschung

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

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

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

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

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

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

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

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

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

1. die Verpflichtung zur Richtigstellung und Löschung von Amts wegen oder
2. das Verfahren der Durchsetzung und die Zuständigkeit zur Entscheidung über Berichtigungs- und Löschanträge von Betroffenen durch Bundesgesetz nicht anderes bestimmt ist.

§ 28 Widerspruchsrecht

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

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

§ 29 Die Rechte des Betroffenen bei Verwendung nur indirekt

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

8. Abschnitt: Besondere Verwendungszwecke von Daten

§ 45 Private Zwecke

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

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

§ 46 Wissenschaftliche Forschung und Statistik

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

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

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

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

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

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

Sollen sensible Daten übermittelt werden, muss ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muss gewährleistet sein, dass die Daten beim Empfänger nur von Personen verwendet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen

Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten, notwendig ist.

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

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

§ 47 Zurverfügungstellung von Adressen zur Benachrichtigung und

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

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

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

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

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

(4) Die Datenschutzkommission hat die Genehmigung zur Übermittlung zu erteilen, wenn der Antragsteller das Vorliegen der in Abs. 3 genannten Voraussetzungen

glaubhaft macht und überwiegende schutzwürdige Geheimhaltungsinteressen der Betroffenen der Übermittlung nicht entgegenstehen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten als Auswahlkriterium, notwendig ist.

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

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

10. Abschnitt: Strafbestimmungen

§ 51 Datenverwendung in Gewinn- oder Schädigungsabsicht

§ 51. (1) Wer in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

§ 52 Verwaltungsstrafbestimmung

§ 52. (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 260 000 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 §§ 46 oder 47 anvertraut wurden, vorsätzlich für andere Zwecke verwendet oder
3. Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtiggestellt oder nicht löscht oder
4. Daten vorsätzlich entgegen § 26 Abs. 7 löscht.

(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 130 000 S zu ahnden ist, wer

1. Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß § 17 erfüllt zu haben oder
2. Daten ins Ausland übermittelt oder überlässt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 eingeholt zu haben oder
3. seine Offenlegungs- oder Informationspflichten gemäß den §§ 23, 24 oder 25 verletzt oder
4. die gemäß § 14 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht lässt.

(3) Der Versuch ist strafbar.

(4) Die Strafe des Verfalls von Datenträgern und Programmen kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 oder 2 in Zusammenhang stehen.

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

3.2. Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl. I Nr. 190/1999) – Angeführte Rechtsnormen

- § 1 Gegenstand und Anwendungsbereich
- § 2 Begriffsbestimmungen
- § 3 Allgemeine Rechtswirkungen
- § 4 Besondere Rechtswirkungen
- § 21 Pflichten des Signators
- § 22 Datenschutz
- § 26 Verwaltungsstrafbestimmungen

1. Abschnitt

§ 1. (1) Dieses Bundesgesetz regelt den rechtlichen Rahmen für die Erstellung und Verwendung elektronischer Signaturen sowie für die Erbringung von Signatur- und Zertifizierungsdiensten.

(2) Dieses Bundesgesetz ist auch anzuwenden in geschlossenen Systemen, sofern deren Teilnehmer dies vereinbart haben, sowie im offenen elektronischen Verkehr mit Gerichten und anderen Behörden, sofern durch Gesetz nicht anderes bestimmt ist.

§ 2. Im Sinne dieses Bundesgesetzes bedeuten

1. elektronische Signatur: elektronische Daten, die anderen elektronischen Daten beigelegt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators, dienen;
2. Signator: eine natürliche Person, der Signaturerstellungsdaten und die entsprechenden Signaturprüfdaten zugeordnet sind und die entweder im eigenen oder im fremden Namen eine elektronische Signatur erstellt, oder ein Zertifizierungsdiensteanbieter, der Zertifikate für die Erbringung von Zertifizierungsdiensten verwendet;
3. sichere elektronische Signatur: eine elektronische Signatur, die
 - a) ausschließlich dem Signator zugeordnet ist,
 - b) die Identifizierung des Signators ermöglicht,
 - c) mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann,
 - d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Veränderung der Daten festgestellt werden kann, sowie
 - e) auf einem qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen, erstellt wird;
4. Signaturerstellungsdaten: einmalige Daten wie Codes oder private Signaturschlüssel, die vom Signator zur Erstellung einer elektronischen Signatur verwendet werden;
5. Signaturerstellungseinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturerstellungsdaten verwendet wird;

6. Signaturprüfdaten: Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden;
7. Signaturprüfeinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturprüfdaten verwendet wird;
8. Zertifikat: eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird;
9. qualifiziertes Zertifikat: ein Zertifikat, das die Angaben des § 5 enthält und von einem den Anforderungen des § 7 entsprechenden Zertifizierungsdiensteanbieter ausgestellt wird;
10. Zertifizierungsdiensteanbieter: eine natürliche oder juristische Person oder eine sonstige rechtsfähige Einrichtung, die Zertifikate ausstellt oder andere Signatur- und Zertifizierungsdienste erbringt;
11. Signatur- und Zertifizierungsdienste: die Bereitstellung von Signaturprodukten und -verfahren, die Ausstellung, Erneuerung und Verwaltung von Zertifikaten, Verzeichnis-, Widerrufs-, Registrierungs- und Zeitstempeldienste sowie Rechner- und Beratungsdienste im Zusammenhang mit elektronischen Signaturen;
12. Zeitstempeldienst: eine elektronisch signierte Bescheinigung eines Zertifizierungsdiensteanbieters, dass bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen sind;
13. Signaturprodukt: Hard- oder Software bzw. deren spezifische Komponenten, die für die Erstellung und Überprüfung elektronischer Signaturen oder von einem Zertifizierungsdiensteanbieter für die Bereitstellung von Signatur- oder Zertifizierungsdiensten verwendet werden;
14. Kompromittierung: die Beeinträchtigung von Sicherheitsmaßnahmen oder Sicherheitstechnik, sodass das vom Zertifizierungsdiensteanbieter zugrundegelegte Sicherheitsniveau nicht eingehalten ist.

2. Abschnitt

Rechtserheblichkeit elektronischer Signaturen

§ 3. (1) Im Rechts- und Geschäftsverkehr können Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen verwendet werden.

(2) Die rechtliche Wirksamkeit einer elektronischen Signatur und deren Verwendung als Beweismittel können nicht allein deshalb ausgeschlossen werden, weil die elektronische Signatur nur in elektronischer Form vorliegt, weil sie nicht auf einem qualifizierten Zertifikat oder nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder weil sie nicht unter Verwendung von technischen Komponenten und Verfahren im Sinne des § 18 erstellt wurde.

§ 4. (1) Eine sichere elektronische Signatur erfüllt das rechtliche Erfordernis einer eigenhändigen Unterschrift, insbesondere der Schriftlichkeit im Sinne des § 886 ABGB, sofern durch Gesetz oder Parteienvereinbarung nicht anderes bestimmt ist.

(2) Eine sichere elektronische Signatur entfaltet nicht die Rechtswirkungen der Schriftlichkeit im Sinne des § 886 ABGB bei

1. Rechtsgeschäften des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind,
2. anderen Willenserklärungen oder Rechtsgeschäften, die zu ihrer Wirksamkeit an die Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts gebunden sind,
3. Willenserklärungen, Rechtsgeschäften oder Eingaben, die zu ihrer Eintragung in das Grundbuch, das Firmenbuch oder ein anderes öffentliches Register einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts bedürfen, und
4. einer Bürgschaftserklärung (§ 1346 Abs. 2 ABGB).

(3) Die Bestimmung des § 294 ZPO über die Vermutung der Echtheit des Inhalts einer unterschriebenen Privaturkunde ist auf elektronische Dokumente, die mit einer sicheren elektronischen Signatur versehen sind, anzuwenden.

(4) Die Rechtswirkungen der Abs. 1 und 3 treten nicht ein, wenn nachgewiesen wird, dass die Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen nicht eingehalten oder die zur Einhaltung dieser Sicherheitsanforderungen getroffenen Vorkehrungen kompromittiert wurden.

§ 21. Der Signator hat die Signaturerstellungsdaten sorgfältig zu verwahren, soweit zumutbar Zugriffe auf Signaturerstellungsdaten zu verhindern und deren Weitergabe zu unterlassen. Er hat den Widerruf des Zertifikats zu verlangen, wenn die Signaturerstellungsdaten abhanden kommen, wenn Anhaltspunkte für eine Kompromittierung der Signaturerstellungsdaten bestehen oder wenn sich die im Zertifikat bescheinigten Umstände geändert haben.

§ 22. (1) Ein Zertifizierungsdiensteanbieter darf nur jene personenbezogenen Daten verwenden, die er zur Durchführung der erbrachten Dienste benötigt. Diese Daten dürfen nur unmittelbar beim Betroffenen selbst oder mit seiner ausdrücklichen Zustimmung bei einem Dritten erhoben werden.

(2) Bei Verwendung eines Pseudonyms hat der Zertifizierungsdiensteanbieter die Daten über die Identität des Signators zu übermitteln, sofern an der Feststellung der Identität ein überwiegendes berechtigtes Interesse im Sinne des § 8 Abs. 1 Z 4 und Abs. 3 DSG 2000 glaubhaft gemacht wird. Die Übermittlung ist zu dokumentieren.

(3) Die Auskunfts- und Mitwirkungspflichten des Zertifizierungsdiensteanbieters gegenüber Gerichten und anderen Behörden bleiben unberührt.

§ 26. (1) Eine Verwaltungsübertretung begeht und ist mit Geldstrafe bis zu 56 000 S zu bestrafen, wer fremde Signaturerstellungsdaten ohne Wissen und Willen des Signators missbräuchlich verwendet.

(2) Ein Zertifizierungsdiensteanbieter begeht eine Verwaltungsübertretung und ist mit Geldstrafe bis zu 112 000 S zu bestrafen, wenn er

1. entgegen § 9 Abs. 1 seine Widerrufspflicht verletzt,
2. entgegen § 11 seine Dokumentationspflicht verletzt,
3. entgegen § 16 Abs. 1 nicht Einsicht in die dort genannten Bücher, sonstige Aufzeichnungen oder Unterlagen gewährt oder nicht die notwendigen Auskünfte erteilt oder
4. entgegen § 20 Abs. 1 und 3 den Zertifikatswerber nicht unterrichtet.

(3) Ein Zertifizierungsdiensteanbieter begeht eine Verwaltungsübertretung und ist mit Geldstrafe bis zu 224 000 S zu bestrafen, wenn er

1. entgegen § 6 Abs. 2 die Aufnahme seiner Tätigkeit nicht anzeigt oder das Sicherheitskonzept oder das Zertifizierungskonzept nicht vorlegt,
2. entgegen § 6 Abs. 5 nicht alle Umstände, die eine ordnungsgemäße und dem Sicherheits- sowie dem Zertifizierungskonzept entsprechende Tätigkeit nicht mehr ermöglichen, der Aufsichtsstelle anzeigt,
3. entgegen § 7 Abs. 1 Z 2 keinen geeigneten Widerrufsdienst oder keinen geeigneten Verzeichnisdienst führt,
4. entgegen § 7 Abs. 1 Z 8 keine geeigneten Vorkehrungen dafür trifft, dass die Signaturerstellungsdaten der Signatoren weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden können,
5. entgegen § 18 keine geeigneten technischen Komponenten und Verfahren für sichere elektronische Signaturen verwendet, bereitstellt oder bezeichnet oder
6. trotz Untersagung durch die Aufsichtsstelle (§ 14 Abs. 2 bis 4) die ihm untersagte Tätigkeit weiterhin ausübt.

(4) Eine Verwaltungsübertretung gemäß den Abs. 1 bis 3 liegt nicht vor, wenn die Tat den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist.

(5) Im Straferkenntnis können die Gegenstände, mit denen die strafbare Handlung begangen wurde, für verfallen erklärt werden.

3.3. Krankenanstaltengesetz, BGBl. Nr. 1/1957, zuletzt geändert durch die Bundesgesetze BGBl. Nr. 732/1995 und BGBl. Nr. 853/1995 sowie BGBl. Nr. 751/1996 (Bundesgesetz, mit dem das Krankenanstaltengesetz geändert wird) – Angeführte Rechtsnormen

Soweit ersichtlich sind hier keine für MAGDA-LENA relevanten Bestimmungen enthalten.

3.4. Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Bundesgesetz, mit dem zur Bekämpfung organisierter Kriminalität besondere Ermittlungsmaßnahmen in die Strafprozessordnung eingeführt sowie das Strafgesetzbuch, das Mediengesetz, das Staatsanwaltschaftsgesetz und das Sicherheitspolizeigesetz geändert werden, das Bundesgesetz über den Schutz vor Straftaten gegen die Sicherheit von Zivilluftfahrzeugen, die Exekutionsordnung, das Zollrechts-Durchführungsgesetz, das Tilgungsgesetz 1972, das Polizeikooperationsgesetz, das Waffengebrauchsgesetz 1969 und das Strafvollzugsgesetz geändert werden (SPG-Novelle 1999, BGBl. Nr. I 146/1999)

§ 67 „DNA-Untersuchungen

§ 70 Erkennungsdienstliche Evidenzen

§ 90 Beschwerden wegen Verletzung der Bestimmungen über den Datenschutz

§ 67. (1) Die DNA eines Menschen darf im Rahmen seiner erkennungsdienstlichen Behandlung nur ermittelt werden, wenn der Betroffene in Verdacht steht, einen gefährlichen Angriff begangen zu haben, und wenn in Hinblick auf diese Tat oder die Persönlichkeit des Betroffenen erwartet werden kann, dieser werde bei Begehung weiterer gefährlicher Angriffe Spuren hinterlassen, die seine Wiedererkennung auf Grund der ermittelten genetischen Information ermöglichen würden.

(2) Genetische Information, die durch erkennungsdienstliche Maßnahmen ermittelt wurde, darf ausschließlich für Zwecke des Erkennungsdienstes ausgewertet werden. Die molekulargenetische Untersuchung hat durch einen Dienstleister zu erfolgen, dem zwar das gesamte Untersuchungsmaterial auszufolgen, nicht aber erkennungsdienstliche Identitätsdaten des Betroffenen zu übermitteln sind.

(3) Die Sicherheitsbehörden haben vertraglich dafür vorzusorgen, dass der Dienstleister nur jene Bereiche in der DNA untersucht, die der Wiedererkennung dienen, sowie dafür, dass er das Untersuchungsmaterial vernichtet, wenn die Sicherheitsbehörde zur Löschung der erkennungsdienstlichen Daten verpflichtet ist."

Dem § 70 Abs. 3 wird folgender Satz angefügt:

„Personenbezogene Daten, die eine Sicherheitsbehörde rechtmäßig ermittelt hat, dürfen im Erkennungsdienst verwendet werden, als wären sie nach den Bestimmungen dieses Hauptstückes ermittelt worden, wenn deren Ermittlung als erkennungsdienstliche Daten zu dem Zeitpunkt zulässig wäre, in dem die Daten verwendet werden sollen."

§ 90 Abs. 1 lautet:

„(1) Die Datenschutzkommission entscheidet gemäß § 14 des Datenschutzgesetzes über Beschwerden wegen Verletzung von Rechten durch Verwenden personenbezogener Daten in Angelegenheiten der Sicherheitsverwaltung entgegen den Bestimmungen des Datenschutzgesetzes. Davon ausgenommen ist die Beurteilung der

Rechtmäßigkeit der Ermittlung von Daten durch die Ausübung
verwaltungsbehördlicher Befehls- und Zwangsgewalt."

3.5. Bundesgesetz vom 25. November 1987, mit dem das Strafgesetzbuch, die Strafprozessordnung, das Strafvollzugsgesetz, das Strafvollzugsanpassungsgesetz, das Einführungsgesetz zum Strafvollzugsgesetz, das Bewährungshilfegesetz, die Bewährungshilfegesetznovelle 1980, das Tilgungsgesetz 1972, das Strafregistergesetz 1968, das Gesetz zum Schutze der persönlichen Freiheit, das Militärstrafgesetz, das Geschwornen- und Schöffenlistengesetz, das Datenschutzgesetz, das Ausfuhrverbotsgesetz, das Devisengesetz, das Nationalbankgesetz 1984, das Außenhandelsgesetz 1984 und das Allgemeine Sozialversicherungsgesetz geändert werden (Strafrechtsänderungsgesetz 1987; BGBl. Nr. 605/1987)

§ 148 a STGB Betrügerischer Datenverarbeitungsmissbrauch

23. Nach § 148 wird folgende Bestimmung eingefügt:

Betrügerischer Datenverarbeitungsmissbrauch

§ 148 a. (1) Wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern, einen anderen dadurch am Vermögen schädigt, dass er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung oder Löschung von Daten (§ 126 a Abs. 2) oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflusst, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer die Tat gewerbsmäßig begeht oder durch die Tat einen 25 000 S übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu drei Jahren, wer durch die Tat einen 500 000 S übersteigenden Schaden herbeiführt, mit Freiheitsstrafe

3.6. Bundesgesetz, mit dem zur Bekämpfung organisierter Kriminalität besondere Ermittlungsmaßnahmen in die Strafprozessordnung eingeführt sowie das Strafgesetzbuch, das Mediengesetz, das Staatsanwaltschaftsgesetz und das Sicherheitspolizeigesetz geändert werden (BGBl. I Nr. 105/1997)

VII. Automationsunterstützter Datenabgleich

§ 149i. (1) Der automationsunterstützte Abgleich von Daten (§ 3 Z 1 des Datenschutzgesetzes) einer Datenverarbeitung, die bestimmte, den mutmaßlichen Täter kennzeichnende oder ausschließende Merkmale enthalten, mit Daten einer anderen Datenverarbeitung, die solche Merkmale enthalten, um Personen festzustellen, die auf Grund dieser Merkmale als Verdächtige in Betracht kommen, ist zulässig, wenn die Aufklärung eines Verbrechens ansonsten aussichtslos oder wesentlich erschwert wäre und nur solche Daten einbezogen werden, die Gerichte und Sicherheitsbehörden für Zwecke eines Strafverfahrens oder sonst auf Grund bestehender Bundes- oder Landesgesetze ermittelt oder verarbeitet haben.

(2) Sofern die Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder eines Verbrechens nach § 278a StGB ansonsten aussichtslos oder wesentlich erschwert wäre, ist es zulässig, in einen automationsunterstützten Datenabgleich auch Daten, die den Gerichten nach § 26 zu übermitteln sind, und Daten über Personen einzubeziehen, die von einem bestimmten Unternehmen bestimmte Waren oder Dienstleistungen bezogen haben oder die Mitglieder von Personenvereinigungen des Privatrechts oder von juristischen Personen des Privatrechts oder des öffentlichen Rechts sind.

(3) Es ist unzulässig, in einen Datenabgleich Daten einzubeziehen, die die rassische Herkunft, politische Anschauungen, religiöse oder andere Überzeugungen oder Merkmale des Gesundheitszustandes oder des Sexuallebens erkennen lassen. Dieses Verbot gilt nicht für die Einbeziehung von Daten über die Staatsangehörigkeit, Daten zur tatbildmäßigen Bezeichnung einer Tätergruppe sowie von Daten, die die Sicherheitsbehörden durch erkennungsdienstliche Maßnahmen ermittelt haben, in einen Datenabgleich nach Abs. 1. Daten von Personenvereinigungen, deren Zweck in unmittelbarem Zusammenhang mit einem der besonders geschützten Merkmale steht, dürfen in einen Datenabgleich in keinem Fall einbezogen werden.

(4) Ein automationsunterstützter Abgleich von Daten ist nur zulässig, soweit die Verhältnismäßigkeit zum Zweck der Maßnahme gewahrt wird. Dabei ist insbesondere darauf Bedacht zu nehmen, dass der angestrebte Erfolg in einem vertretbaren Verhältnis zu den voraussichtlich bewirkten Eingriffen in die Rechte unbeteiligter Dritter steht, und zu prüfen, ob nicht auch mit weniger eingreifenden Maßnahmen begründete Aussicht auf den angestrebten Erfolg besteht.

§ 149j. (1) Die Entscheidung über den automationsunterstützten Datenabgleich obliegt im Fall des § 149i Abs. 1 dem Untersuchungsrichter, im Fall des § 149i Abs. 2 der

Ratskammer; sie setzt einen Antrag des Staatsanwalts voraus. Der Beschluss, mit dem der Datenabgleich angeordnet wird, hat zu enthalten:

1. die Tat, zu deren Aufklärung der Datenabgleich angeordnet wird, und ihre gesetzliche Bezeichnung,
2. die Bezeichnung jener Merkmale, nach deren Übereinstimmung gesucht wird,
3. die Datenverarbeitungen (§ 3 Z 5 des Datenschutzgesetzes) und jene ihrer Daten, welche die gesuchten Merkmale enthalten,
4. die zur Datenübermittlung verpflichteten Auftraggeber (§ 3 Z 3 des Datenschutzgesetzes),
5. die Tatsachen, aus denen sich ergibt, dass die Aufklärung der strafbaren Handlung ansonsten aussichtslos oder wesentlich erschwert wäre,
6. die Tatsachen, aus denen sich ergibt, dass der Datenabgleich verhältnismäßig ist (§ 149i Abs. 4).

(2) Ein Beschluss nach Abs. 1 ist unverzüglich dem Staatsanwalt, der Datenschutzkommission und allen Personen zuzustellen, welche durch den Datenabgleich ausgeforscht werden; die Zustellung an die ausgeforschten Personen kann jedoch aufgeschoben werden, solange dadurch der Zweck der Untersuchung gefährdet wäre. Gegen den Beschluss steht dem Staatsanwalt, der Datenschutzkommission und den ausgeforschten Personen die binnen 14 Tagen einzubringende Beschwerde an den Gerichtshof zweiter Instanz zu (§ 114).

(3) Wird einer Beschwerde gegen die Anordnung Folge gegeben oder die Anordnung des automationsunterstützten Datenabgleichs aus anderen Gründen widerrufen, so ist zugleich anzuordnen, dass alle in den Datenabgleich einbezogenen und alle durch ihn gewonnenen Daten zu vernichten und personenbezogene Daten, die auf andere Datenträger übertragen wurden, unverzüglich zu löschen sind (§ 3 Z 11 lit. a des Datenschutzgesetzes). Gleiches gilt, wenn der automationsunterstützte Datenabgleich ergibt, dass die Merkmale auf keine Person zutreffen.

§ 149k. (1) Jeder Auftraggeber einer Datenverarbeitung, deren Daten in einen Abgleich nach § 149i einbezogen werden sollen, ist verpflichtet, die Datenverarbeitung auf die gesuchten Merkmale hin zu durchsuchen und alle Daten, die diese Merkmale enthalten, in lesbarer Form zu übermitteln. Hierbei hat er sich neben den gesuchten Merkmalen auf die Übermittlung der Namen, der Geburtsdaten und der Anschriften zu beschränken. Danach hat er allfällige Ergebnisse des Suchvorganges zu vernichten und - abweichend von den §§ 7 Abs. 4 und 18 Abs. 5 des Datenschutzgesetzes - lediglich die Daten der Übermittlung und den Beschluss nach Abs. 2 zu protokollieren.

(2) Die Verpflichtung nach Abs. 1 hat der Untersuchungsrichter dem Auftraggeber mit Beschluss aufzutragen; dieser Beschluss hat die entsprechenden Anordnungen der Ratskammer (§ 149i Abs. 1 Z 2 bis 4) anzuführen. Die §§ 143 Abs. 2 und 145 sowie die Bestimmungen über die Hausdurchsuchung gelten sinngemäß.

(3) Das Vernehmungsverbot des § 151 Abs. 1 Z 1 und die Rechte von Personen, die nach § 152 Abs. 1 Z 4 oder 5 oder nach § 31 Abs. 1 des Mediengesetzes von der Verbindlichkeit zur Ablegung eines Zeugnisses gesetzlich befreit sind, dürfen nicht umgangen werden (§§ 151 Abs. 2, 152 Abs. 3 und § 31 Abs. 2 des Mediengesetzes).

§ 149l. Den automationsunterstützten Datenabgleich hat der Untersuchungsrichter oder die von ihm beauftragte Sicherheitsbehörde durchzuführen; die Sicherheitsbehörde hat dem Untersuchungsrichter das Ergebnis unverzüglich mitzuteilen. Der Untersuchungsrichter oder die Sicherheitsbehörde hat dieses Ergebnis des Datenabgleichs, soweit es für die Untersuchung von Bedeutung ist, in Schriftform zu übertragen.

VIII. Besondere Durchführungsbestimmungen

§ 149m. (1) Sämtliche Aufnahmen der Überwachung eines Fernmeldeverkehrs und - wenn das Gericht die Überwachung angeordnet hat - einer optischen oder akustischen Überwachung von Personen unter Verwendung technischer Mittel sowie sämtliche Daten, die in einen Datenabgleich einbezogen oder durch ihn gewonnen wurden, sind vom Gericht zu verwahren und nach rechtskräftigem Abschluss des Verfahrens zu löschen.

(2) Anträge auf Überwachung oder Datenabgleich (Abs. 1) und ihnen stattgebende Beschlüsse sowie Bilder und schriftliche Aufzeichnungen der im Abs. 1 erwähnten Aufnahmen und schriftliche Aufzeichnungen der Ergebnisse eines automationsunterstützten Datenabgleichs sind zunächst getrennt aufzubewahren und erst dann zum Akt zu nehmen, wenn die betreffende Anordnung dem Beschuldigten gegenüber rechtskräftig geworden ist, spätestens jedoch bei Erhebung der Anklage. Bis zur Zustellung des Anordnungsbeschlusses an den Beschuldigten können sie von der Einsicht durch diesen oder dessen Verteidiger und durch die in § 50 Abs. 1 genannten Personen ausgenommen werden, wenn zu befürchten ist, dass andernfalls der Zweck der Untersuchung oder Persönlichkeitsrechte von der Überwachung betroffener oder in den Datenabgleich einbezogener Personen gefährdet wären; im übrigen gilt § 45 Abs. 2.

(3) Solange Bilder und schriftliche Aufzeichnungen einer Überwachung nach § 149d Abs. 1 Z 3 nicht zum Akt genommen werden, sind sie samt den zugehörigen Anträgen, Beschlüssen und sonstigen Aktenstücken unter Verschluss aufzubewahren. Näheres hat der Bundesminister für Justiz durch Verordnung zu bestimmen.

IX. Besonderer Rechtsschutz

§ 149n. (1) Der Bundesminister für Justiz hat zur Wahrnehmung des besonderen Rechtsschutzes nach diesem Abschnitt nach Einholung eines gemeinsamen Vorschlages des Präsidenten des Verfassungsgerichtshofes, des Vorsitzenden der Volksanwaltschaft und des Präsidenten des Österreichischen Rechtsanwaltskammertages einen Rechtsschutz-beauftragten sowie die erforderliche

Anzahl von Stellvertretern mit deren Zustimmung für die Dauer von drei Jahren zu bestellen; Wiederbestellungen sind zulässig. Der Vorschlag hat zumindest doppelt so viele Namen zu enthalten wie Personen zu bestellen sind.

(2) Der Rechtsschutzbeauftragte und seine Stellvertreter müssen besondere Kenntnisse und Erfahrungen auf dem Gebiet der Grund- und Freiheitsrechte aufweisen und mindestens fünf Jahre in einem Beruf tätig gewesen sein, in dem der Abschluss des Studiums der Rechtswissenschaften Berufsvoraussetzung ist und dessen Ausübung Erfahrungen im Straf- und Strafverfahrensrecht mit sich brachte. Richter und Staatsanwälte des Dienststandes, Rechtsanwälte, die in die Liste der Rechtsanwälte eingetragen sind, und andere Personen, die vom Amt eines Geschworenen oder Schöffen ausgeschlossen oder zu diesem nicht zu berufen sind (§§ 2 und 3 des Geschworenen- und Schöffengesetzes 1990), dürfen nicht bestellt werden.

(3) Die Bestellung des Rechtsschutzbeauftragten und seiner Stellvertreter erlischt bei Verzicht, im Fall des Todes, mit Ende der Bestelldauer oder wegen nachträglicher Unvereinbarkeit gemäß Abs. 2. In den Fällen des § 75 oder wenn sonst ein Grund besteht, seine volle Unbefangenheit in Zweifel zu setzen, hat sich der Rechtsschutzbeauftragte von dem Zeitpunkt, in dem ihm der Grund bekannt geworden ist, des Einschreitens in der Sache zu enthalten.

(4) Der Rechtsschutzbeauftragte ist in Ausübung seines Amtes unabhängig und an keine Weisungen gebunden. Er unterliegt der Amtsverschwiegenheit. Seine Stellvertreter haben gleiche Rechte und Pflichten.

(5) Zustellungen an den Rechtsschutzbeauftragten sind im Wege der Geschäftsstelle des Obersten Gerichtshofes vorzunehmen; diese hat auch die Kanzleigeschäfte des Rechtsschutzbeauftragten wahrzunehmen.

(6) Dem Rechtsschutzbeauftragten gebührt als Entschädigung für die Erfüllung seiner Aufgaben nach diesem Abschnitt für jede, wenn auch nur begonnene Stunde ein Zehntel der Entschädigung eines Ersatzmitgliedes des Verfassungsgerichtshofes für einen Sitzungstag (§ 4 Abs. 3 des Verfassungsgerichtshofgesetzes). Für die Vergütung seiner Reisekosten gelten die Bestimmungen der Reisegebührenvorschrift für Bundesbedienstete sinngemäß mit der Maßgabe, dass sein Wohnsitz als Dienort gilt und dass ihm die Reisezulage in der Gebührenstufe 3 gebührt. Für die Bemessung der dem Rechtsschutzbeauftragten zustehenden Gebühren ist der Bundesminister für Justiz zuständig.

§ 149o. (1) Dem Rechtsschutzbeauftragten obliegt die Prüfung und Kontrolle der Anordnung und Durchführung einer optischen oder akustischen Überwachung nach § 149d Abs. 1 Z 3 und eines automationsunterstützten Datenabgleichs nach § 149i. Zu diesem Zweck haben ihm Gerichte, Staatsanwaltschaften und Sicherheitsbehörden jederzeit Akteneinsicht zu gewähren und sind ihm auf sein Verlangen Abschriften (Ablichtungen) einzelner Aktenstücke unentgeltlich auszufolgen und alle Auskünfte zu erteilen. Es ist ihm Gelegenheit zu geben, die Durchführung der erwähnten besonderen

Ermittlungsmaßnahmen zu überwachen, und es ist ihm jederzeit Zutritt zu allen Räumen zu gewähren, in denen Aufnahmen oder sonstige Überwachungsergebnisse aufbewahrt werden oder der Datenabgleich durchgeführt wird.

(2) Beantragt der Staatsanwalt die Anordnung einer Überwachung nach § 149d Abs. 1 Z 3 oder die Anordnung eines Datenabgleichs nach § 149i, so hat er dem Rechtsschutzbeauftragten zugleich eine Ausfertigung dieses Antrags samt einer Abschrift der Anzeige und der maßgebenden Erhebungsergebnisse zu übermitteln sowie im Fall des § 149e Abs. 2 zweiter Satz um Ermächtigung zur Antragstellung zu ersuchen. Eine Ermächtigung zu einem Antrag auf Überwachung nach § 149d Abs. 1 Z 3 in den ausschließlich der Berufsausübung gewidmeten Räumlichkeiten einer der in § 152 Abs. 1 Z 4 und 5 oder in § 31 Abs. 1 des Mediengesetzes erwähnten Personen darf der Rechtsschutzbeauftragte nur erteilen, wenn besonders schwerwiegende Gründe vorliegen, die diesen Eingriff verhältnismäßig erscheinen lassen.

(3) Einen Beschluss, mit dem die Ratskammer eine Überwachung nach § 149d Abs. 1 Z 3 anordnet oder genehmigt oder einen Datenabgleich nach § 149i anordnet, hat der Untersuchungsrichter samt Abschriften (Ablichtungen) aller Aktenstücke, die für die Beurteilung der Anordnungsgründe von Bedeutung sein können, unverzüglich dem Rechtsschutzbeauftragten zu übermitteln. Dieser hat zu beurteilen, ob wegen Fehlens einer Voraussetzung der Anordnung, wie, Tatverdacht, Anordnungsgrund oder Verhältnismäßigkeit, Beschwerde an den Gerichtshof zweiter Instanz zu erheben ist (§ 114). Dieses Beschwerderecht erlischt mit dem Ablauf der Rechtsmittelfrist des Beschuldigten.

(4) Nach Beendigung der Überwachung ist dem Rechtsschutzbeauftragten der Bericht nach § 149f Abs. 2 zu übermitteln und ihm Gelegenheit zu geben, die gesamte Aufnahme anzusehen und anzuhören sowie die hergestellten Bilder und schriftlichen Aufzeichnungen einzusehen, bevor diese zum Akt genommen werden (§ 149m Abs. 2). Er ist ferner berechtigt, die Vernichtung von Bildern und Teilen der schriftlichen Aufzeichnungen (§ 149g Abs. 6) zu beantragen und sich von der ordnungsgemäßen Vernichtung von Aufnahmen und Aufzeichnungen zu überzeugen. Das gleiche gilt für die ordnungsgemäße Löschung von Daten, die in einen Datenabgleich einbezogen oder durch ihn gewonnen wurden. Beabsichtigt der Untersuchungsrichter, einem solchen Antrag des Rechtsschutzbeauftragten nicht nachzukommen, so hat er unverzüglich die Entscheidung der Ratskammer einzuholen.

(5) Bis zum 31. März eines jeden Jahres hat der Rechtsschutzbeauftragte dem Bundesminister für Justiz einen Bericht über seine Tätigkeit und seine Wahrnehmungen zur Anwendung der Bestimmungen über die optische und akustische Überwachung nach § 149d Abs. 1 Z 3 sowie über den automationsunterstützten Datenabgleich im vorangegangenen Jahr zu übermitteln.

X. Schadenersatz

§ 149p. Der Bund haftet für vermögensrechtliche Nachteile, die durch den Einsatz technischer Mittel zur Bild- oder Tonübertragung und zur Bild- oder Tonaufnahme, insbesondere durch das Eindringen in eine Wohnung oder sonstige zum Hauswesen gehörige Räumlichkeiten oder die sonstigen Vorkehrungen für die Durchführung einer Überwachung nach § 149d Abs. 1 oder 2, oder durch einen automationsunterstützten Datenabgleich entstanden sind. Der Ersatzanspruch ist ausgeschlossen, wenn der Geschädigte die Anordnung des Einsatzes technischer Mittel oder des automationsunterstützten Datenabgleichs vorsätzlich herbeigeführt hat. Weitergehende Ansprüche bleiben unberührt. Auf das Verfahren ist das Amtshaftungsgesetz, BGBl. Nr. 20/1949, anzuwenden."

3.7. Vereinbarung zur Sicherstellung der Patientenrechte (Patientencharta), BGBl. I Nr. 195/1999

Der Nationalrat hat beschlossen:

Der Abschluss der nachstehenden Vereinbarung gemäß Art. 15a B-VG wird verfassungsmäßig genehmigt.

Vereinbarung zur Sicherstellung der Patientenrechte (Patientencharta)

Der Bund, vertreten durch die Bundesregierung, und das Land Kärnten, vertreten durch den Landeshauptmann, - im folgenden Vertragsparteien genannt - kommen überein, gemäß Art. 15a B-VG die nachstehende Vereinbarung zu schließen:

Zielsetzung und Definition

Artikel 1

(1) Die Vertragsparteien verpflichten sich, im Rahmen ihrer Zuständigkeit in Gesetzgebung und Vollziehung dafür zu sorgen, dass die folgenden Patientenrechte sichergestellt sind.

(2) Träger von Patientenrechten im Sinne dieser Vereinbarung ist jede Person, die Leistungen auf dem Gebiet des Gesundheitswesens in Anspruch nimmt oder ihrer auf Grund ihres Gesundheitszustandes bedarf.

(3) Leistungen auf dem Gebiet des Gesundheitswesens werden durch freiberuflich tätige Angehörige der Gesundheitsberufe und Einrichtungen erbracht, die der Erhaltung und dem Schutz der Gesundheit, der Feststellung des Gesundheitszustandes, der Behandlung von Krankheiten, der Vornahme operativer Eingriffe, der Geburtshilfe sowie der Pflege und Betreuung von Kranken und Genesenden dienen.

Abschnitt 1

Grundsätzliches

Artikel 2

Die Persönlichkeitsrechte der Patienten und Patientinnen sind besonders zu schützen. Ihre Menschenwürde ist unter allen Umständen zu achten und zu wahren.

Artikel 3

Patienten und Patientinnen dürfen auf Grund des Verdachtes oder des Vorliegens einer Krankheit nicht diskriminiert werden.

Abschnitt 2

Recht auf Behandlung und Pflege

Artikel 4

(1) Die Vertragsparteien verpflichten sich, die zweckmäßigen und angemessenen Leistungen auf dem Gebiet des Gesundheitswesens für alle Patienten und Patientinnen ohne Unterschied des Alters, des Geschlechts, der Herkunft, des Vermögens, des Religionsbekenntnisses, der Art und Ursache der Erkrankung oder ähnliches rechtzeitig sicherzustellen.

(2) Durch die zuständige Gesetzgebung kann unter Beachtung der Verpflichtungen der Republik Österreich angeordnet werden, dass die Behandlung nichtösterreichischer Staatsangehöriger nur dann zu erfolgen hat, wenn die Kosten der Behandlung von den Patienten und Patientinnen oder einem Dritten getragen werden; dies gilt nicht in den Fällen drohender Lebensgefahr, unmittelbar bevorstehender Entbindung oder schwerer gesundheitlicher Schädigung, die eine sofortige Behandlung gebieten.

Artikel 5

(1) Die Leistungen auf dem Gebiet des Gesundheitswesens (Art. 4 Abs. 1) sind durch Krankenanstalten, ambulante Einrichtungen, Dienste der extramuralen medizinischen Betreuung einschließlich der Hauskrankenpflege sowie durch freiberuflich tätige Angehörige der Gesundheitsberufe und Apotheken sicherzustellen. Dies gilt insbesondere auch für die Betreuung psychisch Kranker.

(2) Die Leistungen auf dem Gebiet des Gesundheitswesens sind auch auf den Gebieten der Gesundheitsförderung, der Vorsorge- und Arbeitsmedizin sowie der Rehabilitation und des Kurwesens sicherzustellen.

(3) Die Kontinuität der Behandlung und Pflege ist durch organisatorische Maßnahmen zu wahren.

Artikel 6

(1) Die medizinisch gebotene, nach den Umständen des Einzelfalles jeweils mögliche notärztliche Versorgung, Rettung und Transport sind sicherzustellen.

(2) Weiters ist die notwendige Versorgung mit Arzneimitteln und Medizinprodukten sicherzustellen.

Artikel 7

- (1) Diagnostik, Behandlung und Pflege haben entsprechend dem jeweiligen Stand der Wissenschaften bzw. nach anerkannten Methoden zu erfolgen. Dabei ist auch der Gesichtspunkt der bestmöglichen Schmerztherapie besonders zu beachten.
- (2) Kann nach dem Anstaltszweck und dem Leistungsangebot einer Krankenanstalt eine dem jeweiligen Stand der medizinischen Wissenschaft entsprechende Versorgung eines Patienten oder einer Patientin nicht gewährleistet werden, ist sicherzustellen, dass der Patient oder die Patientin mit seiner bzw. ihrer Zustimmung in eine geeignete andere Krankenanstalt überstellt wird.
- (3) In Krankenanstalten hat die ärztliche Betreuung grundsätzlich auf fachärztlichem Niveau zu erfolgen.

Artikel 8

Die Vertragsparteien kommen überein, dass Leistungen im Bereich des Gesundheitswesens einer Qualitätskontrolle unterzogen und dem Stand der Wissenschaft entsprechend Qualitätssicherungsmaßnahmen gesetzt werden.

Abschnitt 3

Recht auf Achtung der Würde und Integrität

Artikel 9

- (1) Die Privatsphäre der Patienten und Patientinnen ist zu wahren.
- (2) Bei der Aufnahme oder Behandlung mehrerer Patienten oder Patientinnen in einem Raum ist durch angemessene bauliche oder organisatorische Maßnahmen sicherzustellen, dass die Intim- und die Privatsphäre gewahrt werden.
- (3) Insbesondere bei stationärer Aufnahme von Langzeitpatienten und -patientinnen ist dafür zu sorgen, dass eine vertraute Umgebung geschaffen werden kann.

Artikel 10

Die Organisations-, Behandlungs- und Pflegeabläufe in Kranken- und Kuranstalten sind soweit wie möglich dem allgemein üblichen Lebensrhythmus anzupassen.

Artikel 11

Die Vertragsparteien verpflichten sich, dass klinische Prüfungen von Arzneimitteln, von Medizinprodukten sowie die Anwendung neuer medizinischer Methoden erst nach eingehender ethischer Beurteilung vorgenommen werden dürfen.

Artikel 12

Die religiöse Betreuung stationär aufgenommener Patienten und Patientinnen ist auf deren Wunsch zu ermöglichen.

Artikel 13

(1) Gesundheitsbezogene Daten sowie sonstige Umstände, die aus Anlass der Erbringung von Leistungen im Bereich des Gesundheitswesens bekannt werden und an denen Patienten und Patientinnen ein Geheimhaltungsinteresse haben, unterliegen dem Datenschutzgesetz.

(2) Ausnahmen sind nur in den im Datenschutzgesetz vorgesehenen Fällen zulässig.

(3) Auskunfts- und Richtigstellungsrechte sind auch für Daten vorzusehen, die nicht automationsunterstützt verarbeitet werden.

Artikel 14

(1) Es ist sicherzustellen, dass im Rahmen stationärer Versorgung Besuche empfangen werden können und sonstige Kontakte gepflogen werden können. Weiters ist der Wunsch eines Patienten oder einer Patientin zu respektieren, keinen Besuch oder bestimmte Personen nicht empfangen zu wollen.

(2) Es ist dafür zu sorgen, dass die Patienten und Patientinnen Vertrauenspersonen nennen können, die insbesondere im Fall einer nachhaltigen Verschlechterung des Gesundheitszustandes zu verständigen sind und denen in solchen Fällen auch außerhalb der Besuchszeit ein Kontakt mit den Patienten und Patientinnen zu ermöglichen ist.

Artikel 15

(1) In stationären Einrichtungen ist ein Sterben in Würde zu ermöglichen. Auch dabei ist dem Gebot der bestmöglichen Schmerztherapie Rechnung zu tragen.

(2) Vertrauenspersonen der Patienten und Patientinnen ist Gelegenheit zum Kontakt mit Sterbenden zu geben. Andererseits sind Personen vom Kontakt auszuschließen, wenn der Sterbende dies wünscht.

Abschnitt 4

Recht auf Selbstbestimmung und Information

Artikel 16

(1) Patienten und Patientinnen haben das Recht, im vorhinein über mögliche Diagnose- und Behandlungsarten sowie deren Risiken und Folgen aufgeklärt zu werden. Sie haben das Recht auf Aufklärung über ihren Gesundheitszustand, weiters sind sie über ihre erforderliche Mitwirkung bei der Behandlung sowie eine therapieunterstützende Lebensführung aufzuklären.

(2) Die Art der Aufklärung hat der Persönlichkeitsstruktur und dem Bildungsstand der Patienten und Patientinnen angepasst und den Umständen des Falles entsprechend zu erfolgen.

(3) Ist eine Behandlung dringend geboten und würde nach den besonderen Umständen des Einzelfalles durch eine umfassende Aufklärung das Wohl des Patienten oder der Patientin gefährdet werden, so hat sich der Umfang der Aufklärung am Wohl des Patienten oder der Patientin zu orientieren.

(4) Auf die Aufklärung kann von den Patienten und Patientinnen verzichtet werden; sie dürfen zu einem Verzicht nicht beeinflusst werden.

(5) Patienten und Patientinnen sind im vorhinein über die sie voraussichtlich treffenden Kosten zu informieren.

Artikel 17

(1) Patienten und Patientinnen dürfen nur mit ihrer Zustimmung behandelt werden.

(2) Ohne Zustimmung darf eine Behandlung nur vorgenommen werden, wenn eine Willensbildungsfähigkeit der Patienten oder Patientinnen nicht gegeben ist und durch den Aufschub der Behandlung das Leben oder die Gesundheit der Patienten oder der Patientinnen ernstlich gefährdet würde.

(3) Für Patienten und Patientinnen, die den Grund und die Bedeutung einer Behandlung nicht einsehen oder ihren Willen nach dieser Einsicht bestimmen können, ist sicherzustellen, dass eine Behandlung nur mit Zustimmung eines nach Maßgabe der Gesetze zu bestimmenden Vertreters und erforderlichenfalls mit Genehmigung des Gerichtes durchgeführt wird.

(4) Ohne Zustimmung des Vertreters und allenfalls erforderlicher Genehmigung des Gerichtes darf eine Behandlung nur bei Gefahr in Verzug vorgenommen werden, wenn der mit der Einholung der Zustimmung oder der Genehmigung verbundene Zeitaufwand für den Patienten oder die Patientin eine Lebensgefahr oder die Gefahr einer schweren gesundheitlichen Schädigung bedeuten würde.

(5) Maßnahmen, die mit einer Beschränkung der persönlichen Freiheit oder sonstigen Eingriffen in die Persönlichkeitsrechte der Patienten und Patientinnen verbunden sind

und ohne deren gültige Zustimmung vorgenommen werden, sind - sofern nicht der mit der Einholung der Zustimmung verbundene Aufschub mit Lebensgefahr oder mit der Gefahr einer schweren gesundheitlichen Schädigung für den Patienten oder die Patientin verbunden wäre - nur nach entsprechender Befassung des gesetzlichen Vertreters, erforderlichenfalls des Gerichtes, zulässig.

Artikel 18

Patienten und Patientinnen haben das Recht, im vorhinein Willensäußerungen abzugeben, durch die sie für den Fall des Verlustes ihrer Handlungsfähigkeit das Unterbleiben einer Behandlung oder bestimmter Behandlungsmethoden wünschen, damit bei künftigen medizinischen Entscheidungen soweit wie möglich darauf Bedacht genommen werden kann.

Artikel 19

(1) Das Recht der Patienten und Patientinnen auf Einsichtnahme in die über sie geführte Dokumentation der diagnostischen, therapeutischen und pflegerischen Maßnahmen einschließlich allfälliger Beilagen, wie Röntgenbilder, ist sicherzustellen.

(2) Einschränkungen sind nur insoweit zulässig, als sie auf Grund der besonderen Umstände des Einzelfalles zum Wohl des Patienten oder der Patientin unvermeidlich sind. Einem Vertreter des Patienten oder der Patientin kommt auch in einem solchen Fall ein uneingeschränktes Einsichtsrecht zu, sofern der Patient oder die Patientin dies nicht ausgeschlossen hat.

Artikel 20

(1) Niemand darf ohne seine ausdrückliche Zustimmung zu klinischen Prüfungen und zu Forschungs- und Unterrichtszwecken herangezogen werden. Die Zustimmung kann jederzeit widerrufen werden.

(2) Die Verwendung personenbezogener Daten für medizinische Forschungszwecke bedarf der ausdrücklichen Zustimmung des Betroffenen. Dabei ist besonders zu achten, dass die aus dem Grundrecht auf Datenschutz erfließenden Rechte des Betroffenen gewahrt werden.

Abschnitt 5

Recht auf Dokumentation

Artikel 21

(1) Die notwendige Dokumentation der diagnostischen, therapeutischen und pflegerischen Maßnahmen ist sicherzustellen. Weiters ist die Aufklärung der Patienten und Patientinnen und ihre Zustimmung zur Behandlung oder die Ablehnung einer Behandlung zu dokumentieren.

(2) Es ist sicherzustellen, dass in der Dokumentation auch Willensäußerungen der Patienten und Patientinnen festgehalten werden.

(3) Willensäußerungen nach Abs. 2 können insbesondere Widersprüche gegen die Entnahme von Organen gemäß § 62a KAG oder Willensäußerungen gemäß Artikel 18 sein.

Artikel 22

Patienten und Patientinnen haben das Recht, auf ihren Wunsch gegen angemessenen Kostenersatz Abschriften aus der Dokumentation zur Verfügung gestellt zu bekommen. Artikel 19 Abs. 2 gilt sinngemäß.

Abschnitt 6

Besondere Bestimmungen für Kinder

Artikel 23

Die Aufklärung von Minderjährigen hat ihrem jeweiligen Entwicklungsstand entsprechend zu erfolgen.

Artikel 24

Eine Behandlung, die wegen Lebensgefahr oder Gefahr einer schweren gesundheitlichen Schädigung geboten ist, ist bei Gefahr im Verzug auch gegen den erklärten Willen des Erziehungsberechtigten durchzuführen, ansonsten ist die Genehmigung des Gerichtes einzuholen.

Artikel 25

(1) Unter Berücksichtigung der jeweiligen Gegebenheiten ist unmündigen Minderjährigen eine Begleitung durch eine Bezugsperson zu ermöglichen.

(2) Bei der stationären Aufnahme von unmündigen Minderjährigen bis zur Vollendung des 10. Lebensjahres ist auf Wunsch die Mitaufnahme einer Begleitperson zu ermöglichen. Sofern dies aus räumlichen Gründen nicht möglich ist, ist Bezugspersonen ein umfassendes Besuchsrecht einzuräumen, das lediglich aus zwingenden medizinischen oder organisatorischen Gründen eingeschränkt werden darf.

(3) Bezugspersonen sollen auf ihren Wunsch soweit wie möglich an der Betreuung beteiligt werden.

Artikel 26

Einrichtungen, Abteilungen und Bereiche, die überwiegend der Behandlung von Minderjährigen dienen, sind altersgerecht auszustatten.

Artikel 27

(1) Soweit dies organisatorisch möglich ist, hat eine stationäre Aufnahme von unmündigen Minderjährigen getrennt von erwachsenen Patienten zu erfolgen.

(2) Angehörige der Gesundheitsberufe, denen die Behandlung und Pflege von Minderjährigen obliegt, sollen durch ihre Ausbildung befähigt werden, auf die alters- und entwicklungsbedingten Bedürfnisse von Minderjährigen eingehen zu können.

Artikel 28

Die Träger von Krankenanstalten haben organisatorisch dafür vorzusorgen, dass schulpflichtigen Kindern bei einem längeren stationären Aufenthalt nach Maßgabe schulrechtlicher Bestimmungen Unterricht erteilt werden kann.

Abschnitt 7

Vertretung von Patienteninteressen

Artikel 29

(1) Zur Vertretung von Patienteninteressen sind unabhängige Patientenvertretungen einzurichten und mit den notwendigen Personal- und Sacherfordernissen auszustatten. Die unabhängigen Patientenvertretungen sind bei ihrer Tätigkeit weisungsfrei zu stellen und zur Verschwiegenheit zu verpflichten. Es ist ihnen die Behandlung von Beschwerden von Patienten und Patientinnen und Angehörigen, die Aufklärung von Mängeln und Missständen und die Erteilung von Auskünften zu übertragen. Patientenvertretungen können Empfehlungen abgeben.

(2) Die unabhängigen Patientenvertretungen haben mit Patientenselbsthilfegruppen, die Patienteninteressen wahrnehmen, die Zusammenarbeit zu suchen.

(3) Patienten und Patientinnen haben das Recht auf Prüfung ihrer Beschwerden und auf Vertretung ihrer Interessen durch die unabhängigen Patientenvertretungen. Sie sind vom Ergebnis der Überprüfung zu informieren. Die Inanspruchnahme der Patientenvertretungen ist für die Patienten und Patientinnen mit keinen Kosten verbunden.

Artikel 30

(1) Es ist sicherzustellen, dass unabhängigen Patientenvertretungen Gelegenheit geboten wird, vor Entscheidungen in grundlegenden allgemeinen patientenrelevanten Fragen ihre Stellungnahme abzugeben. Dies gilt insbesondere vor der Errichtung neuer stationärer und ambulanter Versorgungsstrukturen, für die öffentliche Mittel eingesetzt werden, für die Durchführung von Begutachtungsverfahren zu Gesetzes- und Verordnungsentwürfen sowie für grundlegende Planungsvorhaben.

(2) Dachorganisationen von Patientenselbsthilfegruppen ist Gelegenheit zu geben, in Begutachtungsverfahren zu patientenrelevanten Gesetzes- und Verordnungsentwürfen gehört zu werden.

Artikel 31

(1) Die Vertragsparteien haben sicherzustellen, dass Informationen über Leistungen im Bereich des Gesundheitswesens für jedermann zur Verfügung stehen.

(2) Es ist sicherzustellen, dass freiberuflich tätige Angehörige der Gesundheitsberufe und Träger von Einrichtungen im Bereich des Gesundheitswesens über ihre Leistungen in sachlicher Weise informieren.

Abschnitt 8

Durchsetzung von Schadenersatzansprüchen

Artikel 32

Im Zusammenhang mit der Haftung für Leistungen auf dem Gebiet des Gesundheitswesens dürfen Abweichungen vom Schadenersatzrecht und von allgemeinen Beweislast- und Gewährleistungsregeln im Sinne der Bestimmungen des ABGB nur zugunsten der Patienten und Patientinnen getroffen werden.

Artikel 33

Vergleichsgespräche vor ärztlichen Schlichtungsstellen und vergleichbaren Einrichtungen hemmen den Ablauf der Verjährung bis zum Verstreichen einer angemessenen Klagefrist nach Abbruch des Verfahrens oder nach einer sonstigen, zuungunsten des Patienten oder der Patientin erfolgenden Beendigung des Schlichtungsverfahrens.

Abschnitt 9

Schlussbestimmungen

Artikel 34

Inkrafttreten

(1) Diese Vereinbarung tritt mit dem Monatsersten nach Einlangen der Mitteilungen der Vertragsparteien beim Bundesministerium für Arbeit, Gesundheit und Soziales,

dass die nach der Bundesverfassung bzw. nach der Verfassung des Landes Kärnten erforderlichen Voraussetzungen für das Inkrafttreten erfüllt sind, in Kraft.

(2) Das Bundesministerium für Arbeit, Gesundheit und Soziales hat die Vertragsparteien in Kenntnis zu setzen, wenn die Mitteilungen nach Abs. 1 eingelangt sind.

Artikel 35

Durchführung

Die Vertragsparteien verpflichten sich, die in ihre jeweiligen Kompetenzbereiche fallenden gesetzlichen Regelungen, die zur Durchführung dieser Vereinbarung erforderlich sind, zu erlassen.

Artikel 36

Abänderung

Eine Abänderung dieser Vereinbarung ist nur schriftlich im Einvernehmen der Vertragsparteien möglich.

Artikel 37

Hinterlegung

Diese Vereinbarung wird in einer Urschrift ausgefertigt. Die Urschrift wird beim Bundesministerium für Arbeit, Gesundheit und Soziales hinterlegt. Dieses hat dem Land Kärnten eine beglaubigte Abschrift der Vereinbarung zu übermitteln.

Für den Bund:

Die Bundesministerin für Arbeit, Gesundheit und Soziales Hostasch

Für das Land Kärnten: Der Landeshauptmann von Kärnten Haider

Diese Vereinbarung tritt gemäß § 34 Abs. 1 mit 1. September 1999 in Kraft.

Klima

3.8. Bundesgesetz: Dokumentation im Gesundheitswesen (BGBl. Nr. 745/1996) **Hauptstück A**

Diagnosen- und Leistungsdokumentation im stationären Bereich

§ 1. (1) Die Träger von Krankenanstalten haben nach der von der Weltgesundheitsorganisation veröffentlichten Internationalen Klassifikation der Krankheiten (ICD), in einer vom Bundesminister für Gesundheit und Konsumentenschutz unter Anpassung an den jeweiligen Stand der medizinischen Wissenschaft herauszugebenden Fassung, die Diagnosen der in stationärer Behandlung befindlichen Pfléglinge originär zu erfassen.

(2) Die Träger von Krankenanstalten sind weiters zur Erfassung von ausgewählten medizinischen Einzelleistungen auf der Grundlage eines vom Bundesminister für Gesundheit und Konsumentenschutz unter Anpassung an den jeweiligen Stand der medizinischen Wissenschaft herauszugebenden Leistungskataloges verpflichtet. Umfang und Inhalt der Leistungserfassung haben den Erfordernissen der leistungsorientierten Krankenanstaltenfinanzierung Rechnung zu tragen.

§ 2. (1) Die Träger von Krankenanstalten haben auf der Grundlage der im § 1 Abs. 1 und 2 genannten Klassifikationen bis zum 31. März jeden Jahres für das vorangegangene Kalenderjahr dem Bundesministerium für Gesundheit und Konsumentenschutz einen Bericht vorzulegen.

(2) Die Träger von Krankenanstalten, die auf der Grundlage der Vereinbarung gemäß Art. 15a B-VG über die Reform des Gesundheitswesens und der Krankenanstaltenfinanzierung für die Jahre 1997 bis 2000 finanziert werden, haben keinen Bericht gemäß Abs. 1 vorzulegen. Diese Krankenanstalten haben zu den in den landesgesetzlichen Bestimmungen über die Finanzierung durch den Landesfonds festgelegten Terminen Berichte dem Land oder dem Landesfonds vorzulegen.

(3) Die Berichte gemäß Abs. 1 und 2 und gemäß § 3 haben in maschinenlesbarer Form zu erfolgen und die Diagnosen der im Berichtszeitraum aus stationärer Behandlung entlassenen, verstorbenen oder in andere Krankenanstalten überstellten Pfléglinge sowie die während des stationären Aufenthaltes erbrachten ausgewählten medizinischen Einzelleistungen zu beinhalten.

(4) Der Bericht pro stationärem Krankenhausaufenthalt hat zu enthalten:

1. Administrative Daten:

- a) Krankenanstaltennummer,
- b) Aufnahmezahl,
- c) entlassende Abteilung,
- d) Geburtsdatum,
- e) Geschlecht,
- f) Staatsbürgerschaft,

- g) Postleitzahl des Hauptwohnsitzes,
- h) Kostenträger,
- i) Aufnahmedatum,
- j) Art der Aufnahme,
- k) Entlassungsdatum und
- l) Art der Entlassung.

2. Medizinische Daten:

- a) Hauptdiagnose,
- b) zusätzliche Diagnosen,
- c) ausgewählte medizinische Einzelleistungen und
- d) Verlegungen innerhalb der Krankenanstalt.

§ 3. (1) Die Länder (Landesfonds) haben - beginnend mit dem Berichtsjahr 1997 - Diagnosen- und Leistungsberichte gemäß § 2 Abs. 3 und 4 der über den Landesfonds abgerechneten Krankenanstalten an das Bundesministerium für Gesundheit und Konsumentenschutz für folgende Berichtszeiträume spätestens zu folgenden Terminen zu übermitteln:

1. einen Bericht über das 1. Quartal bis 31. Mai des laufenden Jahres,
2. einen Bericht über das 1. Halbjahr bis 30. September des laufenden Jahres und
3. einen Jahresbericht bis 31. März des Folgejahres.

(2) Diese Berichte haben je stationärem Aufenthalt weiters die Ergebnisse der Bepunktung im LKF-Kernbereich auf Grundlage des österreichweit einheitlichen Systems der leistungsorientierten Diagnosenfallgruppen zu beinhalten.

§ 4. Der Bundesminister für Gesundheit und Konsumentenschutz hat durch Verordnung nähere Bestimmungen über die Art der von den Trägern der Krankenanstalten sowie von den Ländern (Landesfonds) vorzunehmenden Datenübermittlung sowie über die Gliederung der Merkmale der im § 2 Abs. 4 genannten Daten und den konkreten Datensatzaufbau einschließlich Formatierung zu erlassen.

§ 5. Der Bundesminister für Gesundheit und Konsumentenschutz hat die vorgelegten Jahresberichte dem Österreichischen Statistischen Zentralamt in maschinenlesbarer Form zwecks Erstellung einer länderbezogenen Statistik über die Krankbewegung und deren Veröffentlichung im Gesundheitsstatistischen Jahrbuch zu übermitteln. Die Statistik hat die Krankheitsarten, gegliedert nach Altersgruppen, Geschlecht und Entlassungsart, sowie ausgewählte medizinische Einzelleistungen zu enthalten. Zur Sicherstellung der Anonymität sind Einzelfallkategorien durch entsprechend erweiterte Gliederungsbreiten auszuschließen.

Hauptstück B

Diagnosen- und Leistungsdokumentation im spitalsambulanten Bereich

§ 6. (1) Zur Erarbeitung eines für alle Krankenanstalten Österreichs praktikablen Diagnosen- und Leistungsdokumentationssystems im spitalsambulanten Bereich und zur Erhebung von Datengrundlagen für die Entwicklung eines leistungsorientierten Finanzierungssystems in diesem Bereich ist in einigen ausgewählten Referenzkrankenanstalten eine Datenerhebung im Rahmen eines Pilotprojekts vorzusehen.

(2) Zu diesem Zweck sind gemeinsam mit den Referenzkrankenanstalten für die Dokumentation im spitalsambulanten Bereich geeignete Diagnosen- und Leistungskataloge zu erarbeiten und festzulegen. Des weiteren ist in diesem Pilotprojekt der für die Spitalsambulanzplanerstellung und leistungsorientierte Abrechnung erforderliche Umfang von Diagnosen- und Leistungsberichten im spitalsambulanten Bereich auszuarbeiten und genau zu definieren. Des weiteren ist im Rahmen dieses Pilotprojekts die Periodizität dieser Diagnosen- und Leistungsberichte festzulegen.

(3) Zur Weiterentwicklung des Dokumentationssystems und zur Erarbeitung eines leistungsorientierten Abrechnungssystems haben die ausgewählten Referenzkrankenanstalten anonymisierte Diagnosen- und Leistungsberichte für den spitalsambulanten Bereich an das Bundesministerium für Gesundheit und Konsumentenschutz zu übermitteln.

Hauptstück C

Dokumentation von Statistik- und Kostendaten in Krankenanstalten

§ 7. (1) Die Träger von Krankenanstalten, die auf Grundlage der Vereinbarung gemäß Art. 15a B-VG über die Reform des Gesundheitswesens und der Krankenanstaltenfinanzierung für die Jahre 1997 bis 2000 finanziert werden, haben Statistikdaten über ihre Krankenanstalten und deren Kostenstellen, die das beschäftigte Personal (gegliedert nach Gruppen), die medizinisch-technische Ausstattung, die Gebarung und weitere Leistungsdaten betreffen, sowie die Sammel-Kostennachweise der Krankenanstalten und Kostennachweise der Kostenstellen - gegliedert nach Kostenartengruppen und Kostenarten - jährlich zu erfassen. Dem Landeshauptmann sind für das vorangegangene Kalenderjahr die Statistikdaten sowie der Kostenstellenplan bis 31. März jeden Jahres und die Kostendaten bis 30. April jeden Jahres in maschinenlesbarer Form zu melden. Bis zu den gleichen Terminen eines jeden Jahres sind von den Trägern der Krankenanstalten diese Daten dem Bundesministerium für Gesundheit und Konsumentenschutz als vorläufige Datenmeldungen in maschinenlesbarer Form vorzulegen.

(2) 1. Die Statistikdaten über die Krankenanstalten und deren Kostenstellen gemäß Abs. 1 und der Kostenstellenplan sind vom Landeshauptmann zu prüfen, allenfalls richtigzustellen und von diesem dem Bundesministerium für Gesundheit und Konsumentenschutz bis 30. April jeden Jahres für das vorangegangene Kalenderjahr in maschinenlesbarer Form vorzulegen.

2. Die Sammel-Kostennachweise der Krankenanstalten, gegliedert nach Kostenartengruppen und Kostenarten, sowie über Verlangen des Bundesministeriums für Gesundheit und Konsumentenschutz die Kostennachweise der Kostenstellen, gegliedert nach Kostenartengruppen und Kostenarten, und die Kostenstellenbeschreibungen sind vom Landeshauptmann zu prüfen, allenfalls richtigzustellen und von diesem dem Bundesministerium für Gesundheit und Konsumentenschutz bis 31. Mai jeden Jahres für das vorangegangene Kalenderjahr in maschinenlesbarer Form vorzulegen.

(3) Als Grundlage für die Erfassung und Meldung der Statistik- und Kostendaten haben die Träger der in Abs. 1 genannten Krankenanstalten ein bundeseinheitliches Statistik- und Kostenrechnungssystem anzuwenden. Der Bundesminister für Gesundheit und Konsumentenschutz hat durch Verordnung nähere Bestimmungen über dieses System zu erlassen. Weiters hat der Bundesminister für Gesundheit und Konsumentenschutz unter Bedachtnahme auf Realisierbarkeit, Zweckmäßigkeit und Wirtschaftlichkeit durch Verordnung nähere Bestimmungen über die zu meldenden Statistik- und Kostendaten sowie über die Art der von den Trägern der Krankenanstalten vorzunehmenden Datenübermittlung und den konkreten Datensatzaufbau einschließlich Formatierung zu erlassen.

§ 8. (1) Die Träger von Krankenanstalten, die nicht unter die Bestimmungen des § 7 fallen, haben Statistikdaten über ihre Krankenanstalten, die das beschäftigte Personal (gegliedert nach Gruppen), die medizinisch-technische Ausstattung und weitere Leistungsdaten betreffen, jährlich zu erfassen und dem Bundesministerium für Gesundheit und Konsumentenschutz bis 28. Februar jeden Jahres für das vorangegangene Kalenderjahr (Anm.: richtig: Kalenderjahr) einen entsprechenden Bericht in maschinenlesbarer Form vorzulegen.

(2) Der Bundesminister für Gesundheit und Konsumentenschutz hat durch Verordnung nähere Bestimmungen über die zu erfassenden und zu meldenden Statistikdaten sowie über die Art der von den Trägern der Krankenanstalten vorzunehmenden Datenübermittlung und den konkreten Datensatzaufbau einschließlich Formatierung zu erlassen.

Hauptstück D

Erfassung weiterer Daten

§ 9. (1) Zur Beobachtung, Analyse und Weiterentwicklung des Gesundheitssystems und zur Weiterentwicklung der leistungsorientierten Vergütungssysteme unter Einbeziehung der Gesundheitsbereiche außerhalb der Krankenanstalten können unter

Bedachtnahme auf Realisierbarkeit, Zweckmäßigkeit und Wirtschaftlichkeit weitere erforderliche Daten im extramuralen Bereich erfasst und angefordert werden.

(2) Diese Daten sind primär von jenen Institutionen (Sozialversicherungs-, Bundes- und Landesstellen), die bereits über die für diese Aufgabenstellung erforderlichen Daten verfügen, in anonymisierter Form bereitzustellen.

(3) Der Bundesminister für Gesundheit und Konsumentenschutz kann durch Verordnung nähere Bestimmungen über die zu erfassenden Daten, die zur Datenerfassung und -übermittlung Verpflichteten, die Form und die Termine für die Datenübermittlung erlassen sowie festlegen, an wen die Datenübermittlung zu erfolgen hat.

Hauptstück E

Strafbestimmung

§ 10. Die Träger der Krankenanstalten, die den gemäß § 8 auferlegten Verpflichtungen nicht nachkommen, begehen, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, eine Verwaltungsübertretung und sind mit einer Geldstrafe bis zu 30 000 S zu bestrafen.

Hauptstück F

Inkrafttretens- und Schlussbestimmungen

§ 11. (1) Die auf Grund dieses Gesetzes zu erlassenden Verordnungen können sofort nach der Kundmachung dieses Gesetzes erlassen werden. Sie dürfen frühestens mit dem Inkrafttreten dieses Gesetzes in Kraft gesetzt werden.

(2) Bis zur Erlassung einer Verordnung gemäß § 7 Abs. 3 gilt die Krankenanstaltenkostenrechnungsverordnung (KRV), BGBl. Nr. 328/1977, als Bundesgesetz weiter.

§ 12. Dieses Bundesgesetz tritt mit 1. Jänner 1997 in Kraft.

§ 13. Mit der Vollziehung dieses Bundesgesetzes ist der Bundesminister für Gesundheit und Konsumentenschutz betraut.

3.9. Bundesgesetz, mit dem ein Bundesgesetz über die Ausübung des ärztlichen Berufes und die Standesvertretung der Ärzte (Ärztegesetz 1998 - ÄrzteG 1998) erlassen und das Ausbildungsvorbehaltsgesetz geändert wird; BGBl. I Nr. 169/1998

Dokumentationspflicht und Auskunftserteilung

§ 51. (1) Der Arzt ist verpflichtet, Aufzeichnungen über jede zur Beratung oder Behandlung übernommene Person, insbesondere über den Zustand der Person bei Übernahme der Beratung oder Behandlung, die Vorgeschichte einer Erkrankung, die Diagnose, den Krankheitsverlauf sowie über Art und Umfang der beratenden, diagnostischen oder therapeutischen Leistungen einschließlich der Anwendung von Arzneyspezialitäten und der zur Identifizierung dieser Arzneyspezialitäten und der jeweiligen Chargen im Sinne des § 26 Abs. 8 des Arzneimittelgesetzes, BGBl. Nr. 158/1983, erforderlichen Daten zu führen und hierüber der beratenden oder behandelten oder zu ihrer gesetzlichen Vertretung befugten Person alle Auskünfte zu erteilen. In Fällen eines Verdachts im Sinne des § 54 Abs. 4 sind Aufzeichnungen über die den Verdacht begründenden Wahrnehmungen zu führen. Den gemäß § 54 Abs. 5 oder 6 verständigten Behörden oder öffentlichen Dienststellen ist hierüber Auskunft zu erteilen.

(2) Ärzte sind zur automationsunterstützten Ermittlung und Verarbeitung personenbezogener Daten gemäß Abs. 1 sowie zur Übermittlung dieser Daten

1. an die Sozialversicherungsträger und Krankenfürsorgeanstalten in dem Umfang, als er für den Empfänger zur Wahrnehmung der ihm übertragenen Aufgaben eine wesentliche Voraussetzung bildet, sowie
2. an andere Ärzte oder medizinische Einrichtungen, in deren Behandlung der Kranke steht, mit Zustimmung des Kranken berechtigt. Die zur Beratung oder Behandlung übernommene Person hat das Recht auf Einsicht, Richtigstellung unrichtiger und Löschung unzulässigerweise verarbeiteter Daten.

(3) Die Aufzeichnungen sowie die sonstigen der Dokumentation im Sinne des Abs. 1 dienlichen Unterlagen sind mindestens zehn Jahre aufzubewahren.

Verschwiegenheits-, Anzeige- und Meldepflicht

§ 54. (1) Der Arzt und seine Hilfspersonen sind zur Verschwiegenheit über alle ihnen in Ausübung ihres Berufes anvertrauten oder bekannt gewordenen Geheimnisse verpflichtet.

(2) Die Verschwiegenheitspflicht besteht nicht, wenn

1. nach gesetzlichen Vorschriften eine Meldung des Arztes über den Gesundheitszustand bestimmter Personen vorgeschrieben ist,
2. Mitteilungen oder Befunde des Arztes an die Sozialversicherungsträger und Krankenfürsorgeanstalten oder sonstigen Kostenträger in dem Umfang, als er für

den Empfänger zur Wahrnehmung der ihm übertragenen Aufgaben eine wesentliche Voraussetzung bildet, erforderlich sind,

3. die durch die Offenbarung des Geheimnisses bedrohte Person den Arzt von der Geheimhaltung entbunden hat,
4. die Offenbarung des Geheimnisses nach Art und Inhalt zum Schutz höherwertiger Interessen der öffentlichen Gesundheitspflege oder der Rechtspflege unbedingt erforderlich ist.

(3) Die Verschwiegenheitspflicht besteht auch insoweit nicht, als die für die Honorar- oder Medikamentenabrechnung gegenüber den Krankenversicherungsträgern, Krankenanstalten, sonstigen Kostenträgern oder Patienten erforderlichen Unterlagen zum Zweck der Abrechnung, auch im automationsunterstützten Verfahren, Dienstleistungsunternehmen überlassen werden. Eine allfällige Speicherung darf nur so erfolgen, dass Betroffene weder bestimmt werden können noch mit hoher Wahrscheinlichkeit bestimmbar sind. Diese anonymen Daten sind ausschließlich mit Zustimmung des Auftraggebers an die zuständige Ärztekammer über deren Verlangen weiterzugeben.

- (4) Ergibt sich für den Arzt in Ausübung seines Berufes der Verdacht, dass
1. durch eine gerichtlich strafbare Handlung der Tod oder die Körperverletzung eines Menschen herbeigeführt, oder
 2. ein Minderjähriger oder sonst eine Person, die ihre Interessen nicht selbst wahrzunehmen vermag, misshandelt, gequält, vernachlässigt oder sexuell missbraucht worden ist, so ist er ermächtigt, hierüber persönlich Betroffenen oder Behörden oder öffentlichen Dienststellen Mitteilung zu machen, sofern das Interesse an dieser Mitteilung das Geheimhaltungsinteresse überwiegt.

(5) In den Fällen, in denen sich für den Arzt in Ausübung seines Berufes der Verdacht ergibt, dass durch eine gerichtlich strafbare Handlung der Tod oder die schwere Körperverletzung eines Menschen herbeigeführt worden ist, hat der Arzt der Sicherheitsbehörde unverzüglich Anzeige zu erstatten, es sei denn, die Anzeige würde in den Fällen schwerer Körperverletzung eine therapeutische Tätigkeit beeinträchtigen, deren Wirksamkeit eines persönlichen Vertrauensverhältnisses bedarf; im letztgenannten Fall hat er die betroffene Person über bestehende anerkannte Opferschutzeinrichtungen zu informieren. Die Anzeigepflicht entfällt weiters nicht, wenn die schwere Körperverletzung im Rahmen der ärztlichen Tätigkeit eines anderen Arztes herbeigeführt worden ist.

- (6) In den Fällen des Abs. 4 Z 2 hat der Arzt, sofern dies zur Verhinderung einer weiteren erheblichen Gefährdung des Wohls der betroffenen Person erforderlich ist, Meldung zu erstatten:
1. hinsichtlich Minderjähriger gegenüber dem zuständigen Jugendwohlfahrtsträger,
 2. hinsichtlich sonstiger Personen, die ihre Interessen nicht selbst wahrzunehmen vermögen, gegenüber dem PflEGschaftsgericht.

6. Hauptstück

Strafbestimmungen

§ 199. (1) Wer eine in den §§ 2 Abs. 2 und 3 oder 16 Abs. 1 und 2 umschriebene Tätigkeit ausübt, ohne hiezu nach diesem Bundesgesetz oder nach anderen gesetzlichen Vorschriften berechtigt zu sein, begeht, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, eine Verwaltungsübertretung und ist mit Geldstrafe bis zu 50 000 S zu bestrafen. Der Versuch ist strafbar.

(2) Sofern aus der Tat (Abs. 1) eine schwerwiegende Gefahr für Leib, Leben oder Gesundheit einer Person entstanden ist oder der Täter bereits zweimal wegen unbefugter ärztlicher Tätigkeit bestraft worden ist, ist der Täter mit Geldstrafe bis zu 300 000 S zu bestrafen.

(3) Wer den im § 3 Abs. 1 oder 3, § 12 Abs. 3, § 17 Abs. 1 oder 3, § 27 Abs. 2 oder Abs. 7 zweiter Satz, § 29 Abs. 1, § 31 Abs. 3, § 32 Abs. 3, § 35 Abs. 7, § 36, § 37 Abs. 1 letzter Satz oder 2, § 43 Abs. 2, 3, 4 oder 6, § 44, § 45 Abs. 3 oder 4, § 46, § 47 Abs. 1, § 48, § 49, § 50 Abs. 1 oder 3, § 51, § 52 Abs. 2, § 53 Abs. 1 bis 3, § 54 Abs. 1, § 55, § 56 Abs. 1, § 57 Abs. 1, § 63, § 89 oder § 194 erster Satz enthaltenen Anordnungen oder Verboten zuwiderhandelt, begeht, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, eine Verwaltungsübertretung und ist mit Geldstrafe bis zu 30 000 S zu bestrafen. Der Versuch ist strafbar.

(4) Wer den Anordnungen zuwiderhandelt, die in den auf Grund dieses Bundesgesetzes erlassenen Verordnungen enthalten sind, begeht, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, eine Verwaltungsübertretung und ist mit Geldstrafe bis zu 30 000 S zu bestrafen. Der Versuch ist strafbar.

3.10. Bundesgesetz: Gesundheits- und Krankenpflegegesetz - GuKG sowie Änderung des Krankenpflegegesetzes, des Ausbildungsvorbehaltsgesetzes und des Ärztegesetzes 1984; BGBl. I Nr. 108/1997

2. Abschnitt

Berufspflichten

Pflegedokumentation

§ 5. (1) Angehörige der Gesundheits- und Krankenpflegeberufe haben bei Ausübung ihres Berufes die von ihnen gesetzten gesundheits- und krankenpflegerischen Maßnahmen zu dokumentieren.

(2) Die Dokumentation hat insbesondere die Pflegeanamnese, die Pflegediagnose, die Pflegeplanung und die Pflegemaßnahmen zu enthalten.

(3) Den betroffenen Patienten, Klienten oder pflegebedürftigen Menschen oder deren gesetzlichen Vertretern ist auf Verlangen Einsicht in die Pflegedokumentation zu gewähren.

(4) Bei freiberuflicher Berufsausübung (§ 36) sind die Aufzeichnungen sowie die sonstigen der Dokumentation dienlichen Unterlagen mindestens zehn Jahre aufzubewahren.

Verschwiegenheitspflicht

§ 6. (1) Angehörige der Gesundheits- und Krankenpflegeberufe sind zur Verschwiegenheit über alle ihnen in Ausübung ihres Berufes anvertrauten oder bekannt gewordenen Geheimnisse verpflichtet.

(2) Die Verschwiegenheitspflicht besteht nicht, wenn

1. die durch die Offenbarung des Geheimnisses betroffene Person den Angehörigen eines Gesundheits- und Krankenpflegeberufes von der Geheimhaltung entbunden hat oder
2. die Offenbarung des Geheimnisses für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist oder
3. Mitteilungen des Angehörigen eines Gesundheits- und Krankenpflegeberufes über den Versicherten an Träger der Sozialversicherung und Krankenanstalten zum Zweck der Honorarabrechnung, auch im automationsunterstützten Verfahren, erforderlich sind.

Anzeigepflicht

§ 7. (1) Angehörige des gehobenen Dienstes für Gesundheits- und Krankenpflege, die gemäß § 35 Abs. 1 Z 1 und 6 und § 36 freiberuflich tätig sind, sind verpflichtet, der Staatsanwaltschaft oder der Sicherheitsbehörde unverzüglich Anzeige zu erstatten, wenn sich in Ausübung ihres Berufes der Verdacht ergibt, dass

1. durch eine gerichtlich strafbare Handlung der Tod oder die schwere Körperverletzung eines Menschen (§ 84 Abs. 1 Strafgesetzbuch - StGB, BGBl. Nr. 60/1974) herbeigeführt wurde oder
2. ein Unmündiger, Minderjähriger oder Wehrloser durch das Quälen oder Vernachlässigen (§ 92 StGB) am Körper verletzt oder an der Gesundheit geschädigt wurde (§ 83 Abs. 1 StGB) oder
3. ein Unmündiger oder Minderjähriger durch Beischlaf oder auf andere Weise zur Unzucht missbraucht wurde (§§ 206, 207 und 212 StGB).

(2) Die Anzeigepflicht besteht nicht, wenn

1. die Anzeige eine Tätigkeit der Gesundheits- und Krankenpflege beeinträchtigen würde, deren Wirksamkeit eines persönlichen Vertrauensverhältnisses bedarf oder
2. in den Fällen des Abs. 1 ein Unmündiger oder Minderjähriger betroffen ist und der Jugendwohlfahrtsträger unverzüglich verständigt wurde, sofern nicht durch eine gerichtlich strafbare Handlung der Tod des Unmündigen oder Minderjährigen herbeigeführt wurde.

Meldepflicht

§ 8. (1) Angehörige der Gesundheits- und Krankenpflege, die ihren Beruf im Rahmen eines Dienstverhältnisses gemäß § 35 Abs. 1 Z 2, 3, 4 und 5 oder § 90 ausüben, sind verpflichtet, dem Dienstgeber unverzüglich Meldung zu erstatten, wenn sich in Ausübung ihres Berufes der Verdacht ergibt, dass einer der in § 7 Abs. 1 angeführten Tatbestände vorliegt. Für den Dienstgeber gilt § 7.

(2) Die Meldepflicht gemäß Abs. 1 besteht nicht, wenn die Meldung eine Tätigkeit der Gesundheits- und Krankenpflege beeinträchtigen würde, deren Wirksamkeit eines persönlichen Vertrauensverhältnisses bedarf.

Auskunftspflicht

§ 9. (1) Angehörige der Gesundheits- und Krankenpflegeberufe haben

1. den betroffenen Patienten, Klienten oder pflegebedürftigen Menschen,
2. deren gesetzlichen Vertretern oder
3. Personen, die von den betroffenen Patienten, Klienten oder pflegebedürftigen Menschen als auskunftsberechtigt benannt wurden, alle Auskünfte über die von ihnen gesetzten gesundheits- und krankenpflegerischen Maßnahmen zu erteilen.

(2) Sie haben anderen Angehörigen der Gesundheitsberufe, die die betroffenen Patienten, Klienten oder pflegebedürftigen Menschen behandeln oder pflegen, die für die Behandlung und Pflege erforderlichen Auskünfte über Maßnahmen gemäß Abs. 1 zu erteilen.

3.11. Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird, das Telegraphenwegegesetz und das Fernmeldegebührengesetz geändert werden sowie ergänzende Bestimmungen zum Rundfunkgesetz und zur Rundfunkverordnung getroffen werden, BGBl 1997 Teil I, Nr. 100 vom 19.8.1997

12. Abschnitt - Fernmeldegeheimnis, Datenschutz

§ 87 Allgemeines

(1) Soweit dieses Bundesgesetz nicht anderes bestimmt, sind auf die in diesem Bundesgesetz geregelten Sachverhalte die Bestimmungen des Datenschutzgesetzes, BGBl.Nr. 565/1978, anzuwenden.

(2) Die Bestimmungen der Strafprozeßordnung bleiben durch die Bestimmungen dieses Abschnittes unberührt.

(3) In diesem Abschnitt bezeichnet der Begriff

- 1 “Betreiber“ Anbieter von öffentlichen Telekommunikationsdiensten im Sinne des 3. Abschnittes;
- 2 “Teilnehmer“ eine natürliche oder juristische Person, die mit einem Anbieter eines öffentlichen Telekommunikationsdienstes einen Vertrag über die Inanspruchnahme dieser Dienste geschlossen hat;
- 3 “Benutzer“ eine natürliche Person, die einen öffentlichen Telekommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben;
- 4 “Stammdaten“ alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter von Telekommunikationsdiensten oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:
 - Familienname und Vorname,
 - akademischer Grad,
 - Adresse,
 - Teilnehmernummer,
 - Bonität;
1. “Vermittlungsdaten“ alle personenbezogenen Daten, die sich auf Teilnehmer und Benutzer beziehen und für den Aufbau einer Verbindung oder für die Verrechnung von Entgelten erforderlich sind; dies sind:
 - aktive und passive Teilnehmernummern,
 - Anschrift des Teilnehmers,
 - Art des Endgerätes,
 - Gebührencode,
 - Gesamtzahl der für den Abrechnungszeitraum zu berechnenden Einheiten,
 - Art, Datum, Zeitpunkt und Dauer der Verbindung,
 - übermittelte Datenmenge, _

- andere Zahlungsinformationen, wie Vorauszahlung, Ratenzahlung, Sperren des Anschlusses oder Mahnungen;
2. "Inhaltsdaten" die Inhalte übertragener Nachrichten.

§ 88 Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen die Inhaltsdaten und die näheren Umstände der Kommunikation, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Betreiber und alle Personen, die an der Tätigkeit des Betreibers mitwirken, verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen einer im Rahmen der Nutzung eines öffentlichen Telekommunikationsdienstes erfolgten Kommunikation sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen durch Notruforganisationen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung.

(4) Werden mittels einer Funkanlage, eines Endgerätes oder mittels einer sonstigen technischen Einrichtung Nachrichten empfangen, die für diese Funkanlage, dieses Endgerät oder den Benutzer der sonstigen Einrichtung nicht bestimmt sind, so dürfen der Inhalt der Nachrichten sowie die Tatsache ihres Empfanges weder aufgezeichnet noch Unbefugten mitgeteilt oder für irgendwelche Zwecke verwertet werden. Aufgezeichnete Nachrichten sind zu löschen oder auf andere Art zu vernichten.

§ 91 Datenschutz - Allgemeines

(1) Stammdaten, Vermittlungsdaten und Inhaltsdaten dürfen nur für Zwecke der Besorgung eines Telekommunikationsdienstes ermittelt oder verarbeitet werden.

(2) Die Übermittlung von im Abs. 1 genannten Daten darf nur erfolgen, soweit das für die Erbringung jenes Telekommunikationsdienstes, für den diese Daten ermittelt und verarbeitet worden sind, durch den Betreiber erforderlich ist. Sonstige Übermittlungen dürfen nur auf Grund einer vorherigen schriftlichen Zustimmung der Betroffenen erfolgen. Die Zustimmung gilt nur dann als erteilt, wenn sie ausdrücklich als Antwort auf ein Ersuchen des Betreibers gegeben wurde. Die Betreiber dürfen die Bereitstellung ihrer Dienste nicht von einer solchen Zustimmung abhängig machen.

(3) Der Betreiber ist verpflichtet, den Teilnehmer darüber zu informieren, welche personenbezogenen Daten er ermitteln und verarbeiten wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten

gespeichert werden. Diese Information hat in geeigneter Form, insbesondere im Rahmen allgemeiner Geschäftsbedingungen und spätestens bei Beginn der Rechtsbeziehungen zu erfolgen. Das Auskunftsrecht nach dem Datenschutzgesetz bleibt unberührt.

§ 92 Stammdaten

(1) Stammdaten dürfen von Betreibern nur für folgende Zwecke ermittelt und verarbeitet werden:

1. Abschluß, Durchführung, Änderung oder Beendigung des Vertrages mit dem Teilnehmer;
2. Verrechnung der Entgelte und
3. Erstellung von Teilnehmerverzeichnissen, auch gemäß § 26.

(2) Stammdaten sind spätestens nach Beendigung der Rechtsbeziehungen mit dem Teilnehmer vom Betreiber zu löschen. Ausnahmen sind nur soweit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen.

§ 93 Vermittlungsdaten

(1) Vermittlungsdaten dürfen grundsätzlich nicht gespeichert werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren.

(2) Sofern dies für Zwecke der Verrechnung von Entgelten erforderlich ist, hat der Betreiber Vermittlungsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann. Diese Daten sind im Streitfall der entscheidenden Einrichtung sowie der Schlichtungsstelle unverkürzt zur Verfügung zu stellen. Wird ein Verfahren über die Höhe der Entgelte eingeleitet, dürfen die Daten bis zur endgültigen Entscheidung über die Höhe der Entgelte nicht gelöscht werden. Der Umfang der gespeicherten Vermittlungsdaten ist auf das unbedingt notwendige Minimum zu beschränken.

(3) Die Verarbeitung von Vermittlungsdaten darf nur durch solche Personen erfolgen, die mit der Besorgung jener Aufgaben betraut sind, für die Daten ermittelt und verarbeitet werden dürfen.

(4) Dem Betreiber ist außer den gesetzlich bestimmten Fällen untersagt, einen Teilnehmeranschluß über die Zwecke der Verrechnung hinaus nach den von diesem Anschluß aus angerufenen Teilnehmernummern auszuwerten. Mit Zustimmung des Teilnehmers darf der Betreiber die Daten zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste verwenden.

=== Ende von MAGDA-LENA Version 2.0 ===