BUNDESARBEITSKAMMER

PRINZ EUGEN STRASSE 20-22
1040 WIEN
T 01 501 65 0

www.arbeiterkammer.at

Bundesministerium für Gesundheit
Radetzkystraße 2
1031 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel	501 65	Fax	501 65	Datum
BMG-100000/014-I/2010	SV-GSt	Werner Pletzenauer Daniela Zimmer	DW 2490		DW 2695		25.03.2011

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 Heilmasseurgesetz und das Strafgesetzbuch, geändert werden (Elektronische Gesundheitsakte-Gesetz – ELGA-G)

Die Bundesarbeitskammer bedankt sich für die Übermittlung des Entwurfs und nimmt dazu wie folgt Stellung:

Gegenstand des Entwurfs ist vor allen Dingen die Schaffung einer Rechtsgrundlage für eine Elektronische Gesundheitsakte (ELGA) mit dem Ziel, unter Einhaltung der Bestimmungen des Datenschutzes die PatientInnenrechte – insbesondere das Selbstbestimmungsrecht – zu stärken sowie eine Optimierung der Behandlungsprozesse im Rahmen einer integrierten Versorgung herbeizuführen. Damit soll auch ein wesentlicher Beitrag zur Sicherung der Finanzierung des österreichischen Gesundheitssystems geleistet werden.

Im Zusammenhang mit der ELGA wird die jährlich an die versicherten Personen zu übermittelnde Leistungsinformation dahingehend erweitert, dass alle TeilnehmerInnen der ELGA über ihre aus dieser Teilnahme zustehenden Rechte informiert werden. Weiters werden zum Schutz der Privatsphäre die TeilnehmerInnen der ELGA neben Verwaltungsstrafbestimmungen zwei neue Tatbestände in das Strafgesetzbuch aufgenommen, die das rechtswidrige Verlangen nach ELGA-Gesundheitsdaten sowie die missbräuchliche Verwendung von ELGA-Gesundheitsdaten sanktionieren.

DVR NR. 1048384

Derzeit befinden sich die Unterlagen über empfangene medizinische Leistungen bei den Leistungserbringern. Daher haben die Gesundheitsdiensteanbieter (GDA) bei der Neuaufnahme oder Weiterbehandlung ihrer PatientInnen keinen orts- und zeitunabhängigen Zugang zu den bei den verschiedenen GDA an sich bereits vorliegenden Gesundheitsdaten. Da sich die GDA durch den Zugriff auf ELGA-Gesundheitsdaten ein umfassenderes Bild vom Gesundheitszustand ihrer PatientInnen machen können, kann die elektronische Gesundheitsakte als ein geeignetes Instrument betrachtet werden, um das Entstehen von Informationslücken oder Informationsverlusten zum Nachteil von PatientInnen zu verhindern und dadurch die Qualität der Behandlung zu verbessern. Dazu kommt, dass dadurch Ineffizienzen im Gesundheitswesen wie Doppelbefundungen und Polypharmazie, die zudem eine zusätzliche Belastung der PatientInnen darstellen und unnötige Kosten verursachen, nachhaltig vermieden werden können.

Die Bundesarbeitskammer steht einer elektronischen Gesundheitsakte positiv gegenüber und hat gegen die Zielsetzungen des vorliegenden Entwurfs keine grundsätzlichen Einwände. Im Hinblick auf die Sensibilität von personenbezogenen Gesundheitsdaten besteht die Bundesarbeitskammer jedoch auf die Einhaltung der datenschutzrechtlichen Bestimmungen. Eine nähere Analyse des Entwurfs zeigt, dass dies ohne entsprechende Korrekturen nicht überall der Fall ist.

Allgemeine rechtliche Anforderungen an die Einführung elektronischer Patientenakte:

Die Verwendung von Gesundheitsdaten ist derzeit nur unter den Bedingungen des § 1 Abs 2 oder § 9 Datenschutzgesetz (DSG) 2000 möglich. Die Geheimhaltungsinteressen von Patienten gelten grundsätzlich dann nicht als verletzt, wenn der Betroffene der Verwendung ausdrücklich, *„ohne Zwang und in Kenntnis der Sachlage für den konkreten Fall„* zugestimmt hat oder die Daten unter anderem zum Zweck der Gesundheitsvorsorge, Behandlung oder Verwaltung von Gesundheitsdiensten erforderlich sind. Der letztere Erlaubnistatbestand (Art 8 Abs 3 der Datenschutz-RL 95/46/EG und durch § 9 Z 12 DSG 2000 umgesetzt) wäre aus Sicht der Art 29 Gruppe, die die EU-Kommission in Datenschutzfragen berät, keine ausreichende Rechtsgrundlage für ein so umfangreiches Datenverbundsystem wie ELGA.

Aus Art 8 Abs 4 der Datenschutz-RL 95/46/EG und § 1 Abs 2 iVm § 9 Z 3 DSG 2000 ergibt sich, dass sensible Daten auch dann verwendet werden dürfen, wenn sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen. Dabei müssen aber geeignete Garantien zum Schutz der Geheimhaltungsinteressen der Betroffenen gesetzlich verankert werden. Der vorliegende Entwurf stützt sich auf diese Ermächtigung und ist folglich daran zu messen, ob ein bedeutsames, öffentliches Interesse nachvollziehbar begründet wird und hinreichende Datenschutzstandards für die Betroffenen vorgesehen sind.

Die wichtigsten BAK-Anliegen:

- In den Erläuterungen wird das Kapitel Verbesserung der Qualität und Effizienz der Versorgung mit dem Satz eingeleitet **„Wer mehr weiß, kann mehr."** Den potentiellen Vorteilen einer umfassenden Informationssammlung über ELGA stehen allerdings auch nicht unwesentliche grundrechtliche Eingriffe desjenigen, der „mehr weiß", gegenüber.

Vor diesem Hintergrund ist die **Garantie einer freiwilligen Teilnahme** (unter Ausschluss von Nachteilen für Nicht-Teilnehmer) für die datenschutzrechtliche Beurteilung zentral. Auch wenn der Entwurf vom Prinzip der Selbstbestimmung der Betroffenen ausgeht, sind doch Zweifel angebracht, wie denn in der Praxis diese Privatautonomie verlässlich abgesichert und **faktische Diskriminierung** derjenigen, die sich nicht oder nur teilweise beteiligen, verhindert werden sollen.

- Die Einführung eines **Opt-Out-Systems**, in das Patientendaten automatisch aufgenommen und nur im Fall des Widerrufs des Betroffenen ausgenommen werden, ist aus Datenschutzsicht **keine best-practice Entscheidung**. Die Artikel 29 Gruppe, die die EU-Kommission in Datenschutzfragen berät, präferiert angesichts der hohen Sensibilität von Gesundheitsdaten eine Zustimmungslösung und schlägt als Kompromissvariante ein abgestuftes System an Opt-In- und Opt-Out-Anforderungen vor, abhängig davon, wie eingriffsintensiv die einzelne Datenanwendung ist. Die Datenschutzkommission rät ebenfalls dazu, einer **Opt-In-Lösung** den Vorzug zu geben.

- Da mit dem Gesetzesentwurf vom gesetzlich vorgesehenen Regelfall (dem Einholen einer ausdrücklichen Zustimmung des Betroffenen) abgewichen werden soll, muss der **Patientenautonomie auch bei einem Opt-Out-Modell** (grundsätzliche Teilnahme aller samt Widerrufsmöglichkeit) größte Beachtung geschenkt werden.

- Voraussetzung für die Annahme, dass PatientInnen mangels eines Widerrufs tatsächlich an ELGA teilnehmen wollen, ist eine ausführliche, verständliche und von jedem Betroffenen zuverlässig wahrgenommene **Vorinformation.** Es muss sichergestellt sein, dass auch Personen, die keinerlei Bezug zu Informationstechnologien und Datenschutz haben, die Tragweite ihrer Entscheidung, sich ganz, teilweise oder nicht an ELGA zu beteiligen, abschätzen können. Eine Informationskampagne ist überdies im Vorfeld der Systemeinführung vorzusehen, sodass jeder Einzelne bei Bedarf detailliertere Auskünfte einholen und in Ruhe entscheiden kann.

- Zu den **Mindestinformationen** zählen unter anderem der jeweilige Zweck der Datenverarbeitung, der potentielle Umfang der Datenarten, wer verantwortlicher Auftraggeber ist, welche Dienstleister herangezogen werden können, die potentiellen Empfänger im Fall der Datenweitergabe bzw eingeräumter Zugriffsmöglichkeiten. Weiters die Löschfristen und der Löschumfang, die Belehrung über die verschiedenen Formen des Widerrufsrechtes und die Folgen davon, die Belehrung über Auskunfts- und Berichtigungsrechte, Servicestellen, die beratend und Beschwerden entgegennehmend Hilfestellung anbieten und vieles mehr.

- Eine Vielzahl an Personen wird mit derartigen Informationen und noch mehr mit der Online-Steuerung ihres „Patientenprofils" auf einem Webseitenportal (Ausblenden von Informationen; Verweigerung von Zugriffsrechten) **massiv überfordert** sein. Es braucht daher eines ausreichenden Budgets für Organisationsstrukturen, die sicherstellen, dass Betroffene über Hotlines und eine akzeptable Dichte an Servicestellen ohne unzumutbare Anfahrtswege und ohne besonderen zeitlichen Aufwand Instruktionen erhalten, ihr

„Profil" abfragen und unter Anleitung von Servicepersonal ihre Gestaltungsrechte ausüben können.

- **Die Löschungspflichten sind im Gesetzesentwurf datenschutzrechtskonform auszugestalten**:

  1) Das Recht, der Aufnahme in ELGA ganz oder teilweise widersprechen zu können, setzt voraus, dass die Daten von Personen, die den Widerspruch anbringen**, auch tatsächlich physisch gelöscht** werden. Es entspricht nicht dem Datenschutzgesetz 2000, wenn im Widerrufsfall nur die einzelnen Verweise auf Daten entsprechend dem Zugriffsberechtigungssystem gelöscht werden, die Daten selbst aber in ELGA weiter enthalten bleiben. Mit einem Widerruf wird der weiteren Verwendung der Daten die Rechtsgrundlage entzogen, worunter gemäß den Definitionen des § 4 Z 8 DSG 2000 jede Art der Handhabung von Daten inklusive dem Verarbeiten fällt. Eine Löschung der Verweise und Zugriffberechtigung auf Daten, die als solche aber unlimitiert ein Teil des ELGA-Systems bleiben, reicht keinesfalls aus.

  2) Ebenso wenig kann damit das Auslangen gefunden werden, dass die „höchstzulässige Speicherdauer" mit 36 Monate festgelegt wird, davon aber wiederum nur die Löschung der Verweise betroffen sind und nicht der Dateninhalt selbst.

  Es ist technisch-organisatorisch sicherzustellen, dass sowohl im Widerrufsfall als auch am Ende der gesetzlich höchstzulässigen Speicherdauer die Daten auch physisch aus dem System entfernt werden. Dies setzt selbstverständlich voraus, dass der behandelnde GDA sich für seine eigenen gesetzlichen Dokumentationspflichten bzw Dokumentationsbedürfnisse eine von ELGA getrennte Aufbewahrung organisiert.

- Eine **Nicht-Teilnahme an ELGA darf für PatientInnen zu keinerlei Nachteilen** führen, weil ansonsten auch die Freiwilligkeit ihrer Teilnahme zweifelhaft wäre. Begrüßt wird, dass der Entwurf ein entsprechendes Diskriminierungsverbot enthält. Da der vorliegende Entwurf allerdings offen lässt, wie die Einhaltung dieses Diskriminierungsverbots in der Praxis durch die einzelnen PatientInnen wirksam durchgesetzt werden kann, werden entsprechende Garantien gefordert.

- Vor allem **ein potentieller Nachteil einer Nicht-Teilnahme** drängt sich auf: Es besteht die Sorge, dass die PatienInnen es künftig zu verantworten haben, wenn beispielsweise bestimmte Befunde vom Arzt nicht berücksichtigt wurden, weil er sie elektronisch nicht zugänglich gemacht hat. Vor diesem Hintergrund ist im Gesetz unbedingt auch klarzustellen, dass sich die GDA angesichts der individuellen Gestaltungsrechte des Patienten innerhalb von ELGA **auf die Vollständigkeit des elektronischen Patientenprofils nicht verlassen** dürfen. Die einzelnen GDA haben weiterhin gesprächsweise eine vollständige Anamnese durchzuführen, wollen sie im Schadensfall haftungsrechtliche Folgen ausschließen.

- Für PatientInnen muss die Verwendung ihrer Daten absolut **transparent** sein. Es wird begrüßt, dass der Entwurf dem Betroffenen ermöglicht, über ein Onlineportal nicht nur die zu seiner Person verarbeiteten Patientendaten, sondern auch die Protokolldaten über stattgefundene Zugriffe einzusehen. Die Benutzeroberfläche und Portalnavigation ist allerdings auch so benutzerfreundlich zu gestalten, dass sich dem Anwender der Dateninhalt und die Verwendungsvorgänge übersichtlich und transparent erschließen. Vorgaben dazu und eine Verordnungsermächtigung für die Ausgestaltung der Details fehlen im Gesetzesentwurf.

- Derselbe Grad an Transparenz muss außerdem für PatientInnen, die über keinen Internetanschluss verfügen, gewährleistet sein. Garantien für **alternative Zugangswege** (zB Zugriff beim behandelnden Arzt oder Apotheker) müssen explizit im Gesetz vorgesehen werden, sollen Betroffene ihre Rechte ohne unzumutbare Hürden ausüben können.

- Ein wichtiger Aspekt von Transparenz ist auch, dass die PatientInnen nicht über die **datenschutzrechtliche Rollenverteilung** im Unklaren gelassen werden: Wer verantwortet als Auftraggeber welche Datenanwendung und welche Dienstleister kommen auch noch in Kontakt mit seinen personenbezogenen Daten? Auf dem Onlineportal sind deshalb die jeweils verantwortlichen Auftraggeber auszuweisen, damit PatientInnen wissen, an wen sie sich im Bedarfsfall mit ihren Datenschutzansprüchen wenden.

- Unbeantwortet bleibt im vorliegenden Entwurf die Frage der **Haftung bei falsch bzw unvollständig übermittelten Daten** und daraus resultierenden Behandlungsfehlern. Diesbezüglich sollte der Gesetzgeber eine adäquate Vorgehensweise vorsehen.

- Bei der Ausgestaltung **genereller Zugriffsbefugnisse** durch den Gesundheitsminister ist auf Datensparsamkeit Wert zu legen. Orientieren sich die generellen Ermächtigungen am Maßstab des unbedingt Notwendigen, so wird den PatientInnen der komplizierte Weg erspart, individuelle Zugriffsbefugnisse erst definieren zu müssen. So gäbe es auf Patientenseite etwa große Einwände dagegen, dass GDA ohne weiteres **fachbereichsübergreifend Informationen** abrufen könnten. Plakativ gesagt muss der Zahnarzt nicht wissen, was der Urologe festgestellt hat. Über die generellen Zugriffsberechtigungen sollte nur ein Zugriff auf jene Datenarten eröffnet werden, die für eine Behandlung standardmäßig benötigt werden. Bezüglich der Ausgestaltung der generellen Zugriffsberechtigungen fehlen jegliche Vorgaben im Gesetzesentwurf, mit Blick auf das Bestimmtheitsgebot sind sie aber unbedingt einzuarbeiten.

- Explizit im Gesetz zu verankern ist auch, dass ELGA nur zur **Behandlung der PatientInnen durch GDA** verwendet werden darf **und** eine Datenverwendung für andere Zwecke (wissenschaftliche Forschung, Gutachtenerstellung, Statistik uä) **nur in anonymisierter Form** erfolgen darf.

- Der **Umfang der Datensicherheitsmaßnahmen** ist entscheidend für die Gesamtbewertung des Vorhabens (auch in finanzieller Hinsicht). Es ist keinesfalls ausreichend, Verordnungsermächtigungen zu erteilen, ohne die **Grundzüge des Datensicherheits-**

konzeptes bereits im Gesetz zu regeln. Soweit Datensicherheitsmaßnahmen im Entwurf lückenhaft angesprochen werden, sind sie bei weitem nicht ausreichend (zB § 3: Datensicherheitsmaßnahmen nicht nur für externe Weitergaben, sondern auch zum Schutz vor unberechtigten Zugriffen innerhalb des Betriebs; § 6: nicht bloß eine Verschlüsselung des Personenbezugs, sondern des gesamten elektronischen Aktes zum Schutz der Vertraulichkeit und Integrität).

- Ob die **Datensicherheitsmaßnahmen** aller zentralen und dezentralen Systemkomponenten und Datenschnittstellen dem Stand der Technik und der Sensibilität der Daten entspricht, muss **vor Aufnahme des Betriebs** durch ein unabhängiges Institut geprüft werden. Im **laufenden Betrieb** sind bei allen Akteuren stichprobenartige Kontrollen durchzuführen. Kontrollen, Berichtspflichten und eindeutige Zuständigkeiten hierfür fehlen jedoch im Gesetzesentwurf und sind unbedingt vorzusehen.

- Der Entwurf räumt etliche **Verordnungsermächtigungen ein, ohne dem Bestimmtheitsgebot** entsprechende Vorgaben schon im Gesetz zu verankern. Dies betrifft nicht nur die Datensicherheit, sondern auch die Rollenverteilung der Beteiligten und die Zuordnung der Auftraggebereigenschaft. Diese zentralen Entscheidungen sind im Gesetz zu treffen, Details können einer Verordnung vorbehalten bleiben.

- Die Einrichtung einer **Ombudsstelle** wird begrüßt. Darüber hinaus sind aber auch die **PatientenanwältInnen** als bei den PatientInnen gut eingeführte Erstanlaufstelle in das Auskunfts- und Beschwerdemanagement eng einzubeziehen.

- Von zentraler Bedeutung ist das im Entwurf enthaltene **Verbot, dass unbefugte Dritte wie Arbeitgeber, Versicherer, Behörden und Gerichte ELGA-Daten verlangen bzw auf diese zugreifen** dürfen. Als Vorbild für eine Regelung sollte § 67 des Gentechnikgesetzes (BGBl Nr 510/1994) herangezogen werden, der ein weitreichenderes Verbot enthält. Arbeitgebern und Versicherern einschließlich deren Beauftragten und Mitarbeitern ist demnach ausdrücklich verboten, Ergebnisse von genetischen Analysen von ihren Arbeitnehmern, Arbeitsuchenden oder Versicherungsnehmern oder Versicherungswerbern zu erheben, zu verlangen, anzunehmen oder sonst zu verwerten. Die Art 29 Datenschutzgruppe, die die EU-Kommission berät, empfiehlt darüber hinaus eine korrespondierende Norm im Arbeits- und Versicherungsrecht vorzusehen.

- Die mit dem Projekt ELGA verfolgten Einsparungsziele sind grundsätzlich anzuerkennen.

Zum Entwurf im Detail:

Zu § 1:

Nach § 1 Abs 3 gilt der Gesetzesentwurf nicht für GDA, die über keine IT-Einrichtungen verfügen. Diese nehmen folglich nicht an ELGA teil. Unklar ist, ob und inwieweit PatientInnen Gesundheitsdaten zu ihrer elektronischen Gesundheitsakte hinzufügen können. Entscheidender ist

dabei, ob und wie ELGA-GDA erkennen können, dass eventuell bedeutsame Befunde im System nicht zugänglich sind, weil sie von einem nicht an ELGA teilnehmenden GDA verwaltet werden.

Die nach § 1 Abs 3 von der Geltung des GTelG 2011 ausgenommen GDA sollen verpflichtet werden, in ihren Räumlichkeiten in Form eines leicht lesbaren und gut sichtbaren Aushanges darüber zu informieren, dass sie nicht an ELGA teilnehmen.

Zu § 2 Begriffsbestimmungen:

- § 2 Z 1 definiert Gesundheitsdaten extensiv, bezieht zum Beispiel auch „gesundheitsrelevante Lebensgewohnheiten oder Umwelteinflüsse" mit ein. Es ist im Sinn der Datensparsamkeit kritisch zu hinterfragen, ob es nötig ist, Angaben zu den Lebensumständen den GDA breit zugänglich zu machen.

- § 2 Z 2 definiert GDA derart weit, dass zB auch Krankenversicherungen darunter fallen würden. Die Erläuterungen weisen lediglich darauf hin, dass Rechtsanwälte „mangels Erbringung einer Gesundheitsdienstleistung" nicht als GDA anzusehen sind. Das reicht aus Sicht der Bundesarbeitskammer keinesfalls; erforderlich ist vielmehr eine Beschränkung auf tatsächliche, unmittelbare Erbringer einer Gesundheitsdienstleistung (oder in ihrem Auftrag tätige unselbständige Dienstleister) im Gesetz.

- § 2 Z 5 definiert den Begriff „Rolle", ohne ihn näher zu bestimmen. Mit Blick auf das Determinierungsgebot und der großen Tragweite einer solchen Bestimmung – immerhin hängt der Umfang der Zugriffsberechtigungen davon ab – sollten die Rollen bereits im Gesetz festgelegt werden.

- § 2 Z 6 beschreibt ELGA als „Informationssystem". Die Erläuterungen führen dazu aus, dass ELGA in die „Nähe eines Informationsverbundsystems" gerückt werden könnte, wobei jedoch vor allem die dezentrale Struktur und die „Modularisierung des Opt-Outs" für Infoverbundsysteme nicht charakteristisch wären, weshalb vom DSG abweichende Regeln getroffen worden sind.

  Diese Vorgangsweise ist keinesfalls ausreichend: Zunächst können die Erklärungen in den Erläuterungen keineswegs überzeugen, warum ELGA die Definition eines Infoverbundsystems nicht erfüllen sollte, denn § 4 Z 13 DSG 2000 nennt Voraussetzungen, die – soweit die ELGA-Systemarchitektur bekannt ist – durchaus vorliegen dürften, nämlich *„die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Nutzung der Daten in der Art, dass jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von anderen Auftraggebern dem System zur Verfügung gestellt wurden."*

  Es ist deshalb im Gesetzestext klarzustellen, ob und inwieweit es sich bei ELGA um ein Informationsverbundsystem oder – durchaus denkbar – auch um mehrere Informationsverbundsysteme handelt. Offenzulegen ist auch, wer Auftraggeber bzw nur Dienstleister

des/der System(e) ist, weil erst damit die datenschutzrechtlichen Verantwortlichkeiten zuordenbar sind.

- Nach § 2 Z 10 lit e zählt auch der sogenannte National Contact Point (NCP) zu den ELGA-GDA. Da der beim BMG eingerichtete NCP aber nicht selbst Gesundheitsdienstleistungen erbringt, kann er wohl vernünftigerweise nur die Rolle eines Dienstleisters einnehmen. Vor diesem Hintergrund ist nicht zu erkennen, welche „Auflagen" (lit dd) der NCP zu erfüllen hat.

- § 2 Z 13 definiert den Begriff „Verweisregister". Offen bleibt dabei, wer Betreiber dieser Einrichtung ist, denn die einzelnen GDAs als explizit genannte Auftraggeber kommen hierfür wohl nicht in Frage. Aus dem Blickwinkel der Datensicherheit wäre dies wichtig, weil das Register ein Angriffspunkt ist, der optimal vor einer Verletzung der Datenintegrität abzusichern ist. Es handelt sich dabei eindeutig um ein Informationsverbundsystem, worauf im Gesetz auch explizit hinzuweisen ist.

Zu den §§ 3 ff Datensicherheit:

Um Personen-, Befundverwechslungen uä zuverlässig zu vermeiden und Verantwortlichkeiten lückenlos nachvollziehen zu können, muss die Identifizierung und Authentifizierung von PatientInnen und dem medizinischen Personal ausnahmslos gewährleistet sein. Für die Art 29 Datenschutzgruppe ist dies ein zentraler Bestandteil jedes Sicherheitskonzeptes. Vor diesem Hintergrund sollten §§ 4 bis 7 (Nachweis und Prüfung der Identität, der Rollen und Integrität bzw Vertraulichkeit) auch bei der betriebsinternen Weitergabe elektronischer Gesundheitsdaten innerhalb des Verantwortungsbereiches eines GDA beachtet werden müssen. Gerade bei großen GDA (Krankenhäuser mit zahllosen Abteilungen) sollte dies selbstverständlich sein. Für die in § 3 Abs 1 des Entwurfes enthaltene Ausnahme besteht – nicht zuletzt in Hinblick auf § 14 DSG 2000 – insofern keine sachliche Rechtfertigung, als stets Maßnahmen zu treffen sind, die einen rechtswidrigen Datenzugriff unbefugter Dritter verhindern.

Die einzuhaltenden Datensicherheitsmaßnahmen bei herkömmlichen Datenübermittlungen etwa per Post, Telefon oder Fax sind eigens regelungsbedürftig. Der Entwurf enthält dazu nur Regelungsansätze in den Übergangsbestimmungen des § 26.

In § 3 Abs 2 Z 1 des Entwurfes erscheint die Ermächtigung, Daten aufgrund der Erlaubnistatbestände des gesamten § 9 DSG 200 weitergeben zu dürfen, unverhältnismäßig weit und ist auf Behandlungszwecke bzw lebenswichtige Interessen zu beschränken.

Auch die Erläuterungen geben im Übrigen keinen Aufschluss darüber, wie die eindeutige Identität durch Eintragung bzw Einsichtnahme in den Patientenindex bzw eHealth-Verzeichnisdienst festgestellt werden kann. Grundsätzliche Vorgaben dazu sind bereits im Gesetz zu treffen.

Zu § 6:

Eine Verschlüsselung „zumindest des Personenbezugs" ist keinesfalls ausreichend. Auch andere Akteninhalte sind hinsichtlich ihrer Vertraulichkeit und Integrität unbedingt zu schützen. Zudem müssen gesetzliche Vorgaben hinsichtlich der Anpassung der Datensicherheitsmaßnahmen an den jeweiligen Stand der Technik gemacht werden, um angesichts der hohen Sensibilität der Daten einen zeitgemäßen Schutz vor unberechtigten Zugriffen, Verfälschung etc sicherzustellen. Details, welche privacy enhancing technologies dem Stand der Technik entsprechen, könnten einer Durchführungsverordnung vorbehalten bleiben.

Zu § 11:

Es ist klarzustellen, dass die Auskünfte jedenfalls keine (direkt oder indirekt) personenbezogenen Daten enthalten dürfen.

„Elektronische Gesundheitsakte (ELGA)" – §§ 13 bis 23:

Zu § 13:

Es sollte gleich eingangs darauf eingegangen werden, dass ELGA sich aus einem bzw mehreren Informationsverbundsystemen zusammensetzt und die Auftraggeber-, Betreiber- und Dienstleisterrollen in einem Absatz zu beschreiben sind. Für den Rechtsanwender sind die Verantwortungsbereiche über mehrere Bestimmungen verstreut äußerst schwer nachvollziehbar: § 19 beschreibt die ELGA-GDA als Auftraggeber für die Speicherung von ELGA-Gesundheitsdaten, aber auch für die Speicherung von elektronischen Verweisen im Verweisregister. Die ELGA-Systempartner betreiben das Berechtigungssystem, die ELGA-TeilnehmerInnen sind hinsichtlich individueller Zugriffsberechtigungen Auftraggeber, die ELGA-Systempartner Dienstleister.

Die Stärkung der PatientInnenrechte kann bei der Frage, ob ein wichtiges öffentliches Interesse an ELGA besteht, nicht ernsthaft ins Treffen geführt werden. Ohne ELGA-Vorhaben bedürfte es über das DSG hinaus keine besonderen Vorkehrungen im Sinne zusätzlicher Informationsrechte und Rechtschutzmöglichkeiten. Mit anderen Worte: Die angebotenen Garantien sind die Antwort auf die Grundrechtssensibilität von ELGA, aber kein entscheidendes Motiv für dessen Einführung.

In Abs 4 ist sicherzustellen, dass ein Zugriff auf andere Register durch GDA nur zulässig ist, soweit er für den Behandlungs- oder Betreuungsfall erforderlich und entsprechend den zugehörigen Rollen erfolgt. Ein Zugriff unabhängig von einer Behandlung sollte grundsätzlich nicht möglich sein. Soweit Ausnahmen sachlich gerechtfertigt sind, sollten sie im Entwurf explizit aufgezählt werden. Zudem ist taxativ anzuführen, welche Register gemeint sind.

Die mit Abs 5 iVm § 2 2 Z 10 lit e verfolgten Zwecke sind zu unbestimmt. Dem Betroffenen, der seine Zustimmung erteilt, muss die Tragweite seiner Entscheidung klar sein: Aus welchem Grund der NCP unabhängig von einer Behandlung personenbezogene Daten „zum gegenseiti-

gen Datenaustausch außerhalb der EU" weitergeben sollte, bleibt völlig offen. Von der Befugnis des NCP gemäß § 2 Z 10 lit e aa und bb Daten zur Unterstützung der Gesundheitsversorgung eines Patienten innerhalb der EU weiterzugeben, wird wohl vernünftigerweise nur im Behandlungsfall Gebrauch gemacht werden.

Abs 6 enthält eine Verordnungsermächtigung ohne grundsätzliche Vorgaben für angemessene Sicherheitsmaßnahmen und ist deshalb ergänzungsbedürftig.

Zu § 14:

In § 14 Abs 2 sollte an Stelle des Begriffs „medizinische Notfälle" der datenschutzrechtliche Begriff des *„lebenswichtigen Interesses des Betroffenen"* verwendet werden, um etwaige Unsicherheiten, wann ein Notfall vorliegt, zu vermeiden. Außerdem ist klarzustellen, dass auch im Notfall natürlich nur gesetzlich Berechtigte entsprechend § 7 DSG 2000 auf ELGA-Daten zugreifen dürfen.

Die Verwendungsbeschränkungen in Abs 3 werden grundsätzlich begrüßt. Sie schließen aber allein noch nicht aus, dass Zugriffsbefugnisse in andere Materiengesetze aufgenommen werden. Diese könnten das Nutzungsverbot für andere Zwecke als der Gesundheitsversorgung im Sinn des § 9 Abs 12 DSG 2000 weitreichend unterlaufen. Vor diesem Hintergrund muss die Bestimmung um ein Verwendungsverbot von ELGA-Daten durch Behörden, Arbeitgeber und Versicherungen ausdrücklich ergänzt werden. Für Zwecke der Wissenschaft, Politiksteuerung und von Einsparungseffekten bei den Sozialversicherungsträgern ist eine Verwendung von ELGA-Daten mit (in)direkten Personenbezug zu untersagen, da eine Nutzung statistischer Daten hierfür ausreicht.

In § 14 Abs 4 sind mit „anderen Gesundheitsdiensteanbieter" wohl jene gemeint, die den Patienten nicht behandeln. Eine entsprechende Klarstellung sollte erfolgen. Der letzte Halbsatz sollte entsprechend der Terminologie des DSG 2000 mit *„zu verwenden" enden.*

In § 14 Abs 6 ist die Meldepflicht nach § 17 DSG 2000 keinesfalls abdingbar. Soweit die Einrichtungen als Infoverbundsysteme ausgestaltet werden, besteht zudem die Notwendigkeit einer Vorabkontrolle durch die Datenschutzbehörde.

Zu den §§ 15 und 16:

PatientInnendaten werden automatisch in ELGA einbezogen, sofern der Betroffene nicht widersprochen hat. Wie dargelegt wird aus Datenschutzgründen einer „Opt-In"-Lösung der Vorzug gegeben. Bei einem „Opt-Out" muss das Augenmerk jenen Maßnahmen gelten, die die Beeinträchtigung der Selbstbestimmung abfedern sollen. Dazu muss der Betroffene bereits im Vorfeld alle relevanten Informationen erhalten, um abschätzen zu können, wer unter welchen Umständen was über ihn erfährt.

§ 15 Abs 2 fordert für das Zustandekommen eines gültigen Widerspruchs, dass dieser schriftlich gegenüber einer noch einzurichtenden Widerspruchstelle oder elektronisch über das Zugang-

sportal zu erfolgen hat. Die Identität der Person, die nicht an ELGA teilnehmen möchte, als auch die Authentizität der Mitteilung müssen geprüft werden können. Das ist allerdings nur möglich, wenn die Identität der betreffenden Person anhand ihres Lichtbildausweises überprüft und die Authentizität des Widerspruches sogleich durch die Person bestätigt wird.

Da eine solche eindeutige Prüfung eines schriftlichen Widerspruchs nur ex post und mit erheblichem Aufwand möglich ist, sollte, wenn sich die betreffende Person gewöhnlich im Inland aufhält, zur Verhinderung von Personenverwechselungen und allfälliger daraus resultierenden Löschungen von Daten Dritter sowie zur Vermeidung von Missbrauchsfällen ein Widerspruch bei einer Widerspruchstelle grundsätzlich nur persönlich möglich sein. Dieser schriftliche Widerspruch sollte nur in begründeten Ausnahmefällen bestehen. Die Löschung von Gesundheitsdaten sollte in solchen Fällen erst dann vorgenommen werden, wenn die betreffende Person ihrerseits den Erhalt der Widerspruchsbestätigung bestätigt.

Mit Blick auf ältere und nicht technikaffine Menschen und solche, die überhaupt kein Internet haben, müssen in ausreichender Dichte Servicestellen eingerichtet werden, die einerseits als leicht erreichbare Anlaufstellen für Auskünfte, Hilfestellung und die Einsichtnahme in die eigenen ELGA-Daten und Zugriffsprotokolle fungieren und bei denen andererseits die Abgabe des Widerspruchs möglich ist. Zudem ist eine Abgabe bei jedem GDA zu überlegen.

Nach § 15 Abs 5 zweiter Satz dürfen ELGA-Gesundheitsdaten im Widerspruchsfall nicht verwendet werden, was in der Terminologie des DSG auch das Speichern der Daten umfasst. Nach § 15 Abs 4 sollen aber im Widerspruchsfall bloß die elektronischen Verweise auf ELGA-Daten gelöscht werden, nicht aber die physischen Daten selbst. Eine Weiterverarbeitung der Daten „im Hintergrund" steht aber nicht in Einklang mit den Widerrufs- bzw Widerspruchsrechten des DSG 2000, die in diesem Fall eine vollständige Löschung vorsehen.

Das in § 15 Abs 5 zweiter Satz angeführte Verbot der Verwendung von ELGA-Gesundheitsdaten im Falle eines Widerspruchs bedeutet bei wörtlicher Interpretation, dass nicht einmal die behandelnden GDA auf die in ihren eigenen Krankengeschichten enthaltenen ELGA-Gesundheitsdaten zurückgreifen dürften. Diesbezüglich ist eine Klarstellung erforderlich. Vorgeschlagen wird die Formulierung: *„Solange eine gültiger Widerspruch besteht, dürfen ELGA-Gesundheitsdaten von Unberechtigten nicht verwendet werden".*

Da in § 15 die e-Medikation nur sehr kursorisch angesprochen wird, ist zu betonen, dass diese Datenanwendung im Entwurf überhaupt nicht geregelt ist. Auch die übrigen Datenanwendungen werden nicht näher beschrieben. Wer aufgrund welcher Rolle darauf zugreifen darf, bleibt somit im Dunkeln. Es ist auf das gesetzliche Bestimmtheitsgebot hinzuweisen, aber auch darauf, dass der Betroffene sich nur dann wirksam auf ELGA einlassen oder widersprechen kann, wenn die Infoverbundsysteme bzw Datenbanken ausreichend klar beschrieben werden.

ELGA-TeilnehmerInnen können nach § 16 Abs 1 Z 3 und Z 4 ihren Gesundheitsakt individuell gestalten, indem sie der Datenverarbeitung im Einzelfall widersprechen, elektronische Verweise ausblenden oder einen ELGA-GDA vom Zugriff ausschließen. Nochmals ist in diesem Zusammenhang zu betonen ist, dass durch diese wichtigen Selbstbestimmungsrechte ELGA keinen

verlässlich vollständigen Überblick über die Unterlagen eines Patienten bietet. Die GDA dürfen sich daher bei ihren Dispositionen niemals auf die Eintragungen allein verlassen. Diese Konsequenz ist haftungsrechtlich von großer Bedeutung und sollte auch im Gesetz klargestellt werden.

§ 16 Abs 2 sieht vor, dass im Widerspruchsfall Patientinnen beim Zugang zur medizinischen Versorgung bzw bei der Kostentragung keine Nachteile erfahren dürfen. So sehr diese Regelung auch begrüßt wird, fehlen im vorliegenden Entwurf jedoch Bestimmungen, die eine effektive Sicherstellung dieses Diskriminierungsverbotes garantieren. Die Verletzung dieses Diskriminierungsverbotes sollte jedenfalls in den Strafkatalog des § 24 aufgenommen werden.

Die in § 16 normierten Rechte der ELGA-TeilnehmerInnen, insbesondere das Recht, jederzeit Einsicht in ihre ELGA-Gesundheitsdaten sowie in die Protokolldaten gemäß § 21 Abs 2 nehmen zu können, werden ausdrücklich begrüßt. Diese Einsichtsrechte sollen den Erläuterungen zufolge dem Auskunftsrecht in § 26 DSG vorgehen. Tatsächlich kann DSG diesbezüglich nur ergänzen, weil die Rechte in § 26 auf die Datenschutz-RL 95/46 EG zurückgehen und auch für ELGA-TeilnehmerInnen gelten müssen.

§ 16 Abs 3 sieht vor, dass die TeilnehmerInnenrechte schriftlich gegenüber dem Betreiber des Berechtigungssystems oder elektronisch im Wege des Zugangsportals ausgeübt werden können. Um zu gewährleisten, dass Unbefugte nicht Einsicht in Gesundheits- und Protokolldaten von Dritten erlangen, sollte die Ausübung des Einsichtsrechts nur nach Prüfung der eindeutigen Identität der betreffenden TeilnehmerInnen möglich sein.

Nach § 16 Abs 5 soll eine Rechtsbelehrung über das Widerrufsrecht in Form eines Aushanges erfolgen. Dies ist keinesfalls ausreichend, um davon ausgehen zu können, dass die Betroffenen zuverlässig darüber Kenntnis erlangen. Es ist unverzichtbar, dass im Vorfeld jeder Versicherte durch eine postalische Zusendung über das Widerrufsrecht und über dessen Ausübung informiert wird.

Zu § 19:

Ein „Opt-In" für bestimmte besonders heikle Gesundheitsdaten wird begrüßt. Auch die Art 29 Datenschutzgruppe rät – wie eingangs erwähnt – zu einem abgestuften System an Opt-In und Opt-Out-Anforderungen mit Blick darauf, dass eine unrechtmäßige Verwendung je nach Datenart unterschiedlich schwere Folgen haben kann.

Elektronische Verweise sind grundsätzlich nach 36 Monaten zu löschen. Die in ELGA gespeicherten Gesundheitsdaten würden demnach ad infinitum gespeichert bleiben. Dies ist insofern unverhältnismäßig, als an alten Daten für die in ELGA genannten Zwecke nach Löschung der Verweise keinerlei Dokumentationsbedarf mehr besteht. Die Daten sind daher unbedingt restlos aus dem System zu entfernen. GDA haben ihre gesetzlichen Dokumentationspflichten selbstverständlich weiterhin zu erfüllen, jedoch eine Aufbewahrung zu organisieren, die keinerlei technischen Bezug zu ELGA mehr aufweist.

Die Systemvorgabe einer dezentralen Speicherung wird ebenfalls begrüßt. Allerdings sollte der Entwurf den Datensicherungsmaßnahmen viel größere Beachtung schenken. Zur Absicherung der Geheimhaltung und Integrität der dezentral gespeicherten ELGA-Daten braucht es strenger Datensicherheitsmaßnahmen, die zwingend im Gesetz zu verankern sind. Offen bleibt, weshalb Medikationsdaten zentral gespeichert werden sollen.

Zu § 20:

Der Entwurf muss das generelle Berechtigungssystem und die Rollenverteilung zumindest in Grundzügen regeln. Die Verordnungsermächtigung des Gesundheitsministers ist allerdings nicht näher determiniert. Wer auf welche Daten Zugriff hat ist daher näher auszuführen. Maßstab darf dabei nicht sein, was für die Kommunikation der GDA untereinander unter Umständen nützlich sein kann, sondern welche Daten in Standardfällen typischerweise erforderlich sind. Unbedingt Rücksicht zu nehmen ist dabei auch auf die Wünsche der Patienten, die ohne Zweifel große Vorbehalte hätten, würde der Datenzugriff in jedem Fall fachbereichsüberschreitend ermöglicht („Der Zahnarzt weiß, was der Urologe festgestellt hat") bzw das unbefangene Einholen einer Second Opinion erschwert werden.

Der Entwurf legt fest, dass die PatientInnen hinsichtlich individuell erteilter Zugriffsberechtigungen Auftraggeber wären. Würde es dabei zu missbräuchlichen Abfragen bzw Datennutzungen kommen, wäre der Patient dafür verantwortlich. Da er in keiner Weise Einfluss auf die Sicherheit des Systems hat, kann er diese Verantwortung nicht ernsthaft übernehmen. Das Auftraggeberkonzept ist insgesamt nochmals gründlich zu überdenken. So ist beispielsweise unklar, wer für die richtige Umsetzung von Ausblendungen und individueller Zugriffssperren nach § 16 Abs 1 als Auftraggeber haftet.

Zu § 21:

Das Protokollierungssystem hat technisch unabhängig von ELGA zu sein. Wer es betreibt, als Auftraggeber verantwortlich ist und die Aufbewahrung nach Abs 3 zu organisieren hat, bleibt völlig offen. Protokolldaten sollen nicht nur von betroffenen GDA, sondern natürlich auch von PatientInnen zur Durchsetzung rechtlicher Ansprüche benutzt werden können.

Zu § 24:

Wie die jüngsten sich in Österreich ereigneten Datenmissbrauchsfälle deutlich gemacht haben, kann eine vollständige Datensicherheit nicht gewährleistet werden. Im Hinblick auf die Sensibilität von Gesundheitsdaten erachtet die Bundesarbeitskammer die Schaffung von Straftatbeständen als dringend geboten, um die ELGA-TeilnehmerInnen vor Missbrauch ihrer Gesundheitsdaten zu schützen. Damit das Vertrauen der Bevölkerung in ELGA erhöht wird und um potentielle Täter vorab abzuschrecken, sollte das angedrohte Strafmaß deutlich angehoben sowie bereits bei erstmaliger Tatbegehung eine empfindliche Mindeststrafe verhängt werden. Ausdrücklich sind auch unzulässige zivilrechtliche Sekundärnutzungen der Daten als Straftatbestände aufzunehmen (Arbeitgeber bzw Kranken- oder Lebensversicherungen, die ELGA-Daten von potentiellen Arbeitnehmern bzw Versicherungsnehmern verlangen). In den Katalog

an Straftatbeständen sollte auch das (faktische) Benachteiligen von PatientInnen, die Widerspruch gegen eine ELGA-Teilnahme eingelegt haben, aufgenommen werden.

Nach § 24 Abs 2 begeht, wer ohne nach diesem Bundesgesetz oder nach anderen gesetzlichen Vorschriften dazu berechtigt zu sein, die Einsicht in oder die Weitergabe von ELGA-Gesundheitsdaten verlangt, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, eine Verwaltungsübertretung, die mit Geldstrafe bis zu 15.000 Euro zu ahnden ist.
Nach § 24 Abs 3 begeht, wer als ELGA-GDA oder Personen gemäß § 14 Abs 3 Z 1 lit b ELGA-Gesundheitsdaten verwendet ohne dazu berechtigt zu sein, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, eine Verwaltungsübertretung und ist mit Geldstrafe bis zu 20.000 Euro zu bestrafen.

Gemäß § 1 Abs 3 gilt das GTelG 2011 nur für GDA, die über eine Einrichtungen der Informations- und Kommunikationstechnologie verfügen, um Gesundheitsdaten elektronisch zu verwenden. Sollten allerdings Personen, die nicht vom Geltungsbereich des GTelG 2011 umfasst sind, wie zB Arbeitgeber bzw Vertreter von Kranken- oder Lebensversicherungen, unberechtigt ELGA-Gesundheitsdaten verlangen oder verwenden, so sind auf diesen Personenkreis die Straftatbestände des § 24 Abs 2 und 3 nicht anwendbar.

Die Bundesarbeitskammer fordert, dass alle vom Geltungsbereich des GTelG 2011 ausgenommen Personen unter die Straftatbestände des § 24 Abs 2 und 3 GTelG 2011 fallen. Dies vor allem deshalb, weil der im Entwurf vorgesehene gerichtliche Straftatbestand des § 118b StGB nur das qualifizierte „Verlangen unter Nachdruck" unter Strafe stellt. Auch die Aufforderung allein ohne Hinweis auf einen Nachteil (kein Arbeitsplatz, keine Versicherung) ist in der Praxis geeignet die Betroffenen einem massiven Druck auszusetzen.

Zu § 26:

Für die Ausnahme von den Datensicherheitsmaßnahmen (§ 26 iVm § 3) besteht keine sachliche Rechtfertigung. Gesundheitsdaten dürften demnach auch per Fax, Telefon oder durch persönliche Übergabe übermittelt werden. Auch bei herkömmlichen Datenweitergaben ist nach dem DSG 2000 auf angemessene Datensicherheitsstandards zu achten. Identifizierung, Integrität und Vertraulichkeit und die klare Zuordnung von Berechtigungen zählen zu den Mindeststandards, von denen nicht abgewichen werden kann. In der Übergangsbestimmung fehlt zudem ein fixes Geltungsdatum.

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. Diese Informationspflichten decken sich nicht mit § 24 DSG 2000, weshalb sie diese nur ergänzen,

nicht aber ersetzen können. Vor allem sollte die Sozialversicherung in Bezug auf ELGA verständlich über alle Vorteile und Risiken der jeweilige Zweck der Datenverarbeitung aufklären. Ebenso über den potentiellen Umfang der Datenarten, wer verantwortlicher Auftraggeber ist, welche Dienstleister herangezogen werden können, die potentiellen Empfänger im Fall der Datenweitergabe bzw eingeräumter Zugriffsmöglichkeiten, die Löschfristen und der Löschumfang, die Belehrung über die verschiedenen Formen des Widerrufsrechtes und die Folgen davon, die Belehrung über Auskunfts- und Berichtigungsrechte und über Servicestellen, die beratend und Beschwerden entgegennehmend Hilfestellung anbieten.

III. Zu Art 10 (Änderung des Strafgesetzbuches):

Zu Z 1 (§ 118c):

Der Tatbestand des § 118c StGB stellt die missbräuchliche Verwendung von ELGA-Gesundheitsdaten unter Strafe. Normadressaten dieser Bestimmung sind laut den Erläuterungen nur ELGA-GDA sowie Personen, die die ELGA-GDA bei der Ausübung ihrer Tätigkeiten unterstützen. Nach Ansicht der Bundesarbeitskammer sollte jedoch aus generalpräventiven Gründen jede missbräuchliche Verwendung von ELGA-Gesundheitsdaten, unabhängig von der Person, also auch der Missbrauch von ELGA-Gesundheitsdaten durch Personen, die nicht ELGA-GDA sind, pönalisiert werden.

Herbert Tumpel
Präsident

BUNDESARBEITSKAMMER

Alice Kundtner
iV des Direktors