REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.301/0002-DSR/2011
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für
Gesundheit
Per Mail:
Clemens.Auer@bmg.gv.at
Carina.milisits@bmg.gv.at

Betrifft: Bundesgesetz, 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 Heilmasseuresetz und das Strafgesetzbuch, geändert werden

(Elektronische Gesundheitsakte-Gesetz – ELGA-G)
Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner 206. Sitzung am 28. März 2011 **einstimmig beschlossen**, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

Allgemeine Vorbemerkungen:

Der **Österreichische Datenschutzrat** berät als unabhängiges Beratungsorgan die Bundesregierung in rechtspolitischen Fragen des Datenschutzes. Zur Erfüllung dieser Aufgabe ist dem Datenschutzrat Gelegenheit zur Stellungnahme zu Gesetzesentwürfen der Bundesministerien zu geben, soweit diese datenschutzrechtlich von Bedeutung sind. In diesem Sinne nimmt der Datenschutzrat, im Rahmen der Begutachtung zum Elektronischen Gesundheitsakte-Gesetz, Stellung.

Keinesfalls obliegt es dem Datenschutzrat, eine Beurteilung von ELGA hinsichtlich des allgemeinen Nutzens für das Gesundheitswesen, sowie des Nutzen für die Patienten und von Haftungsfragen, wie auch der Finanzierung vorzunehmen. Dies obliegt der allgemeinen politischen Diskussion, im Zuge dieses Begutachtungsverfahrens.

2) Datenschutzrechtlich relevante Bestimmungen:

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

1.) Vorbemerkungen:

a.) Maßgebliche rechtliche Determinanten

Nach § 1 Abs. 2 DSG 2000 sind, soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, 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.

Bei Gesundheitsdaten handelt es sich um sensible Daten im Sinne des § 4 Z 2 DSG 2000 und damit um besonders schutzwürdige Daten im Sinne des § 1 Abs. 2 DSG 2000.

Neben den nationalen Regelungen sind auch die unionsrechtlichen Vorgaben zu beachten: Nach **Art. 8 Abs. 1 der Datenschutz-Richtlinie 95/46/EG (in der Folge: DS-RL)** untersagen die Mitgliedstaaten die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von **Daten über Gesundheit** oder Sexualleben.

Abs. 2 leg. cit. zählt jene Fälle auf, in denen Abs. 1 leg. cit. keine Anwendung findet.

Der Abs. 1 leg. cit. gilt zudem nach Art. 8 Abs. 3 DS-RL dann nicht, wenn die Verarbeitung der Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal erfolgt, das nach dem einzelstaatlichen Recht, einschließlich der von den

zuständigen einzelstaatlichen Stellen erlassenen Regelungen, dem Berufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen.

Während im vorliegenden Gesetzesentwurf im Hinblick auf die unionsrechtliche Grundlage zutreffender Weise nur 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.

Es wird angeregt, die Erläuterungen dahingehend zu ändern, als nur auf Art. 8 Abs. 4 DS-RL Bezug genommen wird.

b.) Verständlichkeit der Regelungen

Rechtsvorschriften sollen leicht lesbar sein. Grundsätzlich soll sich die Formulierung von Rechtsvorschriften am allgemeinen Sprachgebrauch orientieren; wenn Begriffe in einer davon abweichenden Bedeutung oder wenn Fachbegriffe verwendet werden, so ist dies im Text der Rechtsvorschrift deutlich zu machen. Auf den Adressatenkreis der betreffenden Rechtsvorschrift ist ausdrücklich Bedacht zu nehmen. Dem Text einer Rechtsvorschrift müssen die Normadressaten der einzelnen Regelungen und das vorgeschriebene Verhalten zweifelsfrei zu entnehmen sein.

Der gegenständliche Entwurf ist hinsichtlich der Regelung von ELGA grundsätzlich mit einer „Opt-Out-Lösung“ insb. auch an die Patientinnen und Patienten als Normadressaten gerichtet und regelt dabei eine hochkomplexe sowie zum Teil auch hoch technik-lastige Fachmaterie. **Für die Betroffenen wird daher 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.**

Dazu kommt, dass für Patientinnen und Patienten als Teilnehmerinnen und Teilnehmer von ELGA maßgebliche Regelungen nur sehr kursorisch (z.B. Zweck und Funktion der e-Medikationsdatenbank) oder schwer verständlich (z.B. konkrete Funktionsweise von ELGA bzw. der zugehörigen Verweise) ausgestaltet sind bzw. gar nicht im Entwurf selbst abschließend geregelt werden, sondern einer späteren Verordnung vorbehalten sind, womit eine „Zersplitterung“ der Regelungsmaterie einhergeht und die Transparenz

und Verständlichkeit des Entwurfs für Patientinnen und Patienten weiter erschwert wird (z.B. Festlegung der Rollenverteilung in einer Verordnung).

Aus diesen Gründen hält es der Datenschutzrat daher für erforderlich, dass diese Materie entsprechend dem sensiblen Regelungsinhalt in höchst möglicher Verständlichkeit und sprachlicher Klarheit geregelt wird, damit auch der nicht einschlägig auf diesem Gebiet vorgebildete Normadressat die Möglichkeit hat, den Inhalt des Gesetzes und die damit verbundenen Folgen einigermaßen zu verstehen. Der Entwurf sollte daher vorweg unter diesem Gesichtspunkt nochmals geprüft und grundlegend überarbeitet werden.

c.) „Opt-Out-Lösung“ und Information der Betroffenen

Der Entwurf sieht in § 15 eine „Opt-Out-Lösung“ vor, bei der der Teilnehmer nur durch Widerspruch aus dem ELGA-System austreten kann.

Grundsätzlich merkt der Datenschutzrat an, dass aus datenschutzrechtlicher Sicht 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 – insbesondere in sensiblen Bereichen – besondere Maßnahmen zu treffen.

In diesem Zusammenhang ist auf die Ausführungen der Art. 29-Datenschutzgruppe im Arbeitspapier „Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“, WPA 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.

Essentiell scheint hier vor allem die **Gestaltung der Information**, die an alle potentiellen Teilnehmerinnen und Teilnehmer von ELGA ergehen müsste. Diese müsste verständlich und individuell – **am Besten vor der erstmaligen Behandlung und der Aufnahme personenbezogener Daten des Betroffenen in ELGA** – erfolgen und 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 „Opting-Out“ aus dem System) aufklären.

Die Regelungen der Informationen an die Versicherten und Angehörigen in den § 15 Abs. 2 bis 5 erscheint weiters insofern nicht ausreichend, als auch nicht versicherte Personen einen Anspruch auf eine verständliche Information haben (und mangels einer entsprechenden Bestimmung im Abs. 1 nicht erfasst wären) und die in diesen Bestimmungen bezeichnete Information nicht vor der Inbetriebnahme von ELGA versendet werden. Weder das „Recht“ auf Information durch den ELGA-Gesundheitsdiensteanbieter nach § 16 Abs. 1 Z 3 noch der Aushang gemäß § 16 Abs. 5 in den Räumlichkeiten des Gesundheitsdiensteanbieters kann eine verständliche und individuelle Information der/des Patientin/en im Wege eines persönlichen Anschreibens ersetzen.

Es sollte dementsprechend eine gesetzliche Regelung mit den grundlegenden Eckpunkten für die individuelle Information des (möglichen) Teilnehmers und der grundlegenden Funktionen von ELGA (vor allem hinsichtlich des Widerspruches) im GTelG 2011 geschaffen werden. Der genaue Text der Information könnte in der Folge auch mit Verordnung vorgesehen werden.

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. 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.

Der Patient muss nach Ansicht des Datenschutzrates die Möglichkeit haben, nicht bloß nur die Verweise auf seine ELGA-Daten, sondern auch die ELGA-Daten selbst löschen zu lassen.

Zudem ist zu bemerken, dass auf Grund der Teilnahme mit „Opt-Out-Lösung“ besonders auch auf die einzelnen **Möglichkeiten des Widerspruchs** in einfacher und verständlicher Art und Weise hingewiesen werden sollte. Der Betroffene sollte nachvollziehen können, welche Daten von wem nach einer erfolgten Ausblendung von Verweisen im Einzelfall eingesehen werden können.

Es sollte deutlicher und für den Normadressaten einfach verständlich im Entwurf formuliert werden, dass der Teilnehmer auch im Einzelfall der Aufnahme einzelner

oder bestimmter Gesundheitsdaten oder Behandlungen in ELGA widersprechen kann.

Die Bestimmung des § 16 Abs. 1 erscheint diesbezüglich nicht verständlich genug.

d.) Integriertes Sicherheitsmanagement

Der Datenschutzrat regt daher - aufgrund des sehr komplexen IT-Systemes bei ELGA – an, ein **integriertes Datensicherheitsmanagementsystem** einzuführen. Das gesamte ELGA-System müsste jedenfalls eine anerkannte, standardisierte sicherheitstechnische Zertifizierung aufweisen. **Weiters müsste gesetzlich zumindest eine den Datensicherheitsmaßnahmen gemäß § 14 DSG 2000 entsprechende Regelung im ELGA Gesetz aufgenommen werden.** 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. Die Verschlüsselungstechnik sollte nicht nur für den Transfer, sondern auch zur Speicherung der Daten im System verwendet werden. Jedenfalls müsste sichergestellt werden, dass eine Verschlüsselung der Kommunikation zwischen den GDAs erfolgt, um Unbefugte vom Zugriff auf Gesundheitsdaten von Patienten sicher ausschließen zu können.

e.) Teilnahme von dauerhaft psychisch beeinträchtigten Personen und Minderjährigen

Im Hinblick auf dauerhaft psychisch beeinträchtigte Personen (z.B. Demenzkranke) sollte ein System überlegt werden, welches sicherstellt, dass rechtliche Instrumentarien (insb. Sachwalterschaft) greifen, die die Selbstbestimmung des Patienten angemessen substituieren. Gerade Gesundheitsdiensteanbieter kommen regelmäßig mit derart beeinträchtigten Personen in Kontakt und sind wohl vielfach auch jene Stellen, wo solche Beeinträchtigungen erstmals festgestellt werden.

Die in § 19 Abs. 3 geregelte Aufnahme auf Verlangen erscheint gerade bei dieser Personengruppe problematisch, da es hierbei an der Einsichtsfähigkeit (und damit der Fähigkeit der Möglichkeit zur Zustimmung iSd DSG 2000) mangeln kann.

Der Datenschutzrat weist ausdrücklich darauf hin, dass im vorliegenden Entwurf die Teilnahme von Minderjährigen an ELGA nicht ausdrücklich geregelt ist, dabei geht es um die Frage, unter welchen Voraussetzungen Minderjährige von der „Optout“ Regelung gebrauch machen können, bzw. in welchen Fällen und unter welchen Voraussetzungen der gesetzliche Vertreter eine Entscheidung zu treffen hat (vgl. § 146c ABGB).

2.) Zum Gesetzesentwurf:

Zu § 1:

Das in Abs. 2 Z 2 genannte Ziel, „die für die Entwicklung und Steuerung der Gesundheitstelematik im internationalen Kontext notwendigen Informationsgrundlagen zu schaffen und zu verbreitern“, wird weder im Gesetzestext noch in den Erläuterungen näher ausgeführt. Es kann daher im Lichte des Grundrechtes auf Datenschutz nicht beurteilt werden, ob der Eingriff verhältnismäßig ist. **Es wird angeregt, zumindest in den Erläuterungen den Zweck dieser Bestimmung näher auszuführen.**

§ 1 Abs. 3 gilt nicht für Gesundheitsdiensteanbieter, die über keine Einrichtungen der Informations- und Kommunikationstechnologie verfügen. Diese GDAs nehmen somit nicht an ELGA teil. Daher sollte eine Lösung gefunden werden, in welcher Form Patienten ihre Gesundheitsdaten dieser nicht teilnehmenden GDA 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.

Auch ist der Nutzen von ELGA fraglich, wenn Patienten daran aufgrund der „Opt-Out-Regelung“ teilnehmen, jedoch für den Patienten unklar ist, ob sein konkreter Befund erfasst wird. Im Besonderen könnte dies Personen betreffen, die ihre ELGA-Daten nicht per Internetzugang überprüfen können (z.B. mangels Vorhandenseins eines Internetanschlusses oder mangels ausreichender Computerkenntnisse).

Zu § 2:

a.) Im Zusammenhang mit der „psychischen Befindlichkeit“ (Z 1, insbesondere der „geistigen Verfassung“ nach lit. a und den unter lit. c erfassten „gesundheitsrelevanten Lebensgewohnheiten oder Umwelteinflüssen“ scheint die Definition von ELGA-Gesund-

heitsdaten sehr weitgehend zu sein. Es wird angeregt, die Notwendigkeit dieser weiten Auslegung von ELGA Gesundheitsdaten nochmals zu überdenken und gegebenenfalls im Gesetz einzuschränken.

b.) Zur weit gefassten Definition des Begriffs des Gesundheitsdiensteanbieters in Z 2 wird angemerkt, dass definitionsgemäß jede Person als Gesundheitsdiensteanbieter in Betracht käme, die Gesundheitsdaten regelmäßig verwendet (etwa auch Rechtsanwälte oder Versicherungsunternehmen bei regelmäßiger Verwendung von Gesundheitsdaten). **Der Begriff des Gesundheitsdiensteanbieters sollte daher enger gefasst und auf den medizinischen Bereich eingeschränkt werden.**

c.) Im Hinblick auf die Definition von ELGA in Z 6 und der ELGA-Systempartner in Z 11 sollte ausdrücklich festgelegt werden, ob es sich bei ELGA um **ein** Informationsverbundsystem (§ 4 Z 13 DSG 2000) bzw. um **mehrere** Informationsverbundsysteme handelt.

Sollen – wie im vorlegenden Fall – durch Gesetz Informationsverbundsysteme im Sinne von § 4 Z 13 DSG 2000 geschaffen werden, wäre im Gesetz insbesondere die **Rollenverteilung zu regeln** (wer ist Auftraggeber, wer ist Dienstleister, wer ist Betreiber des Systems). Aus diesem Grund wären daher auch die ELGA-Gesundheitsdiensteanbieter, wenn sie Auftraggeber eines Informationsverbundes werden sollten, möglichst abschließend im Gesetz aufzuzählen.

d.) Es fragt sich, wieso der in § 2 Z 10 lit. e genannte National Contact Point (NCP) ein GDA und damit auch Auftraggeber im ELGA-System sein soll. Es sollte geprüft werden, ob der NCP nicht vielmehr eine Dienstleisterfunktion einnimmt. Unklar erscheint auch, welche konkreten „Auflagen“ der NCP nach lit. dd erfüllen muss.

e.) Bei dem in Z 13 definierten „Verweisregister“ sollte im Gesetz klargestellt werden, dass es sich hierbei um ein Informationsverbundsystem handelt und überdies geregelt werden, wer in diesem Fall „Betreiber“ bzw. allenfalls Dienstleister ist. Aufgrund der engen 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 diese Bestimmung – gemäß den Ausführungen in den Erläuterungen – eine lex specialis zu den im DSG 2000 geregelten „Informationsverbundsystemen“ darstellen soll.

Für den Normadressaten muss verständlich sein, welchen Zweck das „Verweisregister“ hat und wie es funktioniert, da er ansonsten seine individuellen Zugriffsberechtigungen nicht sinnvoll verwalten kann. Diesbezüglich sollte die Funktion der Verweise und des Verweisregisters in verständlicher Form dargestellt werden.

Zu § 3 :

a.) 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.

b.) Die Art. 29-Datenschutzgruppe weist im Arbeitspapier „Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“, WPA 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. Weiters müssen Routinen für eine zweifelsfreie Identifizierung und Authentifizierung eingerichtet werden. Um die mit der Authentifizierung mittels Kennwort verbundenen Risiken zu umgehen, sollte zumindest längerfristig die Authentifizierung mit Hilfe der elektronischen Signatur angestrebt werden, die den Nutzern zusammen mit einer ordentlichen amtlichen Kennung – bspw. auf besonderen Chipkarten – zugeteilt wird. Für medizinisches Personal muss ein Erkennungs- und Authentisierungssystem entwickelt werden, bei dem eine medizinische Fachkraft nicht nur ihre Identität nachweisen muss, sondern auch die Funktion, in der sie elektronisch tätig wird (z.B. als Psychiater oder Krankenschwester). Für den Zugang zu einer elektronischen Patientenakte muss daher der Grundsatz gelten, dass – abgesehen vom Patienten selbst – nur jene medizinischen Fachkräfte oder Mitarbeiter von Gesundheitseinrichtungen zugangsberechtigt sein dürfen, die an der Behandlung des Patienten mitwirken. Es muss somit eine akute Behandlungssituation zwischen dem Patienten und der medizinischen Fachkraft vorliegen, die auf die Daten zugreifen möchte. Der Schutz von Gesundheitsdaten könnte außerdem durch modulare Zugangsrechte erhöht werden, d.h. die medizinischen Daten in einer elektronischen Patientenakte in bestimmte Kategorien eingeteilt werden, auf die jeweils nur bestimmte medizinische Fachkräfte/Einrichtungen zugreifen dürfen.

Die Art. 29-Datenschutzgruppe ist zudem der Ansicht, dass der Zugang zu medizinischen Daten in einer elektronischen Patientenakte für andere als die in Art. 8 Abs. 3 Datenschutz-Richtlinie 95/46/EG genannten Zwecke 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. Außerdem sollten die Verhaltensregeln für medizinische Fachkräfte so beschaffen sein, dass Zuwiderhandlungen wirksam bekämpft werden.

Entsprechend diesen Grundsätzen der Art. 29-Datenschutzgruppe erscheint es aus datenschutzrechtlicher Sicht geboten, entsprechende Regelungen und Maßnahmen unmittelbar im ELGA-G vorzusehen, die einen Zugriff und eine Einschau von unbefugten Dritten in ELGA-Daten bzw. eine Verwendung dieser Informationen ausdrücklich verbietet (ausdrückliches Verwendungsverbot). Vor allem dürfen Patienten auch nicht unter Druck dazu veranlasst werden, ihre Daten offenzulegen, z.B. auf Aufforderung eines möglichen künftigen Arbeitgebers oder einer Versicherungsgesellschaft. Arbeitgeber, Behörden und Versicherungen dürfen keinen Zugang zu ELGA-Gesundheitsdaten bekommen.

In diesem Zusammenhang ist auch auf die Definition der Zustimmung in § 4 Z 14 DSG 2000 hinzuweisen, wonach eine Zustimmung die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen ist, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt. Weiters sind die Vorgaben des § 9 Z 6 DSG 2000 hinsichtlich der Zustimmung zu beachten, wonach der Betroffene seine Zustimmung zur Verwendung sensibler Daten ausdrücklich erteilen muss, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt.

Angesichts der strengen Vorgaben des DSG 2000 ist insbesondere bei Abschluss von Versicherungsverträgen und im Zuge des Bewerbungsverfahrens fraglich, ob hier jemals zweifelsfrei davon ausgegangen werden kann, dass der Antragsteller bzw. Bewerber seine Gesundheitsdaten tatsächlich ohne Zwang übermittelt (bzw. zugänglich macht), wenn er andernfalls damit rechnen muss, dass er benachteiligt wird (so etwa wegen Verweigerung der Versicherung hinsichtlich des Abschlusses einer Lebensversicherung oder Nichtaufnahme in ein Arbeitsverhältnis). Auch ist anzumerken, dass eine Zwangssituation oftmals nur schwierig nachzuweisen sein wird, da diese auch von

subjektiven Erwartungshaltungen und Annahmen des Antragstellers bzw. Bewerbers abhängen kann.

In diesem Zusammenhang wird auch auf § 67 des Gentechnikgesetzes – GTG, BGBl. Nr. 510/1994, verwiesen, der Arbeitgebern und Versicherern einschließlich deren Beauftragten und Mitarbeitern ausdrücklich verbietet, Ergebnisse von genetischen Analysen von ihren Arbeitnehmern, Arbeitsuchenden oder Versicherungsnehmern oder Versicherungswerbern zu erheben, zu verlangen, anzunehmen oder sonst zu verwerten. Von diesem Verbot sind auch das Verlangen nach Abgabe und die Annahme von Körpersubstanz für genanalytische Zwecke umfasst.

c.) Zum **Zugriff** führt die Art. 29-Datenschutzgruppe weiters 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. Die Verschlüsselungstechnik sollte nicht nur für den Transfer, sondern auch zur Speicherung der Daten im System verwendet werden.

In Anbetracht 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 gemäß § 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, insbesondere müsste eine Datenweitergabe protokolliert werden. Nur aus den Erläuterungen – und nicht aus dem Gesetzeswortlaut – ergibt sich, dass es sich dabei um ein „Inhouse-Privileg“ handeln soll, wonach das GTelG 2011 nicht auf die

Weitergabe von elektronischen Gesundheitsdaten innerhalb eines Gesundheitsdiensteanbieters (z.B. Spital) anzuwenden ist.

Ausnahmen von Datensicherheitsmaßnahmen sollten – soweit sie erforderlich und verhältnismäßig sind – nur als Übergangsbestimmungen in einem zeitlich **äußerst eng begrenzten Rahmen** und darüber hinaus nur für konkret im Gesetz zu definierende **Ausnahmefälle**, wie etwa bei einem Systemausfall oder bei akuten Gesundheitsbedrohungen, zulässig sein.

§ 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.

Es sollte daher in § 3 Abs. 2 Z 1 klargestellt werden, dass diese Bestimmung nicht für die Verwendung von ELGA-Daten gilt.

Schließlich ist zu bedenken, dass es wohl immer Fälle 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 daher auch für diese Übermittlungsarten die jeweils entsprechend geeigneten Datensicherheitsmaßnahmen normiert werden. Derzeit sind solche nur lückenhaft in Gestalt der Übergangsbestimmungen des § 26 enthalten.

Zu § 4:

Fraglich 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 zugeschrieben werden.

Es wird daher vorgeschlagen, § 4 Abs. 2 Z 1 wie folgt zu formulieren: „1. durch Verwendung qualifizierter elektronischer Signaturen sowie bereichsspezifischer Personenkennzeichen (§ 9 E-GovG) oder“.

Unklar ist weiters, wie die Überprüfung der Identität von Gesundheitsdiensteanbietern durch Einsichtnahme in den eHealth-Verzeichnisdienst von statten gehen soll. Hier wäre eine detaillierte Regelung von Vorteil.

Zur Verwendung der bPK und den Verweis auf § 9 E-GovG wird weiters darauf hingewiesen, dass das System der bPK nur für natürliche Personen zur Anwendung kommen kann. Da Gesundheitsdiensteanbieter offensichtlich auch nicht natürliche Personen sein können, bestünden für diese somit zwei Varianten: Bei der qualifizierten elektronischen Signatur und dem bPK nach der vorgeschlagenen Z 1 müsste es sich um die Signatur und das bPK des Vertreters (samt der Stammzahl der vertretenen nicht natürlichen Person - vgl. dazu § 6 Abs. 3 E-GovG) handeln; andernfalls wäre die Variante der Z 2 zu wählen (Einsichtnahme in den eHVD).

Zu § 5:

Die in Abs. 2 vorgesehene Anpassung der Rollen sollte angesichts der von der jeweiligen Rolle abhängigen Möglichkeiten hinsichtlich der Verwendung von sensiblen Daten möglichst bereits im Gesetz festgelegt werden.

Zu § 6:

Es sollte dargelegt werden, welche Zugriffkontrollmechanismen im Sinne der Abs. 1 Z 2 als effektiv angesehen werden.
Zum Zugriff auf Daten führt die Art. 29-Datenschutzgruppe unter anderem 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 möglich, sollten daher datenschutzfreundliche Technologien (Privacy Enhancing Technologies) zum Einsatz kommen und es sollte eine weitestgehende Verschlüsselung angestrebt werden. Wobei eine Verschlüsselung in dem Ausmaß vorzunehmen ist, dass ein Personenbezug nicht mehr herstellbar ist.

Zu § 7:

Es wäre zu prüfen, 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:

Im Hinblick auf die Übermittlung der Dokumentation sollte dargelegt werden, ob diese Dokumentation auch personenbezogene Daten enthält. Zudem ist der Zweck der Übermittlung der Dokumentation an den Bundesminister für Gesundheit und der ELGA-Ombudsstelle nicht erkennbar. **Es sollte grundsätzlich eine lückenlose Protokollierung aller Zugriffe auf Gesundheitsdaten gesetzlich normiert werden.**

Zu § 9:

a.) Abs. 3 legt nicht fest, *wer* die in Z 1 aufgezählten Daten *an wen* übermitteln soll. Die Bestimmung sollte daher konkretisiert werden.

In § 9 Abs. 3 Z 3 sollte zudem ausgeführt werden, welche „übrigen" GDA in dieser Bestimmung gemeint sein könnten. Hier sollte eine taxative Aufzählung im Gesetz erfolgen.

b.) Die in Abs. 5 vorgesehenen, in Form einer Verordnung näher festzulegenden technischen Anforderungen sollten an den Stand der Technik gekoppelt werden. Die Verordnungsermächtigung erscheint im Lichte des Bestimmtheitsgebots des Art. 18 B-VG zudem als zu unbestimmt und sollte konkretisiert werden.

Zu § 10:

Unklar erscheint, was unter der „Staatszugehörigkeit des Gesundheitsdiensteanbieters" (Abs. 1 Z 7) zu verstehen ist. Die Staatsbürgerschaft (Art. 6 Abs. 1 B-VG) erscheint nicht als ein im Rahmen des eHealth-Verzeichnisdienstes relevantes Datum. Darüber hinaus wird es sich bei Gesundheitsdiensteanbietern häufig um juristische Personen handeln. Allenfalls scheint es sinnvoll, stattdessen auf den Niederlassungsort, bzw. die Behörde abzustellen, die die Berufsausübung genehmigt hat.

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

Zu § 11:

Aus der Bestimmung geht nicht hervor, ob die Berichte und Auskünfte allenfalls auch (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.

Zu § 13:

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 jeweilige ELGA-Teilnehmer Auftraggeber und die ELGA-Systempartner sind 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.

Abs. 4 wäre dahingehend klarer zu formulieren, dass die Register zwar bei Nichtvorliegen eines Widerspruches bereitgestellt werden dürfen, aber ein konkreter Zugriff auf diese Register durch GDA nur im Behandlungs- oder Pflegefall entsprechend den zugehörigen Rollen zulässig ist. Insofern scheinen sowohl die Formulierung des Abs. 4 als auch die diesbezüglichen Erläuterungen irreführend. Weiters ist in Abs. 4 nicht erkennbar, 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. Abs. 4 ist keine ausreichende Rechtsgrundlage zur konkreten Verwendung von Gesundheitsdaten aus Registern, insbesondere auch nicht für eine Verknüpfung derartiger Daten mit ELGA-Gesundheitsdaten.

In § 2 Z 1 lit. a wird als ELGA-Gesundheitsdatum auch die psychische Befindlichkeit von Personen und insbesondere auch deren „geistige Verfassung“ definiert. Entsprechend § 19 Abs. 3 des Entwurfes, dürfen aber genau diese Informationen nur auf Verlangen

von den ELGA Teilnehmer/innen gespeichert werden. Daher wäre eine Zugänglichmachung derartiger Informationen aus anderen Registern (wie z.B. etwa Register aus psychiatrischen Anstalten) für ELGA im Sinne des Grundrechts auf Datenschutz gemäß § 1 Abs. 2 DSG 2000 als unverhältnismäßig einzustufen. Es ist daher datenschutzrechtlich geboten, keine automatische Speicherung von Informationen über psychische Befindlichkeiten von Personen und insbesondere deren „geistige Verfassung“ in der elektronischen Gesundheitsakte vorzunehmen.

Zu Abs. 5 wird angemerkt, dass eine Übermittlung von Daten ins Ausland unabhängig von einer Behandlung oder Betreuung **ausschließlich mit Zustimmung des Betroffenen** hinsichtlich des konkreten Zwecks der Übermittlung zulässig sein kann. Diesbezüglich müsste vorrangig im Gesetz oder zumindest in den Erläuterungen festgelegt werden, welcher Zweck hier jeweils in Betracht kommt. Im Übrigen ist fraglich, ob der NCP ein GDA sein kann (siehe auch Anmerkungen 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:

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.

Die in § 14 Abs. 6 enthaltene Behauptung, dass die Meldepflicht nach § 17 DSG 2000 für Datenanwendungen auf Grund dieses Abschnitts mit diesem Bundesgesetz erfüllt sei, ist **unzutreffend und widerspricht überdies den einschlägigen Bestimmungen der Datenschutzrichtlinie 95/46/EG (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 keine Anwendung auf Verarbeitungen findet, deren einziger Zweck das Führen eines Register 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 des GTelG 2011 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 solche 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 erscheint die Bezugnahme in den Erläuterungen auf Art. 18 Abs. 3 DS-RL als 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 leg. cit. werden etwa Berufsverzeichnisse, Handelsregister oder bibliografische Verzeichnisse verstanden (vgl. *Dammann/Simitis*, EG-Datenschutzrichtlinie [1997] Art. 18 Anm. 3.3.).

Nachdem von Art. 18 DS-RL eine Meldung bei der Kontrollstelle verpflichtend vorgesehen ist und keine der in dieser Bestimmung aufgezählten Ausnahmen zur Anwendung kommt, kann eine Anwendung des § 17 DSG 2000 („Meldepflicht des Auftraggebers"), der die Meldepflicht auf nationaler Ebene regelt, richtlinienkonform nicht ausgeschlossen werden.

Allenfalls denkbar scheint eine Ausnahme von der Meldepflicht für den eHealth-Verzeichnisdienst. Aus rechtssystematischen Gründen stellt sich aber die Frage, ob dies nicht besser durch eine Novelle zur Standard- und Musterverordnung 2004 erreicht werden sollte (vgl. LRL 65; Vermeidung einer lex fugitiva).

Abs. 6 sollte daher ersatzlos gestrichen werden.

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 nochmals anzumerken, dass aus Datenschutzsicht stets eine „Opt-In-Lösung", also die Erteilung einer Zustimmung vor der Verarbeitung von Daten, als eingriffsschonendste Variante wäre. Entscheidet man sich dennoch – wie im vorliegenden 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.**

§ 15 Abs. 4 legt fest, dass zwar alle bis zum Zeitpunkt des Widerspruchs vorhandenen elektronischen Verweise auf ELGA-Gesundheitsdaten unwiderruflich zu löschen sind. Die ELGA-Gesundheitsdaten würden jedoch trotz Löschung der Verweise weiterhin gespeichert bleiben. Dies entspricht nicht den Vorgaben des DSG 2000 und der DS-RL, aufgrund derer jedenfalls auch eine Löschung der hinter den Verweisen stehenden ELGA-Gesundheitsdaten erforderlich wäre. Im Übrigen wird in § 15 Abs. 5 vorgesehen, dass ELGA-Gesundheitsdaten nicht verwendet werden dürfen, solange ein gültiger Widerspruch besteht. Eine „Verwendung“ von ELGA-Gesundheitsdaten würde nach der datenschutzrechtlichen Terminologie (§ 4 Z 8 iVm Z 9 DSG 2000) jedoch auch eine Speicherung umfassen. **Auf Grund dessen sollten § 15 Abs. 4 und 5 dahingehend überarbeitet werden, dass für den Betroffenen klar erkennbar ist, in welchen Fällen nur die Verweise ausgeblendet und wann tatsächlich ELGA-Gesundheitsdaten gelöscht werden müssen.**

Zudem müsste auf die Möglichkeiten, einen Widerspruch im Einzelfall zu erheben, klar und verständlich hingewiesen werden. Weder eine Information im Wege eines Aushanges gem. § 16 Abs. 5 noch die Information durch den ELGA-GDA nach § 16 Abs. 1 Z 3 (die überdies nur beim „Erstkontakt“ stattfinden soll) können eine individuelle Information des Teilnehmers – etwa im Wege eines entsprechend klar und verständlich formulierten Informationsschreibens, in welchem auch die einzelnen Widerspruchsmöglichkeiten dargestellte werden – ersetzen (siehe hierzu auch die Anmerkungen in den Vorbemerkungen, Pkt. I.1.c.).

§ 16 sollte weiters 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 Computer bzw. ohne Internetanschluss 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 ist der Entwurf zu ergänzen. Es müssten verständliche und detaillierte Regelungen zur E-Medikation (konkrete Ausgestaltung als Informationsverbundsystem/e) 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 ist fraglich, 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 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.

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 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:

a.) Aus dem Entwurf geht nicht ausreichend klar hervor, über welche technischen Methoden Patientinnen und Patienten identifiziert werden und wie der sichere Zugang zum Portal ausgestaltet wird.

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

c.) 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 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 Gesetzeswortlaut klar und verständlich hervorgeht, *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:

Zu Abs. 2 ist anzumerken, dass zwar technische Details in Verordnungen geregelt werden können, grundlegende organisatorische Regelungen jedoch im Gesetz vorgegeben sein sollten.

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.

§ 19 Abs. 3 sieht zwar nun im Sinne eines graduellen Systems für bestimmte Krankheiten eine „Opt-in"-Regelung vor. Es ist jedoch nicht ersichtlich, weshalb nur die in Abs. 3 angeführten Krankheiten einer „Opt-in"-Regelung unterliegen sollen. Vielmehr sollten Krankheiten mit besonders schwerwiegenden potenziellen Folgen für den Betroffenen bzw. Krankheiten, die für die Patienten von besonderer Sensibilität sein können, nur auf Verlangen in ELGA aufgenommen werden. **Der Datenschutzrat regt daher an, Datenkategorien festzulegen, die die Krankheiten mit potenziell schwerwiegenden Folgen oder hoher Sensibilität für den Patienten (wie z.B. psychische Erkrankungen, psychosomatische Störungen, Geschlechtserkrankungen, Erkrankungen und Eingriffe die Rückschlüsse auf das Sexualleben zulassen, Suchterkrankungen u.a.) der „Opt-In"-Regelung unterstellen.**

Weiters müsste – im Hinblick auf die bessere Nachvollziehbarkeit – ein derartiges ausdrückliches Verlangen der Patienten in ELGA schriftlich durch den GDA festgehalten werden.

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 ist aus datenschutzrechtlicher Sicht ausdrücklich abzulehnen.

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

Zu § 20:

Zur 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. dass 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 bleibt offen, welche konkrete Stelle hier als Dienstleister fungiert. Das Verhältnis zwischen „generellen“ und „individuellen“ Zugriffsberechtigungen bleibt ebenso unklar, insbesondere auch im Hinblick auf die Rechtsform, mit der die Berechtigungen eingeräumt werden sollen.

Zu § 22:

Die Regelung zum Zugangsportal lässt klare Bestimmungen darüber vermissen, mit welcher Methode auf Gesundheitsdaten im Wege dieses Portals zugegriffen werden muss. Nach der derzeit geltenden Rechtslage kommt hiefür ausschließlich jene Methode

in Frage, die auf Grund des E-Government-Gesetzes dafür vorgesehen ist, den Nachweis der eindeutigen Identität und der Authentizität des elektronisch gestellten Anbringens zu erbringen (§ 4 E-GovG). Eine ausdrückliche Normierung wäre nach Ansicht des Datenschutzrates wichtig, um auch sicherzustellen, dass nicht unsicherere Verfahren eingeführt werden.

Zu § 24:

Fraglich scheint, 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 Gesundheitsdaten iSd § 19 Abs. 3, die besonders schwerwiegende potenzielle Folgen für die/den Patientin/en nach sich ziehen kann, 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.

Darüber hinaus sollte auch eine Verwendung von ELGA-Daten für besonders missbräuchlich Zwecke – wie etwa durch einen Arbeitgeber im Weg einer unzulässigen Druckausübung auf den Betroffenen als Voraussetzung für die Aufnahme in ein Dienstverhältnis oder durch eine Versicherung als zwingende Voraussetzung im Hinblick auf den Abschluss einer Lebensversicherung – als strafbarer Tatbestand mit erhöhter Strafandrohung verankert werden.

Zu § 26:

a.) Eine Ausnahme von den Datensicherheitsmaßnahmen sieht § 3 Abs. 1 iVm § 26 des Entwurfes vor. Auf Grund dieser Bestimmung können sensible Daten va. auch per Fax oder Telefon oder im persönlichen Weg übermittelt werden. Durch diese „Übergangs-bestimmungen“ wird das vom GTelG grundsätzlich vorgegebene Datensicherheits-niveau 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 im Gesetz festgelegt werden.

Ausnahmen von Datensicherheitsmaßnahmen sollten – soweit sie erforderlich und verhältnismäßig sind – daher nur als Übergangsbestimmungen in einem **zeitlich äußerst eng begrenztem Rahmen** und 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-Krafttretens-Bestimmungen geregelt werden.

b.) In § 26 Abs. 2 ist unklar, 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.

Grundsätzlich wird bemerkt, 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.

Darüber hinaus lassen diese Regelungen offen, wie der ELGA-Teilnehmer bereits bei der Einführung von ELGA individuell informiert werden soll.

III. 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 dahingehend zu eng, als der Druck auf die/den Patient/in/en zur Zugänglichmachung ihrer/seiner ELGA-Gesundheitsdaten nicht immer mit einem Hinweis auf das drohende schädliche Verhalten einhergehen muss, sondern sich auch schon bloß aus der Tatsache des Verlangens heraus (z.B. Verlangen von ELGA-Daten beim Abschluss einer Lebensversicherung) ergeben kann. Auch erscheint der Beweis des Beabsichtigens der Setzung eines schädlichen Verhaltens für den Fall der Weigerung in vielen Fällen nur schwer zu erbringen, da sich ein derartiger Zwang auch schlüssig ergeben kann und im Hinblick auf den Zwang auf die (subjektive) Ebene der/des Patientin/en abgestellt werden müsste.

Daher sollte, nach Ansicht des Datenschutzrates, bereits das bloße widerrechtliche Verlangen von ELGA-Daten unter Strafe gestellt werden.

Zu § 118c wird angemerkt, dass eine Wortinterpretation des Tatbestandes dieser Bestimmung zu einer generellen Strafbarkeit von ELGA-Gesundheitsdiensteanbietern

führen könnte. Diesbezüglich sollte in § 118c insbesondere die Zeichensetzung nochmals überprüft werden.

Hinsichtlich des Tatbestandes des § 118c ist auch fraglich, weshalb nur jener Fall mit Strafe bedroht ist, in dem ELGA-Gesundheitsdaten missbräuchlich verwendet werden, die „vertraulich erhalten“ wurden. Dies könnte dazu führen, dass zwar die missbräuchliche Verwendung von ELGA-Gesundheitsdaten aus einem Patientenverhältnis unter Strafeandrohung gesetzt wird, ein Missbrauch von ELGA-Daten in jenen Fällen, in denen kein Patientenverhältnis mit dem Betroffenen vorliegt (etwa ein Patient eines anderen ELGA-GDAs), nicht unter diesen Tatbestand subsumiert werden kann. Diesbezüglich sollte die Bestimmung geprüft werden.

Abschließend verweist der Datenschutzrat auf die europäische Diskussion und Initiativen der EU-Kommission. So hat die EU-Kommission vorgeschlagen, den Zugang zu grenzüberschreitender Gesundheitsversorgung zu vereinfachen und führt auch Pilotmaßnahmen durch, um Europäer mit sicherem Onlinezugang zu ihrem medizinischen Gesundheitsdaten auszustatten, um eine breite Nutzung von Telemedizindiensten bis 2020 zu erreichen. Die Kommission wird außerdem einen gemeinsamen Mindestsatz an Patientendaten empfehlen, um bis 2012 die Interoperabilität beim Zugang und elektronischen Austausch von Patientenakten zwischen den Mitgliedsstaaten sicher zu stellen.

Sollte diese Entwicklung tatsächlich Realität werden müsste dieser Entwurf neu diskutiert werden, nicht nur hinsichtlich eines Mindestsatzes von Patientendaten, sondern insbesondere auch hinsichtlich Datenschutz und Patientensicherheit.

4. April 2011
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt