Hans G. Zeger[1],

Anmerkungen zu den IT-Sicherheitsleitlinien von ELGA[2]

IT-Sicherheitskonzepte, das europäische und das österreichische Datenschutzrecht gehen bei der Verwendung vertraulicher Daten von der Verantwortlichkeit EINES Auftraggebers aus, der letztlich auch den Schutz der Grundrechte und der Privatsphäre der Patienten zu garantieren hat. Diesen Anforderungen werden die vorglegten Sicherheits-Leitlinien der ELGA GmbH nicht gerecht. Sie beschränken sich in einem Sammelsurium von Allgemeinplätzen und Stilblüten.

ELGA SICHERHEITS-LEITLINIEN[3]

Dem Autor liegen eine Reihe sogenannter ELGA-Sicherheits-Leitlinien vor:
001 - ELGA ISMS - Informationssicherheitspolitik
002 - ELGA ISMS - Informationssicherheitsorganisation
006 - ELGA ISMS - Generelle Vorgaben für die Netzwerksicherheit und Rechnerverwaltung
007 - ELGA ISMS - Systemzugriffsüberwachung und Zugriffskontrolle
008 - ELGA ISMS - Beschaffung, Entwicklung und Wartung von ELGA-Komponenten und ELGA-Anwendungen
ELGA ISMS - Leitlinien Glossar

Um den Sinn und auch die Verwendbarkeit dieser Leitlinien beurteilen zu können, wurden sie auf Praxis- und Prozesstauglichkeit (enthalten sie genügend klare operative Aussagen, die überhaupt technisch realisiert werden können?), auf Umsetzbarkeit (technischer und organisatorischer Art) und auch dahingehend geprüft, ob sie mit bestehenden rechtlichen Rahmenbedingungen vereinbar sind.

Die Anmerkungen geben nur einen ersten Eindruck zu den Leitlinien wieder und können keine tiefergehende Analyse der Sicherheitsanforderungen zu ELGA ersetzen. Da die meisten Formulierungen extrem allgemein gehalten sind, entziehen sie sich - ohne Vorlage der konkreten Umsetzungskonzepte - weitgehend einer abschließenden Abschätzung der Konsequenzen für die österreichische Gesundheitsversorgung.

001 - ELGA ISMS - INFORMATIONSSICHERHEITSPOLITIK

Bei oberflächlicher Betrachtung klingen die angestrebten Ziele durchaus sinnvoll, tatsächlich erschöpfen sie sich jedoch durchgängig in Allgemeinplätze und Plattitüden.

001 - BEISPIEL 1:

Als Ziel der Sicherheitspolitik wird beispielsweise genannt "LL01_Z1 Die Verfügbarkeit und Kontinuität von ELGA ist, unter Berücksichtigung der jeweiligen Rahmenbedingungen, bestmöglich erfüllt."

---

1 Jahrgang 1955, Studium Philosophie, Mathematik, Sozialwissenschaften, Autor von "MENSCH.NUMMER.DATENSATZ. Unsere Lust an totaler Kontrolle", Residenzverlag 2008, "Paralleluniversum Web2.0", Kremayr&Scheriau 2009 und zahlreicher weiterer Fachpublikationen, Lektor am Juridicum Wien, Mitglied des Datenschutzrates im Bundeskanzleramt und Geschäftsführer der "e-commerce monitoring GmbH", Obmann der "ARGE DATEN - Österreichische Gesellschaft für Datenschutz" (http://www.zeger.at)

2 ELGA = **EL**ektronischer **G**esundheits**A**kt laut vorliegendem Entwurf zum ELGA-Gesetz

3 Die Leitlinien waren in der Version 2.0 vom 28.9.2011 verfügbar, sie waren nicht als vorläufige Version oder Entwurfsversion gekennzeichnet.

Diese Formulierung ist kein Ziel sondern ein nichtssagender Allgemeinplatz. Niemand, weder ein Auftraggeber, noch Patienten oder Ärzte könnten daraus irgendwelche Hinweise über die Verfügbarkeit von ELGA ableiten oder Rechte bezüglich der Verfügbarkeit in Anspruch nehmen.

Sinnvolle Ziele im Sinne einer funktionsfähigen IT-Lösung müssten quantitativ determiniert sein, etwa eine garantierte Verfügbarkeit von ELGA-Dokumenten zu mindestens 99,9% der Zeit, wobei die tägliche Ausfallszeit nicht mehr als 10 Minuten und die Maximaldauer eines Ausfalls nicht mehr als 5 Minuten beträgt. Erst zu derartigen Vorgaben könnten seriöse Aufwands- und Kostenschätzungen erfolgen und es wäre möglich die Konsequenzen für die Gesundheitsversorgung abzuschätzen.

Gleiches gilt für alle anderen "Ziele", wobei LL01_Z2 als besondere Stilblüte hervorsticht: "Die Vertraulichkeit und Integrität der durch ELGA verfügbaren Informationen und Daten ist sichergestellt."

Hier werden Ziele quasi dekretiert "ist sichergestellt". Sollte damit gemeint sein, dass die gesetzliche Anforderung des DSG 2000 § 14 (Datensicherheit) erfüllt wird, ist das Ziel überflüssig, gesetzliche Bestimmungen sind einfach einzuhalten, das muss nicht extra in einer Leitlinie formuliert werden.

Ansonsten müsste als Ziel angegeben werden, in welcher Art Vertraulichkeit und Integrität erfüllt werden. Eine entsprechendes Ziel wäre etwa: *Die Vertraulichkeit wird durch durchgängige Verschlüsselung aller Dokumente, sowohl während der Übertragung, als auch bei Speicherung auf Datenträgern gesichert. Die Integrität wird durch ein digitales Signier- und Vidierverfahren sichergestellt, das zumindest dem Standard der fortgeschrittenen Signatur gemäß SigG entspricht und bei dem fälschungssicher jene Organisation feststellbar ist, die für die Ausgabe des Dokuments verantwortlich ist. Weiters erhält jedes Dokument durch eine unabhängige Organisation einen fälschungssicheren Zeitstempel zur Feststellung des Erzeugungsdatums des Dokuments.*

001 - BEISPIEL 2:

Unter "4. Verantwortung" findet sich folgender Gemeinplatz: "1. Die ELGA-Systempartner sind sich ihrer Verantwortung bewusst und haben aus diesem Grund die Einführung des ELGA ISMS beschlossen."

Abgesehen davon, dass es sich um eine völlige Leeraussage handelt, ist sie auch sachlich falsch. Die Entscheidung für oder gegen ein ELGA ISMS kann und darf nicht im Ermessen der "ELGA-Systempartner" liegen, sondern bedarf einer eindeutigen gesetzlichen Vorgabe.

001 - BEISPIEL 3:

Unter "5. Geltungsbereiche" finden sich Aussagen zum "Zugangsportal". Der Zugang soll in drei Stufen organisiert werden, wobei im nächsten Absatz angegeben wird, dass die beiden ersten Stufen sich auf das "Österreichische Gesundheitsportal" beziehen, das gar nicht Teil von ELGA ist.

Umgekehrt erschöpft sich die Aussage zum ELGA-Teil, Stufe 3, wieder in einem Gemeinplatz: "Stellt für authentifizierte ELGA-Teilnehmer und ELGA-GDA den Zugang zu ELGA dar." Hier wären Angaben zu einem Berechtigungssystem erforderlich, u.a. wie werden welche Mediziner bzw. GDAs berechtigt auf Dokumente zuzugreifen, wie sind Vertretungslösungen zu organisieren (z.B. Urlaubsvertretungen bei den Ärzten oder auch Auskunftsmöglichkeiten von Angehörigen der Patienten, wie sind die Zugriffsregeln für Patientenanwälte usw. zu organisieren)? Weiters, wie sind Vertretungen von Vertretungen zu handhaben? Es muss daran erinnert wrden, dass es bei der Bürgerkarte, die bloß ganz

einfache Verwaltungsvorgänge unterstützt, bis heute nicht gelungen ist, ein funktionsfähiges Vertretungssystem darzustellen.

ELGA macht sich somit Gedanken über ELGA-fremde Dinge, bleibt aber bei einer Zentralfrage, der ELGA-Authentifizierung, völlig nebulos.

001 - BEISPIEL 4:

Unter "7. Vorgehensweise" wird zwar auf den IT-Sicherheitsstandard ISO 27*** Bezug genommen, im gleichen Absatz aber davon abgewichen: "Diese Normserie wurde adaptiert, da sie auf eine juristische Person und nicht auf ein Konstrukt von mehreren juristischen und natürlichen Personen ausgerichtet ist. Damit ist die ISO 27000 zwar nicht direkt anwendbar, trotzdem wird systematisch und methodisch danach vorgegangen."

Diese Vorgangsweise ist völlig unzulässig. Standards sind eben keine Selbstbedienungsläden, bei denen man sich beliebige Einzelteile herausnimmt und den Rest ignoriert. Die eindeutige Verantwortung für ein Gesamtsystem ist zentraler Kern eines Sicherheitsmanagementsystems und kann nicht "adaptiert", sprich weginterpretiert werden. Im übrigen verlangt auch das DSG 2000 die eindeutige Verantwortlichkeit eines Auftraggebers für eine Datenanwendung.

Eine "Absicherung über Verträge", wie es die Leitlinie in Aussicht stellt, kann nur dann sinnvoll sein, wenn diese "Verträge" tatsächlich die alleinige Verantwortung einer Stelle für das ELGA-System festschreiben, dann wäre aber der eingangs zitierte Satz überflüssig.

001 - BEISPIEL 5:

Die Zahl der Plattitüden ließe sich endlos fortsetzen, zum Abschluss noch eine besondere Stilblüte, die in der Leitlinie fett hervorgehoben wurde: "**Der Fokus der Informationssicherheit in ELGA ist auf die Besonderheit der verteilten Aufgaben, Kompetenzen und Verantwortungen zu legen.**" Was soll das heißen? Weder werden die Besonderheiten der Aufgaben, noch von Kompetenzen oder Verantwortung dargelegt.

Wenn jedoch damit gemeint ist, dass mit der jetzigen Konstruktion von ELGA kein verantwortlicher Betrieb möglich ist, dann ist dem absolut zuzustimmen.

002 - ELGA ISMS - INFORMATIONSSICHERHEITSORGANISATION

Auch diese Leitlinie beschränkt sich auf Allgmeinplätze, in unzulässiger Weise werden Ziele mit Ist-Feststellungen vermischt. Über weite Strecken finden sich bloß abstrakte Wiedergaben von Planungs- und Risikobewertungsprozessen, etwa des PDCA-Modells oder dem COBIT-Bewertungsschema.

002 - BEISPIEL 1:

Als Ziel LL02_Z5 findet sich folgende Formulierung "Eine angemessene und überprüfbare Sicherheitskultur in ELGA, der die ELGA-Benutzer vertrauen können, ist vorhanden." Das ist eine Feststellung, kein Ziel und es ist nicht erkennbar, welche Schritte zur Erreichung einer derartigen "überprüfbaren Sicherheitskultur" gesetzt werden sollen.

Gleiches gilt für die anderen "Ziele" wie "LL02_Z3 Die Leistungen, die mit Hilfe von ELGA erbracht werden können, sind patientengerecht, effizient und effektiv gestaltet." oder "LL02_Z6 Ein Notfall- und Wiederanlaufprozess liegt vor, ist etabliert und wird regelmäßig geprüft."

Statt überprüfbarer Ziele finden sich bloß Wunschdenken, formuliert als allgemeine Feststellungen.

002 - BEISPIEL 2:

Unter 5.1.3. wird eine "ELGA-Sicherheitskommission" definiert, konkrete Aufgaben sind ihr nicht zugedacht, es wird nur abstrakt ein PDCA-Zyklus dargestellt. Die Konstruktion muss als praxisfern eingestuft werden. Wenn in Zukunft tatsächlich eine Sicherheitslücke auftreten sollte und nur für diesen Ernstfall benötigt man Sicherheitskonzepte, wird dann diese Kommission abstimmen, wer daran "schuldig" ist, oder wird die Verantwortung so lange hin und her geschoben bis der betroffene Patient aufgegeben hat (oder tot ist)?

002 - BEISPIEL 3:

Als sachlich problematisch ist auch das Vorhaben unter "5.1.4 CERT" anzusehen: "Die ELGA GmbH und die ELGA-Systembetreiber haben beim Aufbau eines Computer Emergency Response Teams (E-Health CERT) mitzuwirken." Damit CERT-Einrichtungen effizient arbeiten können, benötigen sie eine Mindestausstattung von Personen und technischem Equipment und bedürfen einer ausgezeichneten internationalen Vernetzung.

Tatsächlich gibt es in Österreich schon einen Wildwuchs von Mini-Certs (cert.at und govcert, auch die A-SIT reklamiert CERT-typische Aufgaben für sich). Jede dieser Stellen (bei teilweiser personeller Überschneidung) ist ohne eigenes Budget und mit 3-4 Personen ausgestattet und damit nicht in der Lage selbständig IT-Sicherheitsbedrohungen zu erkennen, zu analysieren und gegebenenfalls zu bekämpfen. Mit Aufbau eines E-Health CERT, auch wenn sich dieses mit cert.at "abstimmen" soll, wird der Zersplitterung bloß weiterer Vorschub geleistet.

Es sollte eher auf eine europäische Koordination hingearbeitet werden. Im übrigen hat die Organisation einer unabhängigen Hilfseinrichtung nichts in der Informationssicherheitsorganisation der ELGA GmbH verloren.

Ein derartiges CERT dürfte keinesfalls durch die ELGA GmbH betrieben werden. Hier besteht bei ELGA-Sicherheitslücken ansonsten die Gefahr von Interessenskonflikten. Nicht ohne Grund schreiben Sicherheitszertifizierungen die zwingende Trennung bestimmter IT-Aufgaben, wie den operativen Bereich und die Sicherheitsüberwachung vor.

006 - ELGA ISMS - GENERELLE VORGABEN FÜR DIE NETZWERKSICHERHEIT UND RECHNERVERWALTUNG

Auch für diese Leitlinie gilt grundsätzlich das zuvor gesagte. Statt jene Punkte - Netzwerksicherheit und Rechnerverwaltung -, die Thema dieser Leitlinie sein sollten zu präzisieren, werden sie bloß nochmals in allgemeiner Form wiederholt.

Die schon unter Leitlinie 001 besonders auffällige Stilblüte Ziel "LL01_Z2" wird jetzt unter "LL006_Z5" fast wörtlich übernommen: "Die Integrität und die Verfügbarkeit von Informationen und informationsverarbeitenden Einrichtungen sind sichergestellt." Bloß die Vertraulichkeit fiel nunmehr unter den Tisch.

Andere Platitäten, wie "LL006_Z6 Die Informationen sind vor missbräuchlicher Verwendung im Netzwerk geschützt und werden überwacht.", "LL006_Z7 Die Sicherheit und die sichere Nutzung von ELGA sind gewährleistet." oder "LL006_Z8 Sicherheitsvorfälle werden erkannt, gemeldet, bearbeitet und behoben." sprechen für sich und müssen nicht weiter kommentiert werden.

Mit "Sicherheitsvorfälle werden erkannt, gemeldet, bearbeitet und behoben." wurde kein Ziel, bestenfalls Wunschdenken formuliert. Auch hier fehlen operativ nachvollziehbare Vorgaben die dieses Ziel überprüfbar machen. Sollen alle Sicherheitsvorfälle erkannt, gemeldet, bearbeitet und behoben werden? Oder 99%? Innerhalb welcher Zeit? Soll das Erkennen proaktiv oder reaktiv erfolgen usw.

DIE WEITEREN LEITLINIEN

007 - ELGA ISMS - Systemzugriffsüberwachung und Zugriffskontrolle
008 - ELGA ISMS - Beschaffung, Entwicklung und Wartung von ELGA-Komponenten und ELGA-Anwendungen

Diese Leitlinien haben, lässt man den jeweiligen Mantel weg, jeweils nur 2-3 Seiten Umfang und bestehen bloß aus einigen Allgemeinplätzen, die weder die Komplexität der "Systemzugriffsüberwachung und Zugriffskontrolle", noch der "Beschaffung, Entwicklung und Wartung" großer IT-Systeme gerecht werden.

Als Beispiel seien einige besondere Stilblüten zitiert:
- "LL007_Z1 Die Überwachung der Nutzung von ELGA ist gewährleistet.",
- "LL007_Z2 Die Protokolle zur Systemzugriffsüberwachung und die Zugriffsprotokolle der ELGA-Anwendungen sind verlustfrei, unveränderbar und vor unbefugtem Zugriff geschützt vorhanden.",
- "LL007_Z5 In ELGA sind Protokollierungen über Administrator- und Operatortätigkeiten eingerichtet und regelmäßig geprüft.",
- "LL007_Z8 Die Systemzugriffsüberwachung und die Zugriffskontrolle sind durch Anweisungen und Standards hinsichtlich Protokollierung konkretisiert.",
- "LL007_M4 Fehler sind zu protokollieren und zu analysieren und es sind entsprechende Maßnahmen zu ergreifen",
- "LL008_M1 Im Zuge der Beschaffung bzw. Entwicklung neuer ELGA-Komponenten oder ELGA-Anwendungen oder deren Erweiterung sind Anforderungen an Sicherheitsmaßnahmen zu spezifizieren." usw.

Bei allen Punkten handelt es sich um gesetzliche Vorgaben des DGS 2000, diese müssen nicht gesondert deklariert werden.

Als besonders problematisch ist LL008_M5 anzusehen: "Testsysteme, die eine Verwendung personenbezogener oder anderer sensibler Informationen erforderlich machen, unterliegen den Sicherheitsrichtlinien des Produktivsystems mit Ausnahme der Vorgaben zu Integrität, Verfügbarkeit und Konsistenz." Die Verwendung personenbezogner Daten bloß zu Testzwecken ist als berechtigter Zweck gemäß DSG 2000 nicht vorgesehen und müsste mit den Betroffenen gesondert vereinbart werden. Eine derartige Verpflichtung fehlt in den Leitlinien.

Im übrigen wird ausdrücklich darauf hingewiesen, dass es aus entwicklungstechnischer Sicht unter keinen Umständen zwingend notwendig ist, tatsächlich auf eine Person zurückführbare Daten zu Testzwecken zu verwenden. Es gibt ausreichend erprobte technische Verfahren (etwa Testgeneratoren) um die Verwendung von Echtdaten zu vermeiden.

RESÜMEE ZU DEN VORLIEGENDEN ELGA ISMS-LEITLINIEN

Wie die Informationssicherheitspolitik (ELGA ISMS Leitlinie 001) auf Seite 9 richtig wiedergibt, geht jedes Sicherheitskonzept (und im übrigen auch das europäische und das österreichische Datenschutzrecht) von der Verantwortlichkeit EINES Auftraggebers aus, der letztlich auch den Schutz der Grundrechte und der Privatsphäre der Patienten zu garantieren hat.

Doch statt die einzig sinnvolle Konsequenz zu ziehen und an dieser Stelle ein Konzept vorzulegen, wie EIN Auftraggeber ausgestattet sein müsste, um die notwendigen rechtlichen und technischen Vorgaben zu erfüllen, schwindelt sich das Papier um diese zentrale Frage herum und konstruiert ein kollektives Vertrags- und Kommissionsmodell.

Die vorliegenden Leitlinien enthalten ein Sammelsurium von Allgemeinplätzen und Standardtextbausteinen wie sie in zahllosen IT-Security-Fachbüchern zu finden sind. Die umfangreichen allgemeinen Ausführungen, etwa zu PDCA-Zyklen, Risikoanalysen und/oder IT-Sicherheit sind jedenfalls entbehrlich, sie sind in Fachbüchern besser dargestellt.

Die Papiere sind sogar in den allgemeinen Formulierungen fachlich schwach. Sie befinden sich nicht einmal am letzten Stand der Technik, u.a. wurden die spezifischen eHealth-Sicherheitsrichtlinien von ISO (=ISO 27799) ignoriert, die sich besonders mit den Sicherheitsanforderungen des Gesundheitsbereiches beschäftigen.

Die Leitlinien bleiben zwangsläufig vage und unbestimmt, da sie von keiner gesicherten Grundlage aus erstellt wurden.

NOTWENDIGE SCHRITTE ZU EINEM PRAKTIKABLEN PATIENTENAKT

Da es sich bei ELGA um ein österreichweites, flächendeckendes öffentlich-rechtliches Vorhaben handelt, bedarf es dazu zwingend eines ausreichend determinierten ELGA-Gesetzes. Dieses müsste (1) die fachlichen (medizinischen) Anforderungen für einen Patientenakt definieren, (2) die organisatorischen Rahmenbedingungen für die Erstellung und Verwendung der Akten und (3) die rechtliche Verantwortung und die berechtigten Verwendungszwecke für das gesamte System festlegen.

Ausgehend von einem derartigen Gesetz könnten durch Verordnung bestimmte technische Mindeststandards in der Dokumentation und bei der Datenverwendung definiert werden. Diese Mindeststandards müssten, jeweils am Stand der Technik angepasst, jedenfalls Vorgaben zur Verschlüsselung bei Datenübertragung, zur revisionssicheren Langzeitarchivierung, aber auch über den Inhalt und den Aufbau der Patientenakte enthalten, weiters welche Dokumentationsstandards verpflichtend zu verwenden sind und wie die Schnittstellen zwischen den technischen Systemen (z.B. bilderzeugenden Systemen, Laborsystemen, den Dokumentenverwaltungssystemen und den Anwendungen/Applikationen) auszusehen haben. Für die Funktionsweise eines flächendeckenden Patientenverwaltungssystems ist die Klärung der Interoperabilität und Schnittstellen aller Komponenten von entscheidender Bedeutung.

Erst auf Basis dieser Verordnungen lassen sich Pflichtenhefte definieren, die im Zuge einer öffentlichen Ausschreibung zu vergeben wären.

Diese drei Schritte Gesetzgebung, Erlass von Verordnungen und Durchführung von Ausschreibungen sind jedoch klassische hoheitliche Aufgaben und können nicht an eine GmbH delegiert werden.

Im Zuge der Ausschreibung müssten dann von den Bietern Sicherheitskonzepte und Sicherheitsleitlinien verlangt werden. Diese sind Voraussetzung zur Beurteilung der Zuverlässigkeit eines Anbieters. Üblicherweise werden Anbieter, die sich an derartig großen Projekten beteiligen, Zertifizierungen durch Dritte vorlegen können (z.B. ISO 27001 oder BSI-Grundschutz, ...). Im Zuge dieser Zertifizierungen wurden die unternehmensinternen Leitlinien geprüft, die ausschreibende Stelle hat nur dafür zu sorgen, dass diese Leitlinien dann auch in ihrem Projekt (bei ELGA) angewandt werden.

Wenn die ELGA GmbH Leitlinien erstellt, ist deren Funktion völlig unklar, das Pferd wird quasi von hinten aufgezäumt. Soll die ELGA GmbH die hoheitlichen Aufgaben übernehmen? Wenn ja, welche? Sollen operative Aufgaben übernommen werden? Marktregulierungsaufgaben, analog der RTR bzw. der E-Control? Oder soll die ELGA GmbH mit Verordnungsermächtigung ausgestattet werden?

Die international bei Großprojekten übliche strikte Trennung von Teilprozessen, wie (a) Definition der Zielvorgaben, (b) Definition eines Pflichtenheftes, (c) Ausschreibung und Angebotsprüfung, (d) Projektumsetzung, (e) Projektbetrieb und (f) laufende Kontrolle fehlt bei der derzeitigen ELGA-Konzeption völlig. Schon die wenigen verfügbaren ISMS-Leitlinien + den laut Inhaltsverzeichnis weiteren geplanten Leitlinien, zeigen eine Vermischung planerischer, operativer und kontrollierender Aufgaben, die alle durch die ELGA GmbH erledigt werden sollen.

Im wohlmeinendsten Fall wurde mit der ELGA GmbH eine Schulungsfirma für herangehende IT-Referenten geschaffen, in der Datenverarbeitung auf Steuerkosten geübt wird.

Leider ist zu befürchten, dass mit der ELGA GmbH - als klassische österreichische Lösung - eine kompetenzlose Koordinationsstelle geschaffen werden soll, die zwar alle Teilprozesse eines Großprojekts besetzt, aber gegenüber den tatsächlich Verantwortlichen im Gesundheitswesen (den Bundesländern und den Sozialversicherungsträgern) keinerlei Kompetenzen hat und bloß Empfehlungen aussprechen kann.

Weder "ISMS-Beauftragter" (5.1.1.), "ISMS-Koordinator" (5.1.2.) noch "ELGA-Sicherheitskommission" (5.1.3.) können laut Leitlinie 002 - ELGA ISMS - Informationssicherheitsorganisation direkt in ELGA-Systeme eingreifen und Sicherheitslücken abstellen, sie können bloß Berichte dazu verfassen und Empfehlungen abgeben.

Diese Konstruktion, ist sowohl praxisfremd, als auch EU-vertragswidrig. Derartige öffentliche Großprojekte sind zwingend öffentlich auszuschreiben. Vor Abschluss der zwingenden Vorarbeiten (Gesetzgebung, Erlass von Verordnungen und Durchführung von Ausschreibungen) sollte jedenfalls die Tätigkeit der ELGA GmbH eingestellt werden.

AUSBLICK

Soll ein Patientenaktensystem in Österreich funktionieren UND akzeptiert werden, dann braucht es klare Verantwortlichkeiten durch einen geeigneten Betreiber, der für alle Dokumentationsfragen eines Patienten zuständig ist und kein Verschleierungsmodell. Das Bundesministerium für Gesundheit ist daher gefordert den derzeitigen Unfug zu stoppen und mit einer geordneten Neukonzeption das Vertrauen aller Beteiligten wieder zu gewinnen.

Die bisherigen Millionen-Kosten sind nur Peanuts gegenüber den weiteren Kosten, wenn auf dieser dilettantischen Ebene weiter gearbeitet wird. Es wäre sinnvoll die Grundlagen eines Patientenaktensystems vorrangig durch die direkt Betroffenen formulieren zu lassen (GDAs, Patienten/Patientengruppen +

Patientenvertreter, Ethikeinrichtungen und Grundrechtsexperten), dann daraus ein Gesetz zu formulieren und dann erst die Techniker, Informatiker, IT-Unternehmen, Controller usw. ranzulassen. ELGA könnte dann ein nützliches Patientensystem sein und nicht, wie im Gesetzesentwurf formuliert, ein Förderprojekt zur Stärkung des (IT-)Wirtschaftsstandortes Österreich.