REPUBLIK ÖSTERREICH
DATENSCHUTZKOMMISSION

A-1010 Wien, Hohenstaufengasse 3
Tel. ++43-1-531 15/2525
Fax: ++43-1-531 15/2690
e-mail: dsk@dsk.gv.at
DVR: 0000027

GZ: DSK-K054.123/0002-DSK/2011

An das
Bundesministerium für Gesundheit

per E-Mail: clemens.auer@bmg.gv.at
carina.milisits@bmg.gv.at
vera.pribitzer@bmg.gv.at

Betrifft: Entwurf eines Bundesgesetzes, mit dem ein Gesundheitstelematikgesetz 2011 erlassen und das Allgemeine Sozialversicherungsgesetz, das Gewerbliche Sozialversicherungsgesetz, das Bauern-Sozialversicherungsgesetz, das Beamten-Kranken- und Unfallversicherungsgesetz, das Gentechnikgesetz, das Gesundheits- und Krankenpflegegesetz, das Hebammengesetz, das Medizinische Masseur- und Heilmasseurgesetz und das Strafgesetzbuch, geändert werden (Elektronische Gesundheitsakte-Gesetz – ELGA-G);

Stellungnahme der Datenschutzkommission

Die Datenschutzkommission nimmt zu dem im Betreff genannten Entwurf wie folgt Stellung:

Vorbemerkungen

Der wesentliche Inhalt des vorliegenden Gesetzesentwurfs über die elektronische Gesundheitsakte liegt in der Schaffung „eines Informationsverbundes“, in dem alle Gesundheitsdiensteanbieter (Ärzte, Zahnärzte, Apotheken und Krankenanstalten) – unabhängig von weiteren Zustimmungen der Betroffenen – grundsätzlich Zugriff auf die über Verweise zugänglichen Gesundheitsakten haben. Die Ziele liegen im Wesentlichen in einer verbesserten Betreuung der Patienten und einer allgemeinen Verbesserung des Gesundheitssystems. Weite Teile der Konkretisierung – wie etwa das gesamte System der Rollenverteilung – werden späteren Verordnungen vorbehalten.

Zu dem im Gesetz auch in anderen Zusammenhängen vorgenommen Verweis auf spätere Verordnungen ist darauf hinzuweisen, dass die wesentlichen Eingriffe in das Grundrecht bereits durch das Gesetz zu determinieren sind. Gegenstand der datenschutzrechtlichen Bewertung ist daher ausschließlich das Gesetz.

Nach der Verfassungsbestimmung des § 1 Abs. 2 letzter Satz DSG 2000 ist selbst bei zulässigen Beschränkungen des Datenschutzgrundrechtes der Eingriff nur in der gelindesten zum Ziel führenden Art durchzuführen. Eine der zentralen Aufgaben der Bestimmungen des Datenschutzes liegt darin, Gefährdungspotentiale faktisch dadurch zu unterbinden, dass die Einrichtung von Datenverarbeitungen, die sensible Daten (etwa Gesundheitsdaten) betreffen, teilweise schon gar nicht zugelassen werden (vgl. § 19 DSG 2000). Zeigt doch die praktische Erfahrung, dass rechtliche Schranken oft nicht ausreichen, wenn faktisch die Erlangung der Informationen durch die zentrale Datenverarbeitung einfach ist (dazu reicht schon ein Blick in die Tageszeitungen, in denen immer wieder selbst dem Amtsgeheimnis unterliegende Daten veröffentlicht werden).

Mit dem Gesetzesvorschlag wird nun einer beinahe unüberblickbaren Personengruppe (alle niedergelassenen Ärzte, Zahnärzte, Ordinationsgehilfen, Krankenhauspersonal etc.) in einer derzeit nicht absehbaren Weise der Zugang zu den Gesundheitsdaten möglichst aller Patienten eröffnet.

Derzeit werden dagegen die Gesundheitsdaten dadurch, dass sie sich (ohne Verweise) dezentral bei Personen und Institutionen befinden, denen der Patienten im Rahmen des Behandlungsvertrags sein Vertrauen ausgesprochen hat und von denen ein potentieller nicht berechtigter Interessent an diesen Gesundheitsdaten meist keine Kenntnis hat, wesentlich sicherer aufgehoben.

Grundsätzlich wäre daher zu bedenken, dass dem Ziel der besseren Verfügbarkeit der Gesundheitsdaten zur Behandlung der Patienten auch in einer weniger eingriffsintensiven Art genauso gedient wäre. So könnten etwa nur die Patienten selbst oder die behandelnden Ärzte faktisch über diese Daten verfügen (Chip, Memory-Stick, Sicherungskopie bei einem Vertrauensarzt – Übermittlung im Anlassfall über Ersuchen des Patienten). Jedenfalls könnte selbst beim vorliegenden System vorgesehen werden, dass der Zugriff der Mitwirkung der Patienten bedarf (etwa Abruf nur bei Übergabe der e-card und eines Codes, der für Fälle, in denen die Zustimmung des Patienten nachweislich nicht eingeholt werden kann, bei einer unabhängigen Stelle aufliegt).

Dem Ziel der Verbesserung der allgemeinen Planung und Steuerung im Gesundheitswesen wäre auch durch Daten ohne Personenbezug ausreichend Rechnung getragen.

Nach dem vorgesehenen System bleibt aber für den Patienten die Zahl der Personen, die faktisch Zugriff haben, völlig unüberblickbar, mag der unberechtigte Zugriff im Nachhinein auch dokumentiert und strafbar sein. Die Strafbarkeit reicht aber bei ausreichendem Interesse (Gesundheitsdaten Prominenter, wirtschaftlich schwerwiegende Entscheidungen etc.) und einer unüberblickbaren Zahl potentieller Täter oft selbst bei schwereren Strafandrohungen nicht zur Abschreckung aus. Bei der kleinen Gruppe jener Personen, die

unmittelbar bei der Wartung und Kontrolle der EDV-Systeme tätig sind, werden darüber hinaus wohl auch die unberechtigten Zugriffe nie nachweisbar sein.
Zwar werden dem Patienten im vorliegenden Entwurf „Widerspruchsrechte“ eingeräumt, jedoch werden diese für breite Kreise nicht nachvollziehbar und effektiv ausübbar sein. Hinzu kommt, dass dann, wenn in der täglichen Routine der Zugriff auf die elektronische Gesundheitsakte selbstverständlich wird, nicht nur ein hoher Druck auf Unterlassung derartiger Widersprüche vorhanden sein wird, sondern auch die Gefahr besteht, dass die Gesundheitsanbieter mit dieser Situation nicht mehr adäquat umgehen werden können.

I. Zu Art. 1 (Gesundheitstelematikgesetz 2011 – GTelG 2011)

1.) Allgemeines:

a.) Bei Gesundheitsdaten handelt es sich um sensible Daten im Sinne des § 4 Z 2 DSG 2000 und damit besonders schutzwürdige Daten im Sinne des § 1 Abs. 2 DSG 2000. Diese dürfen nach dem DSG 2000 nur unter bestimmten Bedingungen verwendet werden (siehe dazu die Bestimmungen des § 1 Abs. 2 iVm § 9 DSG 2000): Bei der Verwendung des äußerst zwiespältigen Satzes *„Wer mehr weiß, kann mehr.“*, der in den Erläuterungen (S. 6) offenbar zur Untermauerung des Nutzens von ELGA dienen soll, wird übersehen, dass *der, der „mehr weiß“, auch wesentlich mehr in Grund- und Menschenrechte anderer eingreifen* kann. Auf Grund der Sensibilität der Daten kann eine gesetzliche Regelung, die eine derartige Verwendung von Patientendaten in einem Informationsverbundsystem vorsieht, nur dann gerechtfertigt werden, wenn dabei in höchstmöglichem Maß die Patientenautonomie gewahrt bleibt. Obwohl im gegenständlichen Gesetzesentwurf grundsätzlich versucht wird, ein gewisses Maß an Selbstbestimmung der Patient/inn/en zu gewährleisten, fragt es sich grundsätzlich, wie diese Autonomie in der Praxis gewährleistet werden soll. So fehlen etwa wirksame Mittel, um eine faktische Diskriminierung jener Personen zu verhindern, die generell oder im Einzelfall Widerspruch zur Verwendung ihrer Daten erheben.

Im Übrigen wird angemerkt, dass ein grundsätzliches Opt-In-Verfahren für ELGA aus Datenschutzsicht gegenüber einem grundsätzlichen Opt-Out vorzuziehen wäre.

Weiters wird festgehalten, dass ein Entwurf, der eine so sensible Materie regelt und sich vor allem auch an Patientinnen und Patienten als Normunterworfene wendet, auch entsprechend klar und verständlich sein sollte. Beim vorliegenden Entwurf scheint dies nicht ausreichend gewährleistet. Für Patientinnen und Patienten wird vielmehr – vor allem wenn es sich dabei um ältere oder nicht technikaffine Personen handelt – aus dem vorliegenden Gesetzesentwurf kaum verständlich sein, dass hierbei sensible Daten ohne vorherige

Zustimmung verwendet werden sollen und welche datenschutzrechtlichen Folgen eine derartige Verwendung mit sich bringt.

Der Entwurf sollte daher vorweg unter diesem Gesichtspunkt nochmals geprüft und überarbeitet werden.

b.) Zur unionsrechtlichen Rechtsgrundlage von ELGA ist anzumerken, dass die beim BMG eingerichtete STRING-Kommission in ihrer datenschutzrechtlichen Analyse (vom Jänner 2005) dargelegt hat, dass der in Art. 8 Abs. 3 der Datenschutzrichtlinie 95/46/EG (DS-RL) und durch § 9 Z 12 DSG 2000 umgesetzte Tatbestand keine ausreichende Rechtsgrundlage für ein umfassendes Datenverbundsystem wie ELGA sein kann.[1] Auch die Art. 29-Gruppe kommt in ihrem im Arbeitspapier „Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“, WP 131, zu dem Ergebnis, dass Art. 8 Abs. 3 DS-RL allein als Rechtsgrundlage nicht ausreicht und geht in weiterer Folge von Art. 8 Abs. 4 DS-RL als Grundlage aus.

Während im vorliegenden Gesetzesentwurf nun zutreffender Weise auf Art. 8 Abs. 4 DS-RL Bezug genommen wird, führen die Erläuterungen auf Seite 4 aus, dass „sowohl Abs. 3, der als spezielle, auf den Gesundheitsbereich zugeschnittene Ausprägung des Abs. 4 anzusehen ist, als auch Abs. 4 als unionsrechtliche Grundlage für eine gesetzliche Grundlage von ELGA in Betracht“ kämen, und um dem wichtigen öffentlichen Interesse an ELGA besonderen Ausdruck zu verleihen, ausdrücklich Art. 8 Abs. 4 DS-RL als unionsrechtliche Grundlage herangezogen wird.

Es wird daher angeregt, die Erläuterungen (S. 4 f) entsprechend zu ändern und nur auf Art. 8 Abs. 4 DS-RL einzugehen.

2.) Zum Gesetzesentwurf

Zu § 1:

Nach § 1 Abs. 3 des Entwurfs gilt dieses Gesetz nicht für Gesundheitsdiensteanbieter (im Folgenden: GDA), die über keine Einrichtungen der Informations- und Kommunikationstechnologie verfügen. Das bedeutet, dass diese GDA nicht an ELGA teilnehmen. In der Folge ist fraglich, ob Patienten dieser nicht teilnehmenden GDA ihre Gesundheitsdaten zu ihrer elektronischen Gesundheitsakte hinzufügen können oder wie an ELGA teilnehmende GDA erkennen können, dass allenfalls für die Behandlung wichtige Befunde der/des Patientin/en von einem nicht an ELGA teilnehmenden GDA in der elektronischen Gesundheitsakte fehlen.

1 Siehe dazu auch Daniel ENNÖCKL, Datenschutzrechtliche Fragen der elektronischen Gesundheitsakte (ELGA), in: Kierein/Lanske/Wenda (Hg), Jahrbuch Gesundheitsrecht 2010, 61 ff.

Der Wortlaut des in § 1 Abs. 4 stehenden Satzes „In diesen Fällen ist der Auftraggeber des privaten Bereichs für den Bereich der Erzeugung und der Verwendung der bPK wie ein Auftraggeber des öffentlichen Bereiches zu behandeln“ ist insofern missverständlich, als er zur Annahme führen könnte, dass in diesem Bereich die Datenschutzkommission zuständig wäre. Dies würde der Verfassungsbestimmung des § 1 Abs. 5 DSG 2000 widersprechen. Die in den Erläuterungen getroffene Klarstellung („Die Zuständigkeit der Zivilgerichte gemäß § 1 Abs. 5 DSG 2000 bleibt unberührt.“) sollte daher in den Gesetzestext übernommen werden.

Zu § 2:

Die in § 2 Z 1 getroffene Definition von Gesundheitsdaten scheint sehr weit, da diese beispielsweise auch die „gesundheitsrelevanten Lebensgewohnheiten oder Umwelteinflüsse“ umfassen. Im Hinblick darauf, dass im Prinzip alle Gesundheitsdaten in ELGA einfließen können, wäre diese weite Definition nochmals zu prüfen.

Die in § 2 Z 2 genannte Definition des GDA ist zu weitgehend. Man könnte darunter etwa auch Versicherungen subsumieren. Eine Einschränkung dieser weiten Interpretation in den Erläuterungen (wie dies im Fall der Rechtsanwälte vorgenommen wurde) scheint im Allgemeinen nicht ausreichend. Vielmehr sollte von vornherein im GTelG 2011 eine entsprechend engere Legaldefinition des GDA (abstellend auf das Kriterium der Erbringung einer Gesundheitsdienstleistung) geschaffen werden, um insb. Versicherungen und Rechtsanwälte auszunehmen.

Im Hinblick auf die Definition von ELGA in § 2 Z 6 sollte ausdrücklich festgelegt werden, ob es sich bei ELGA um ein Informationsverbundsystem (§ 4 Z 13 DSG 2000) bzw. um mehrere Informationsverbundsysteme handelt und wer der konkrete „Betreiber“ und „Auftraggeber“ bzw. wer allenfalls Dienstleister dieses Informationsverbundsystems (dieser Informationsverbundsysteme) ist/sind.

Es fragt sich, wieso der in § 2 Z 10 lit. e genannte National Contact Point (NCP) GDA und damit auch Auftraggeber im ELGA-System sein soll. Vielmehr wurde bisher vom BMG im Zusammenhang mit epSOS die Meinung vertreten, dass der NCP als datenschutzrechtlicher Dienstleister fungiert, was auch konsequent erscheint, da der beim BMG eingerichtete NCP wohl nicht selbst Gesundheitsdienstleistungen erbringt und „für eigene Zwecke“ Gesundheitsdaten verwendet. Unklar erscheint auch, welche konkreten „Auflagen“ der NCP nach lit. dd erfüllen muss.

Bei dem in § 2 Z 13 definierten „Verweisregister“ sollte im Gesetz klargestellt werden, dass es sich hierbei um ein Informationsverbundsystem handelt und wer in diesem Fall „Betreiber“ bzw. wer allenfalls Dienstleister dieses Verweisregisters ist. Angesichts der knappen Regelung des § 19 Abs. 3, welcher nur festlegt, dass Auftraggeber für die Speicherung der

jeweilige ELGA-GDA ist, geht aus dem Entwurf auch der Zweck und die Funktion des Verweisregisters nicht ausreichend klar hervor. Weiters scheint unklar, wieso in den Erläuterungen ausgeführt wird, dass diese Bestimmung eine lex specialis zu den im DSG 2000 geregelten „Informationsverbundsystemen“ darstellt.

Zu § 3:

Vorweg ist anzumerken, dass aus dem Entwurf nicht hervorgeht, in welchem Zusammenhang der 2. Abschnitt zu den Datensicherheitsmaßnahmen (§§ 3 ff) zu den übrigen Abschnitten, insb. zum 4. Abschnitt (Elektronische Gesundheitsakte – ELGA), steht und auf welche Teile des Entwurfes der 2. Abschnitt Anwendung findet.

Die Art. 29-Datenschutzgruppe weist in ihrem Arbeitspapier WP 131 ausdrücklich darauf hin, dass die Identifizierung und Authentifizierung von Patienten und medizinischem Personal absolut zweifelsfrei gewährleistet werden muss, damit nicht auf Grund von Fehlern bei der Patientenidentifikation irrtümlicherweise Daten einer anderen Person verwendet werden.

Angesichts der zur Verarbeitung von Patientendaten in elektronischen Patientenakten von der Art. 29-Datenschutzgruppe erarbeiteten Grundsätze ist es nicht nachvollziehbar, weshalb die §§ 4 bis 7 (insb. Nachweis und Prüfung der Identität, der Rollen und Integrität sowie die Gewährleistung der Vertraulichkeit) bei der Weitergabe elektronischer Gesundheitsdaten gemäß § 3 Abs. 1 des Entwurfes nicht angewendet werden sollen, wenn Gesundheitsdaten so weitergegeben werden, dass unbefugte Dritte vom Zugriff auf Gesundheitsdaten ausgeschlossen sind.

Unbefugte Dritte müssen nach § 1 Abs. 1 bzw. § 14 Abs. 1 zweiter Satz DSG 2000 immer vom Zugriff auf Daten ausgeschlossen sein. Dies zu gewährleisten wäre gerade die Aufgabe von Datensicherheitsmaßnahmen und kann daher nicht zum Ausschluss ihrer Anwendung führen. Es ist nicht nachvollziehbar, weshalb die Weitergabe von Gesundheitsdaten innerhalb von Spitälern (und damit allenfalls zwischen völlig unterschiedlichen Abteilungen) keinen Datensicherheitsmaßnahmen gemäß den §§ 4 ff unterliegen sollte. Ausnahmen von Datensicherheitsmaßnahmen sollten einerseits – soweit sie erforderlich und verhältnismäßig sind – nur als Übergangsbestimmungen in einem zeitlich äußerst eng begrenzten Rahmen und andererseits darüber hinaus nur für konkret im Gesetz zu definierende Ausnahmefälle, wie etwa bei einem Systemausfall oder bei akuten Gesundheitsbedrohungen, zulässig sein.

Zwar ist zu bedenken, dass es wohl immer besondere Ausnahmefälle geben wird, in denen keine elektronische Datenübermittlung zur Verfügung steht oder nicht benutzt werden kann, so dass auf „konventionelle“ Übermittlungstechniken (Post, Fax, Telefon oder persönliche Übergabe) zurückgegriffen werden muss; es sollten für diese Übermittlungsarten aber auch die jeweils entsprechend geeigneten Datensicherheitsmaßnahmen normiert werden. Derzeit

sind solche nur lückenhaft in Gestalt der Übergangsbestimmungen des § 26 enthalten (siehe hierzu auch die Anmerkungen zu § 26).

§ 3 Abs. 2 Z 1 des Entwurfes nimmt auf eine Weitergabe von Daten nach § 9 DSG 2000 Bezug. In diesem Zusammenhang ist zu bemerken, dass die Weitergabe von personenbezogenen ELGA-Daten nicht auf Grund sämtlicher Tatbestände des § 9 DSG 2000 möglich sein darf, sondern dass der Verwendungszweck dieser Daten auf die Behandlung der Patienten (unter Heranziehung früherer einschlägiger Dokumentationen) eingeschränkt werden muss.

Auch die Art. 29-Datenschutzgruppe vertritt die Ansicht, dass der Zugang zu medizinischen Daten in einer elektronischen Patientenakte für andere als die „Behandlungszwecke" grundsätzlich verboten sein sollte. Dies würde den Zugang von praktischen Ärzten, die als Sachverständige für Dritte arbeiten (z.B. für private Versicherungsunternehmen, bei Gericht und für Arbeitgeber) ausschließen.

Es ist daher in Z 1 klarzustellen, dass nicht alle Zwecke des § 9 DSG 2000 für die Verwendung von ELGA-Daten herangezogen werden dürfen.

Zu § 4:

Unklar ist, wie die Überprüfung der Identität von Personen durch „Eintragung bzw. Einsichtnahme" in den Patientenindex stattfinden soll. Es müssten – angesichts der allenfalls schwerwiegenden medizinischen Folgen – Maßnahmen ergriffen werden, die sicherstellen, dass Patienten zweifelsfrei identifiziert werden, um ausschließen zu können, dass Befunde falschen Patienten zugewiesen werden.

Unklar ist auch, wie die Überprüfung der Identität von GDA durch „Eintragung bzw. Einsichtnahme" in den eHealth-Verzeichnisdienst vonstattengehen soll. In Entsprechung des E-Government-Systems des Bundes sollte zudem bei der Identifikation von GDA der Nutzung des bereichsspezifischen Personenkennzeichen der Vorzug gegeben werden und andere Identifikationssysteme nur für einen im Vorhinein zeitlich begrenzten Übergangszeitraum subsidiär zugelassen werden.

Zu § 5:

Eine allgemeine Festlegung der Rollen sollte angesichts der von der jeweiligen Rolle abhängigen Möglichkeiten hinsichtlich der Verwendung von sensiblen Daten bereits im Gesetz selbst erfolgen (siehe dazu auch die Bemerkungen zu § 20).

Zu § 6:

Bei der Verschlüsselung sollte beachtet werden, dass sich ein Personenbezug nicht nur aus dem Namen, sondern unter Umständen auch aus den Inhalten der Befunde ableiten lassen

kann. Zum Zugriff auf Daten führt die Art. 29-Datenschutzgruppe aus, dass dieser durch Unbefugte faktisch unmöglich sein und von vornherein unterbunden werden muss, wenn das System aus Sicht des Datenschutzes annehmbar sein soll. Die Sicherheit des Systems muss mit Hilfe des aktuellen Wissenstands und der neuesten Techniken im Bereich der Informatik und Informationstechnik gewährleistet werden. Soweit irgend möglich, sollten daher datenschutzfreundliche Technologien (Privacy Enhancing Technologies) zum Einsatz kommen.

Eine weitestgehende Anwendung der Verschlüsselungstechnik wäre daher anzustreben.

Zu § 7:

Es ist fraglich, ob es eine Wahlmöglichkeit zwischen der Verwendung fortgeschrittener oder qualifizierter elektronischer Signaturen geben soll bzw. nach welchen Grundsätzen sonst zu entscheiden ist, welche elektronischen Signaturen verwendet werden müssen. Grundsätzlich wäre der höchstmögliche Sicherheitsstandard heranzuziehen.

Zu § 8:

Hier sollte der Zweck der Übermittlung der Dokumentation an die genannten Stellen angeführt werden.

Zusätzlich zu der in § 8 vorgesehenen Dokumentationspflicht sollte unbedingt eine lückenlose Protokollierung aller Zugriffe auf Gesundheitsdaten normiert werden. Dies könnte in einem weiteren § 9 neu erfolgen. Insofern scheint es auch zu eng, dass die Bestimmungen des 2. Abschnitts nur auf die „Weitergabe von Daten“ beschränkt sind, da auch sichergestellt werden muss, dass auch im Bereich etwa einer Abteilung eines Krankenhauses nur befugte Personen Zugriff nehmen.

Zu § 9:

§ 9 Abs. 3 legt nicht fest, *wer* die in Z 1 aufgezählten Daten *an wen* übermitteln soll. Diesbezüglich sollte die Bestimmung konkretisiert werden.

Weiters erscheint in § 9 Abs. 3 Z 3 nicht klar, welche „übrigen“ GDA in dieser Bestimmung gemeint sind. Auch die Erläuterungen geben keinen Aufschluss darüber. Es sollte diesbezüglich – insb. auch im Sinne der Rechtssicherheit – eine abschließende Aufzählung im Gesetz vorgenommen werden.

Zu § 10:

Aus § 10 Abs. 1 Z 7 geht nicht hervor, zu welchem Zweck die Datenart „Staatsangehörigkeit“ des GDA verwendet wird.

In § 10 Abs. 5 wäre der Zweck der Übermittlung zu ergänzen (d.h. es wäre festzulegen, woraus sich der Bedarf von Auftraggebern oder Dienstleistern im Gesundheitswesen ergeben kann).

Zu § 11:

Aus der Bestimmung wird nicht klar, ob die Berichte und Auskünfte allenfalls auch (direkt oder indirekt) personenbezogene Daten enthalten können. Weiters ist unklar, wie der unterschiedliche Detaillierungsgrad festgelegt wird und welche Informationen dann jeweils umfasst sind. Schließlich ist nicht erkennbar, in welcher Form bzw. durch welchen Rechtsakt (Verordnung?) das Berichtswesen in Abs. 1 eingerichtet und Art und Umfang der Erhebungen in Abs. 2 festgelegt werden sollen.

Zum 4. Abschnitt „Elektronische Gesundheitsakte (ELGA)“ - §§ 13 bis 23:

Vorbemerkung:

Grundsätzlich scheint es angesichts der „Zersplitterung“ der Angaben zu Betreiber und Auftraggeber im 4. Abschnitt (so sind die ELGA-GDA nach § 19 Abs. 1 Auftraggeber für die Speicherung von ELGA-Gesundheitsdaten sowie nach Abs. 2 Auftraggeber für die Speicherung von elektronischen Verweisen im Verweisregister; in weiterer Folge „betreiben“ die ELGA-Systempartner ein Berechtigungssystem nach § 20 Abs. 1; bei den Zugriffsberechtigungen ist wiederum der/die jeweilige ELGA-Teilnehmer/in Auftraggeber und sind die ELGA-Systempartner Dienstleister) und den damit zusammenhängenden Unklarheiten erforderlich, zu Beginn dieses Abschnittes übersichtlich und verständlich darzustellen, ob es sich bei ELGA um ein oder mehrere Informationsverbundsysteme handelt, wer jeweils Auftraggeber, wer Betreiber und wer allenfalls Dienstleister ist.

Zu § 13:

Zunächst ist festzuhalten, dass der in § 13 Abs. 1 Z 1 scheinbar primär festgelegte Zweck von ELGA in dieser Formulierung irreführend und nicht zutreffend scheint, da die Probleme des Rechtsschutzes und der Informationsrechte in dieser Form gar nicht bestünden, gäbe es nicht die mit ELGA verbundenen Eingriffe. Zutreffender wäre es daher, etwa an die Z 2 den Zusatz „unter völliger Wahrung der Patient/inn/en/rechte, insbesondere der Informationsrechte und dem Rechtsschutz gemäß DSG 2000“ anzubringen.

Es sollte daher in der Aufzählung in § 13 Abs. 1 vorweg angeführt werden, dass die Nutzung von ELGA primär dem Behandlungszweck dient. Erst danach sollte bezeichnet werden, welchen sekundären Zwecken ELGA dient. Darüber hinaus sollte bei den genannten Zwecken erkenntlich sein, ob Daten personenbezogen verwendet werden.

In § 13 Abs. 4 ist schon im Ansatz nicht erkennbar, um welche Daten es sich hierbei konkret handelt und zu welchem Zweck die genannten Daten in personenbezogener Form benötigt werden. Es ist nicht ersichtlich, um welche Register es sich hierbei handelt. Wenngleich die Erläuterungen eine exemplarische Aufzählung von verschiedenen Registern enthalten, sollten aufgrund der Sensibilität der Regelungsmaterie stattdessen alle Register, aus denen Daten für ELGA verwendet werden, im Gesetz abschließend aufgezählt werden. Es ist auch davon auszugehen, dass ein Zugriff auf Register durch GDA nur im Behandlungsfall zulässig wäre. Abs. 4 ist im Übrigen nicht als ausreichende Rechtsgrundlage zur konkreten Verwendung von Gesundheitsdaten aus Registern, insbesondere auch nicht für eine Verknüpfung derartiger Daten mit ELGA-Gesundheitsdaten, zu werten.

Abs. 5 ist insofern nicht nachvollziehbar, als davon auszugehen ist, dass die Übermittlung von ELGA-Gesundheitsdaten in das Ausland und vice versa immer zu Behandlungszwecken erfolgt. Sollte dies nicht der Fall sein, so müsste jedenfalls eine Zustimmung der Betroffenen für die Übermittlung für diesen konkreten Zweck vorliegen (welche Zwecke hier denkbar sind, sollte sinnvollerweise im Gesetz, mindestens aber in den Erläuterungen ausgeführt sein). Weiters wird darauf hingewiesen, dass die Qualifizierung des NCP als GDA zweifelhaft scheint (siehe die Ausführungen zu § 2).

Die in Abs. 6 genannte Verordnungsermächtigung scheint bezüglich technischer Gegebenheiten, die sich häufig nach dem Stand der Technik ändern, sinnvoll. Grundsätzliche Regelungen hinsichtlich zu ergreifender Sicherheitsmaßnahmen sollten jedoch bereits im Gesetz selbst enthalten sein. Unklar ist auch, in welchem Verhältnis diese Regelungen zu den im 2. Abschnitt des Entwurfes geregelten Datensicherheitsmaßnahmen stehen bzw. ob für ELGA im Wege der Verordnungsermächtigung über Abs. 6 hinaus andere oder zusätzliche Regelungen geschaffen werden sollen.

Zu § 14:

Die in § 14 Abs. 2 genannte Ausnahme ist in mehrfacher Weise unklar. Zunächst ist unklar, was unter „medizinischen Notfällen“ gemeint ist (ist damit die Verwendung „im lebenswichtigen Interesse der Betroffenen“ gemeint?). Weiters ist unklar, wer in solchen Notfällen zugreifen darf, wenn nicht der berechtigte GDA. Aus datenschutzrechtlicher Sicht darf nur jener Daten verwenden, der auch über eine entsprechende rechtliche Befugnis verfügt (§ 7 Abs. 1 DSG 2000).

In § 14 Abs. 3 ist unklar, wieso die Daten zur Wahrnehmung der Teilnehmer/innen/rechte gemäß § 16 von „gesetzlichen oder bevollmächtigten Vertreter/innen“ verwendet werden dürfen. Soweit diese andere ELGA-Teilnehmer/innen vertreten, geht es um die

Wahrnehmung der Rechte dieser Teilnehmer/innen. Soweit die Vertreter/innen selbst Patient/inn/en sind, sind sie selbst unter § 14 Abs. 3 Z 2 lit. a zu subsumieren.

Grundsätzlich stellt sich die Frage nach einem expliziten Verwendungsverbot der ELGA-Daten für andere Zwecke als die genannten, welches wohl einer verfassungsrechtlichen Absicherung bedürfte, um zu verhindern, dass durch einfaches Gesetz das Verwendungsverbot unterlaufen wird bzw. zumindest Interpretationsschwierigkeiten erzeugt werden. Es muss sichergestellt werden, dass beispielsweise Arbeitgeber, Behörden und Versicherungen keinen Zugang zu ELGA-Gesundheitsdaten bekommen dürfen und können.

In § 14 Abs. 4 sollte klargestellt werden, dass es sich bei „anderen Gesundheitsdiensteanbietern" um solche handelt, die nicht in die Behandlung der Patient/inn/en eingebunden sind. Der letzte Halbsatz sollte lauten „…ist es verboten ELGA-Gesundheitsdaten zu verlangen oder *zu verwenden*."

In § 14 Abs. 5 wäre zu präzisieren, was als „rechtlich zulässiger Grund" zu verstehen ist.

Überdies sollte eine ausdrückliche Verschwiegenheitspflicht für allfällige Dienstleister gesetzlich festgelegt werden. Eine weite physische Auslagerung der Daten an externe Dienstleister sollte zudem verboten sein.

Die in § 14 Abs. 6 enthaltene Anordnung, dass die Meldepflicht nach § 17 DSG 2000 für Datenanwendungen aufgrund dieses Abschnitts mit diesem Bundesgesetz erfüllt sei, widerspricht den einschlägigen Bestimmungen der DS-RL. Hiezu ist auf die Pflicht zur Meldung *bei der Kontrollstelle* nach Art. 18 DS-RL hinzuweisen: Demnach sehen die Mitgliedstaaten eine Meldung durch den für die Verarbeitung Verantwortlichen oder gegebenenfalls seinen Vertreter bei der in Art. 28 DS-RL genannten Kontrollstelle vor, bevor eine vollständig oder teilweise automatisierte Verarbeitung oder eine Mehrzahl von Verarbeitungen zur Realisierung einer oder mehrerer verbundener Zweckbestimmungen durchgeführt wird.

Die Mitgliedstaaten können eine Vereinfachung der Meldung oder eine Ausnahme von der Meldepflicht nur in den in Art. 18 Abs. 2 DS-RL aufgezählten Fällen vorsehen, so ua. dann, wenn für Verarbeitungskategorien, bei denen unter Berücksichtigung der zu verarbeitenden Daten eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen unwahrscheinlich ist, die Zweckbestimmungen der Verarbeitung, die Daten oder Kategorien der verarbeiteten Daten, die Kategorie(n) der betroffenen Personen, die Empfänger oder Kategorien der Empfänger, denen die Daten weitergegeben werden, und die Dauer der Aufbewahrung festgelegt werden.

Die Mitgliedstaaten können gemäß Art. 18 Abs. 3 DS-RL auch vorsehen, dass Art. 18 Abs. 1 DS-RL keine Anwendung auf Verarbeitungen findet, deren einziger Zweck das Führen eines

Registers ist, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht.

Die Erläuterungen zum vorliegenden Entwurf nehmen diesbezüglich auf die in Art. 18 Abs. 2 DS-RL normierte Ausnahme Bezug, dass eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen unwahrscheinlich ist.

An die Anwendbarkeit einer solchen Ausnahme bei Gesundheitsdaten ist aber nur etwa dann zu denken, wenn Daten zur Gesundheit vom behandelnden Arzt unter Beachtung des Berufsgeheimnisses und der sonstigen spezifischen Pflichten verarbeitet werden (vgl. *Dammann/Simitis*, EG-Datenschutzrichtlinie [1997] Art. 18 Anm. 3.1.). Dazu kommt, dass bei einer Verwendung samt Übermittlung oder Überlassung von Gesundheitsdaten im weiten Rahmen von ELGA eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Person nicht generell als unwahrscheinlich angesehen werden kann.

Ebenso scheint die (allgemein gehaltene) Bezugnahme in den Erläuterungen auf Art. 18 Abs. 3 DS-RL unzutreffend, da die Verarbeitung der Gesundheitsdaten in ELGA nicht bloß zum Zweck des Führens eines Registers, das zur Information der Öffentlichkeit bestimmt ist, vorgenommen wird. Denn unter solchen Registern zur Information der Öffentlichkeit im Sinne des Art. 18 Abs. 3 werden etwa Berufsverzeichnisse, Handelsregister oder bibliografische Verzeichnisse verstanden (vgl. *Dammann/Simitis*, EG-Datenschutzrichtlinie [1997] Art. 18 Anm. 3.3.).

Denkbar wäre aus Sicht der Datenschutzkommission die Verwendung von Ausfüllmustern oder allenfalls die Schaffung von Musteranwendungen.

Abs. 6 wäre daher ersatzlos zu streichen.

Zu den §§ 15 und 16:

Aus § 15 Abs. 1 geht hervor, dass eine Teilnahme an ELGA immer dann stattfindet, wenn kein Widerspruch der Betroffenen vorliegt. Grundsätzlich ist anzumerken, dass aus Datenschutzsicht stets eine „Opt-In-Lösung“, also die Erteilung einer Zustimmung vor der Verarbeitung von Daten, als eingriffsschonendste Variante anzusehen ist. Entscheidet man sich dennoch wie im Entwurf für eine „Opt-Out-Lösung“, sind zum Ausgleich für den damit einhergehenden Verlust an „informationeller Selbstbestimmung“ Maßnahmen zu treffen, insbesondere in sensiblen Bereichen.

In diesem Zusammenhang ist auf die Ausführungen der Art. 29-Datenschutzgruppe im Arbeitspapier „Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“, WP 131, hinzuweisen. Demnach muss der Patient entsprechend informiert werden, damit

eine „Opt-Out-Lösung“ wirklich eine angemessene Garantie darstellen kann. Der Patient muss im Vorfeld wissen, wer, wann und warum auf seine Daten zugreifen will und welche Folgen eine Zugangsverweigerung haben könnte.

Ausgehend von der Annahme, dass niemand gezwungen werden kann, sich an einem System mit elektronischen Patientenakten zu beteiligen, müssen nach Ansicht der Art. 29-Datenschutzgruppe die Rechtsvorschriften über die Einführung eines solchen Systems auch die Möglichkeit eines kompletten Ausstiegs aus dem System in Betracht ziehen, wobei den „aussteigenden“ Patienten keine Nachteile erwachsen dürfen. Es sollte daher im Sinne der Patientenautonomie und des Selbstbestimmungsrechtes dem Patienten die Möglichkeit offen stehen, auch alle seine bereits in ELGA vorhandenen Daten nachhaltig löschen zu können. Aus § 15 Abs. 4 geht hervor, dass nach einem Widerspruch nur die vorhandenen elektronischen Verweise auf ELGA-Gesundheitsdaten zu löschen sind, die ELGA-Gesundheitsdaten des Betroffenen aber offenbar nicht nachhaltig gelöscht werden, sondern für den Fall des Widerrufs des Widerspruches „im Hintergrund“ weiterhin bereitgehalten werden. Dies entspricht jedenfalls nicht dem im DSG 2000 und in der DS-RL geregelten Widerspruchsrecht, da Letzteres eine Löschung der Daten (und nicht bloß ein Ausblenden von Verweisen zu diesen Daten) zur Folge hat. Demgegenüber sieht § 15 Abs. 5 vor, dass bei bestehendem Widerspruch ELGA-Gesundheitdaten *nicht verwendet* werden dürfen. Da das „Speichern“ von Daten auch unter den Begriff „Verwenden“ fällt, würde dies bedeuten, dass die ELGA-Daten auch nicht mehr gespeichert und tatsächlich gelöscht werden müssen. Es wäre daher zu klären, wann nur durch ein „Ausblenden der Verweise“ vorzugehen ist und wann eine Löschung der ELGA-Gesundheitsdaten erfolgt.

Überdies wäre zu gewährleisten, dass aufgrund der Teilnahme mit „Opt-Out-Lösung“ besonders auch auf die Möglichkeiten des Widerspruchs im Einzelfall in einfacher und verständlicher Art und Weise hingewiesen wird. § 16 Abs. 5 sieht eine Information in Form eines Aushanges vor; dennoch scheint es zweifelhaft, dass diese generelle Information in jedem Fall ausreicht und von allen gelesen wird; es fragt sich auch, wie eine Information des Betroffenen stattfinden soll, falls in seiner Abwesenheit eine Eintragung oder Abfrage erfolgen soll. Bei einem durchgängigen Widerspruchsrecht müsste auch in derartigen Fällen eine Möglichkeit eines Widerspruchs der Patient/inn/en gewährleistet sein, was eine vorherige Information über die geplante Eintragung oder Abfrage voraussetzt. Es bleibt unklar, wie dies in der Praxis gewährleistet werden soll. § 16 sollte klar verständlich und abschließend darlegen, an wen der Teilnehmer in welchen Fällen den Widerspruch richten kann. Dabei sollte berücksichtigt werden, dass regelmäßig ältere Teilnehmer das Internet und damit möglicherweise auch das Zugangsportal nicht nutzen können. Daher sollten alternative Möglichkeiten des Widerspruchs – vor allem etwa die Abgabe einer postalischen Erklärung oder einer Erklärung gegenüber dem behandelnden Arzt – möglich sein.

Dementsprechend sollten auch alternative Möglichkeiten im Hinblick auf die Einsichtnahme des Patienten in seine eigenen Daten gemäß § 16 Abs. 1 Z 1 lit. a geschaffen werden. Auch dies sollte für Personen ohne Computerkenntnisse möglich sein.

Zu den §§ 15 und 16 wird im Zusammenhang mit dem Widerspruch gegen die Verwendung der Daten in der E-Medikationsdatenbank angemerkt, dass die E-Medikation bzw. die zugehörigen E-Medikationsdatenbanken im gesamten Entwurf nur unzureichend geregelt sind bzw. Zweck und Funktion der E-Medikation überhaupt fehlen. Diesbezüglich sollten verständliche und detaillierte Regelungen zur E-Medikation (konkrete Ausgestaltung als Informationsverbundsystem/e) in den Entwurf aufgenommen werden.

In § 16 Abs. 2 wird normiert, dass Personen, die ihr generelles Widerspruchsrecht wahrnehmen, weder im Zugang zur medizinischen Versorgung noch hinsichtlich der Kostentragung für diese schlechter gestellt werden dürfen als Personen, die diese Rechte nicht ausüben. Diesbezüglich fragt sich, wie dieses Recht in der Praxis tatsächlich gewährleistet werden kann. Jedenfalls wäre eine diesbezügliche Strafbestimmung im Gesetz vorzusehen, mittels derer eine Benachteiligung der betroffenen Personen geahndet werden kann. Dies gilt auch für allfällige Benachteiligungen wegen eines Widerspruchs im Einzelfall.

Die Erläuterungen gehen davon aus, dass das in § 16 verankerte Einsichtsrecht dem Auskunftsrecht nach § 26 DSG 2000 vorgeht. Die unionsrechtlichen Vorgaben des Art. 12 lit. a DS-RL müssen dem Betroffenen aber auch im ELGA-System zuerkannt werden. Auch schreibt Art. 12 DS-RL vor, dass das Auskunftsrecht gegenüber dem für die Verarbeitung Verantwortlichen (in österreichischer Diktion also gegenüber dem Auftraggeber) einzuräumen ist. Ein vom Auftraggeber losgelöstes Einsichtsrecht könnte daher wohl nur zusätzlich zum Auskunftsrecht nach § 26 DSG 2000 eingeräumt werden und dürfte im Hinblick auf die abschließende Regelung des Art. 12 lit. a DS-RL keinen datenschutzrechtlichen Charakter haben. Die oben genannten Ausführungen in den Erläuterungen wären daher in die Richtung zu ändern, dass das hier vorgesehene Einsichtsrecht als „geeignete Garantie“ zusätzlich zum Auskunftsrecht hinzutritt.

Für ältere Personen, die möglicherweise keinen Zugang zum Internet besitzen, sollte überdies auch hier eine alternative Möglichkeit (z.B. Zugriff beim behandelnden Arzt oder Apotheker) geschaffen werden.

In § 16 Abs. 4 sollte normiert werden, dass die Mitarbeiter/innen der Ombudsstelle zur Verschwiegenheit verpflichtet sind.

Im Zusammenhang mit der automatischen Teilnahme an ELGA und dem Widerspruch sowie der nachträglichen Aufnahme von elektronischen Gesundheitsdaten gemäß § 15 Abs. 5, die in Zeiten eines gültigen Widerspruchs angefallen sind, ist auch anzumerken, dass aus dem

Entwurf nicht klar hervorgeht, ob und gegebenenfalls welche „Altdaten“ (d.h. Daten, die schon vor der Einführung von ELGA vorhanden waren) von Patienten vorweg in ELGA übernommen werden sollen und wie in einem solchen Fall die Richtigkeit der vorhandenen „Altdaten“ überprüft werden soll bzw. wie eine Richtigstellung durch den Patienten erfolgen kann. Bei einer Übernahme von „Altdaten“ müsste vom zeitlichen Ablauf her auch angedacht werden, dass die betroffenen Personen von ihrem Widerspruchsrecht vor der Aufnahme ihrer Daten in ELGA informiert werden und erst nach Verstreichen einer konkret festzulegenden Zeitspanne (z.B. vier Wochen) für den Fall, dass kein Widerspruch erfolgt, mit der Aufnahme der Daten der betroffenen Personen in ELGA begonnen wird, damit das Selbstbestimmungsrecht gewahrt bleibt.

In diesem Zusammenhang wird auch auf die Anmerkungen zu § 1 Abs. 3 hinsichtlich der Frage der Aufnahme von Befunden von nicht an ELGA teilnehmenden GDA hingewiesen.

Zu § 17:

Im Hinblick auf die Identifikation von Teilnehmern sollte in § 17 Abs. 2 Z 4 verständlich dargelegt werden, was unter der „lokalen Patient/innenkennung“ zu verstehen ist.

Grundsätzlich wäre zu hinterfragen, inwieweit die Verwendung des „bPK-GH“ tatsächlich ein ausreichendes Instrument darstellt, um unzulässige Verknüpfungen von Datenbanken und/oder ELGA-Daten und eine Rückführbarkeit auf den Betroffenen zu verhindern. Daher stellt sich die Frage nach der Verwendung von mehreren Sub-bPK im Gesundheitsbereich.

Unklar bleibt auch, wie der Patientenindex befüllt werden soll bzw. aus welchen Quellen die Daten übermittelt werden. § 17 Abs. 3 nimmt hierbei ua. auf § 31 Abs. 4 Z 3 lit. a ASVG, der die Errichtung und Führung einer zentralen Anlage zur Aufbewahrung und Verarbeitung der für die Versicherung bzw. den Leistungsbezug und das Pflegegeld bedeutsamen Daten regelt, Bezug. Nicht geregelt wird aber, *wer* konkret *von wem* welche Daten ermittelt und in der Folge verarbeitet. Offen lässt diese Regelung auch, *welcher* der ELGA-Systempartner den Patientenindex nach § 17 Abs. 1 einzurichten und zu betreiben hat.

Es sollte diesbezüglich unmittelbar in § 17 Abs. 3 eine klare Regelung geschaffen werden. Relevant erscheint diesbezüglich insbesondere, dass aus dem Entwurf klar und verständlich erkennbar ist, *welchen Institutionen welche Aufgaben* der Datenverwendung zukommen. Insbesondere im Hinblick auf die Rechte des Betroffenen (§§ 26 bis 28 DSG 2000) sollte auch ein einheitlicher Ansprechpartner im Entwurf angegeben werden.

Zu § 18:

Die in § 18 Abs. 2 vorgesehenen „organisatorischen“ Regelungen sollten bereits im Gesetz festgelegt werden.

Zu § 19:

Die Art. 29-Datenschutzgruppe nimmt in ihrem Arbeitspapier ausdrücklich auf das Selbstbestimmungsrecht Bezug: Da die verschiedenen Arten von Krankendaten unterschiedlich schwerwiegende Konsequenzen haben können, sollte zwischen verschiedenen Verwendungsmöglichkeiten mit abgestuften Arten der Ausübung des Selbstbestimmungsrechts unterschieden werden: So sollten die Rechtsvorschriften über die Einführung des Systems für die Eingabe von Daten in eine elektronische Patientenakte oder den Zugang zu diesen Daten ein graduelles System vorsehen, das zum Teil die Einwilligung („Opt-In-Verfahren"), vor allem wenn es um die Verarbeitung von Daten mit besonders schwerwiegenden potenziellen Folgen geht, und bei weniger kompromittierenden Daten die ausdrückliche Ablehnung („Opt-Out-Verfahren") vorschreibt.

Das nunmehr in § 19 Abs. 3 vorgesehene „Opt-in" für bestimmte besonders sensible Gesundheitsdaten wird in diesem Sinne zwar begrüßt, jedoch scheint der Katalog der dort genannten Datenarten willkürlich gewählt und nicht vollständig, da z. B. Hepatitis-Erkrankungen u.Ä. für die Patient/inn/en ebenso von besonderer Sensibilität sein können.

Gemäß § 19 Abs. 5 sind die elektronischen Verweise grundsätzlich nach 36 Monaten zu löschen. Dies würde bedeuten, dass die ELGA-Inhalte weiterhin unbegrenzt gespeichert werden könnten. Dies wird ausdrücklich abgelehnt.

Grundsätzlich fragt es sich, wieso eine dezentrale Speicherung bei Medikationsdaten nicht möglich sein soll.

Im Zusammenhang mit der dezentralen Speicherung sollten auch die entsprechende Funktionsweise und die notwendige Datensicherheitsmaßnahmen geregelt werden. Insbesondere fragt sich, ob aufgrund der dezentralen Speicherung die entsprechenden technischen Systeme der ELGA-GDA ständig online sein müssen.

Zu den in § 19 Abs 9 Z 3 genannten bPK-GH siehe die Anmerkungen zu § 17.

Unklar ist, was unter dem in § 19 Abs. 9 Z 3 lit. d genannten „Hinweis auf allenfalls frühere ELGA-Gesundheitsdaten" gemeint sein soll. Die Erläuterung, dass durch diesen Hinweis eine „Versionierung" von ELGA-Gesundheitsdaten erlaubt werden soll, schafft keine abschließende Klarheit; auch ist dies aus dem Wortlaut nicht erschließbar.

Zu § 20:

Hinsichtlich der Ausgestaltung des Berechtigungssystems ist wiederum auf das Arbeitspapier WP 131 der Art. 29 Datenschutzgruppe zu verweisen, wonach der Datenschutz durch modulare Zugangsrechte erhöht werden könnte, d.h. die medizinischen Daten in einer elektronischen Patientenakte in bestimmte Kategorien eingeteilt werden, auf

die jeweils nur bestimmte medizinische Fachkräfte/Einrichtungen zugreifen dürfen (vgl. die Ausführungen zu § 3).

Da sich aus dem Berechtigungssystem ergibt, wer auf welche Daten Zugriff hat, wären die Eckpunkte dieses Systems im Gesetz selbst zu verankern. Offen bleibt auch, in welcher Form die generellen Zugriffsberechtigungen eingerichtet werden sollen.

In § 20 Abs. 3 wird ausgeführt, dass die ELGA-Systempartner Dienstleister sind. Es fragt sich in diesem Zusammenhang, welche konkrete Stelle hier als Dienstleister fungiert. Das Verhältnis zwischen „generellen" und „individuellen" Zugriffsberechtigungen bleibt im Übrigen unklar, insbesondere auch im Hinblick auf die Rechtsform, mit der die Berechtigungen eingeräumt werden sollen.

Zum 5. Abschnitt „Schlussbestimmungen" - §§ 24 bis 29:

Zu § 24:

Es scheint zweifelhaft, ob die Androhung der in § 24 Abs. 2 angeführten Geldstrafe im Sinne einer wirksamen Prävention ausreichend ist. Darüber hinaus sollte für die rechtswidrige Verwendung von den in § 19 Abs. 3 genannten Gesundheitsdaten, die potenziell schwerwiegende Folgen für die/den Patientin/en nach sich ziehen kann, aber auch für die speziellen Gruppen nach § 14 Abs. 4 (etwa Arbeitgeber, Versicherungen etc) eine besonders abschreckende Strafandrohung gesetzt werden.

Das faktische Benachteiligen von Patient/inn/en, die einen generellen oder einzelnen Widerspruch abgegeben haben oder die Verweise für den einzelnen GDA ausgeblendet haben, sollte ebenfalls unter (empfindliche) Strafe gestellt werden.

Zu § 26:

a.) Eine Ausnahme von den Datensicherheitsmaßnahmen sieht § 3 Abs. 1 iVm § 26 des Entwurfes vor. Aufgrund dieser Bestimmung können sensible Daten va. auch per Fax oder Telefon oder im persönlichen Weg übermittelt werden. Durch diese „Übergangsbestimmungen" wird das vom GTelG grundsätzlich vorgegebene Datensicherheitsniveau unterlaufen. Dies widerspricht den Vorgaben des Art. 8 Abs. 4 der DS-RL, wonach „die Mitgliedstaaten vorbehaltlich angemessener Garantien aus Gründen eines wichtigen öffentlichen Interesses entweder im Wege einer nationalen Rechtsvorschrift oder im Wege einer Entscheidung der Kontrollstelle andere als die in Absatz 2 genannten Ausnahmen vorsehen" können.

Auch die Art. 29-Datenschutzgruppe merkt in ihrem Arbeitspapier zur „Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)" an, dass der ordnungspolitische Rahmen zum Zwecke des Datenschutzes besondere Maßnahmen vorsehen muss, und führt

insbesondere die Entwicklung eines zuverlässigen, effektiven elektronischen Identifizierungs- und Authentisierungssystems, die Verhinderung des Zugriffs auf Daten oder der Änderung der Daten durch unberechtigte Personen und die klare Abgrenzung der Funktionen und Befugnisse der Personen, die für das System verantwortlich sind oder zumindest daran mitwirken, an.

Die von § 26 vorgesehenen Übermittlungsarten reichen aber nicht aus, um die von § 1 Abs. 2 DSG 2000 geforderten angemessenen Garantien und die von der Art. 29-Datenschutzgruppe geforderten Datensicherheitsmaßnahmen zu erfüllen. Überdies wird von § 26 auch offen gelassen, in welchen konkret umschriebenen Fällen die Anschaffung und Einrichtung entsprechender technischer Infrastruktur nicht zumutbar sei.

Überdies wird angemerkt, dass es der „Übergangsbestimmung" des § 26 – mit Ausnahme der Anwendung auf die Rettungsdienste – an einem im Vorhinein fixierten Zeitpunkt, ab welchem die Übergangsbestimmungen nicht mehr gelten sollen, mangelt. In § 26 Abs. 5 sollte daher der zeitliche Geltungsrahmen der Übergangsbestimmungen – statt in einer noch zu erlassenden Verordnung – bereits exakt im Gesetz festgelegt werden.

Ausnahmen von Datensicherheitsmaßnahmen sollten einerseits – soweit sie erforderlich und verhältnismäßig sind – daher nur als Übergangsbestimmungen in einem zeitlich äußerst eng begrenzten Rahmen und andererseits darüber hinaus nur für konkret im Gesetz zu definierende Ausnahmefälle, wie etwa bei einem Systemausfall oder bei akuten Gesundheitsbedrohungen, zulässig sein. Diese Ausnahmefälle sollten im Sinne der Klarheit und Verständlichkeit systematisch im Gesetz im Rahmen der Datensicherheitsmaßnahmen – und nicht bei den Schluss- und In-Kraft-Tretens-Bestimmungen – geregelt werden.

b.) Zu § 26 Abs. 2 ist anzumerken, dass unklar ist, was unter der „erstmaligen" Weitergabe von Gesundheitsdaten zu verstehen ist, zumal nach § 7 Abs. 2 DSG 2000 Daten insb. nur übermittelt werden dürfen, wenn 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. Im Rahmen der Vorgaben des § 7 DSG 2000 muss daher grundsätzlich bei jeder Übermittlung von Daten die Identität und Berechtigung des Empfängers überprüft werden.

II. Zu Art. 2 (Änderung des Allgemeinen Sozialversicherungsgesetzes), Art. 3 (Änderung des Gewerblichen Sozialversicherungsgesetzes), Art. 4 (Änderung des Bauern-Sozialversicherungsgesetzes) und Art. 5 (Änderung des Beamten-Kranken- und Unfallversicherungsgesetzes)

Die Art. 2 bis 5 regeln jeweils die Information an den Versicherten und ihre Angehörigen.

In diesem Zusammenhang wird darauf hingewiesen, dass die hier vorgesehene Information nicht ident ist mit der in Art. 11 DS-RL vorgesehenen Information. Die hier vorgesehene allgemeine Information kann die Information im Einzelfall (siehe dazu auch § 24 DSG 2000) nicht ersetzen, sondern nur ergänzen.

Weiters sollte die Information durch die Sozialversicherungen im Fall von ELGA verständlich über sämtliche Möglichkeiten und Risiken (z.B. konkrete Aufklärung darüber, unter welchen Bedingungen welche Daten von wem in ELGA verwendet werden dürfen, und weiters über die Folgen des „Opt-Out“ aus dem System) aufklären.

Nachdem die Informationen nach den Art. 2 bis 5 jeweils nur an Versicherte und ihre Angehörigen ergehen, sollten auch Bestimmungen geschaffen werden, die die Information an jene Personen, die nicht versichert sind, aber bei ELGA teilnehmen, regeln.

III. Zu Art. 8 (Änderung des Hebammengesetzes)

Der Sinn der Bestimmung des § 40 Abs. 4 scheint nicht nachvollziehbar: Da das Österreichische Hebammengremium ein Auftraggeber des öffentlichen Bereichs ist, gilt ohnehin § 8 Abs. 3 Z 1 DSG 2000 und wäre die vorgeschlagene Bestimmung redundant bzw. aufgrund der abweichenden Diktion sogar verwirrend. Sie wäre daher ersatzlos zu streichen.

VI. Zu Art. 10 (Änderung des Strafgesetzbuches)

Zu Z 1 (§§ 118b und 118c):

Der Tatbestand des § 118b stellt zwar das Verlangen unter Strafe, dies jedoch nur dann, wenn dem Verlangen dadurch Nachdruck verliehen wird, dass im Falle der Weigerung beabsichtigt ist, für die sich weigernde Person ein schädliches Verhalten zu setzen. Diese Formulierung erscheint unklar. Der Druck auf die/den Patient/in/en zur Zugänglichmachung ihrer/seiner ELGA-Gesundheitsdaten muss nicht immer mit einem Hinweis auf das drohende schädliche Verhalten einhergehen, sondern kann sich auch schon aus den Umständen des Verlangens heraus (z.B. Verlangen von ELGA-Daten beim Abschluss einer Lebensversicherung) ergeben. Auch erscheint der Beweis, dass beabsichtigt wurde, ein schädlichen Verhaltens für den Fall der Weigerung zu setzen – was offensichtlich dem „Weigernden“ auch vermittelt werden muss – in vielen Fällen nur schwer zu erbringen. Ein derartiger Zwang kann sich auch schlüssig ergeben.

Aus diesem Grund sollte bereits das bloße widerrechtliche Verlangen von ELGA-Daten von bestimmten konkreten Personengruppen in bestimmten Situationen unter Strafe gestellt werden.

Darüber hinaus wird angemerkt, dass eine angedrohte Freiheitsstrafe nach Abs. 1 von sechs Monaten vor allem im Hinblick auf die Generalprävention als zu gering erscheint.

Hinsichtlich des angedrohten Strafausmaßes in § 118c wird auf die Ausführungen zu § 118b verwiesen.

Diese Erledigung ergeht auch an das Präsidium des Nationalrates.

11. März 2011
Für die Datenschutzkommission
Der stellvertretende Vorsitzende:
Hofrat des OGH Hon.Prof. Dr. KURAS

Signaturwert	Vforv4TyNc4r/q9magx+A9yblg6eGcKinK8jjscxFaKuVxwacO8tgkeV0oP7ERgNwbH 52iGhD8C/czxDhlgeyPERBCG6sRaFDJY9jfffCMP9alzoaf7ranSrnGc1yIfkSfdVKn sgHJjiwL+rQi2JxCWN1eVbrOtaODd5zWNFR4kamkVEeUxUq/o6Yg2JQBWszsrxkARJs y5YUKJRb4YTGwX4mXvE82KyCOqO3doFDKZglk8JcxFDlnymQ/0ql+0y11C4HZ+nbHQH si6YkMkemQu9bylVqfpGwKyEVfWdYcIUUXEvb+NT5hMcB7adLLx3f937qR0XddSCbDW v+DRpZg==	
	Unterzeichner	serialNumber=117229306313,CN=Amtssignatur Datenschutzkommission,O=Amtssignatur Datenschutzkommission,C=AT
	Datum/Zeit-UTC	2011-03-17T08:56:09+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	543759
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bka.gv.at/verifizierung	