Hans G. Zeger[1],

Datenschutz- und Datensicherheit zum ELGA-Ministerratsentwurf 7.10.2012

Die vorliegenden Anmerkungen konzentrieren sich auf Datenschutz- und Datensicherheitsfragen zum ELGA-Entwurf. Die Gesamtkonzeption ist weiterhin missglückt, unklar und in vielen Punkten widersprüchlich. Die durch das DSG 2000 erforderliche klare Zweckdefinition und Trennung unterschiedlicher, teilweise entgegengesetzter Zwecke wird im ELGA-Entwurf missachtet. Sanierbar ist das Gesetz nur durch eine grundlegende Designänderung, die die verschiedenen Verwendungszwecke der Gesundheitsdaten sauber trennt und unterschiedlich regelt. Im letzten Abschnitt wird - in Stichworten - skizziert, wie eine deratige, datenschutz- und damit verfassungskonforme Gesamtkonzeption in der Verwendung der Gesundheitsdaten aussehen könnte.

1. Anmerkung zur Gesamtkonzeption von ELGA

Das Design-Konzept von ELGA bleibt fehlerhaft, es vermischt unterschiedlichste Zwecke und wird dadurch unnötig unklar und komplex.

Das DSG 2000 geht von klar definierten Zwecken aus, jeder Zweck entspricht einer eigenen Datenanwendung. Die Datenanwendung muss so gestaltet sein, dass sie nicht mit anderen unvereinbaren Zwecken in Konflikt kommt.

Genau diese Trennung verabsäumt jedoch ELGA, es vermischt (auch im letzten Entwurf) mehrere, widersprüchliche Zwecke. Daraus entsteht ein zu komplexes, sicherheitstechnisch nicht administrierbares System, mit teils zu vielen Daten, zu vielen Zugriffsberechtigten und teils zu starren Speicher- und Löschungsfristen.

Folgende Zwecke sollten exakter unterschieden und getrennt behandelt werden. In Stichworten werden wesentliche Designkomponenten genannt. Selbstverständlich sind in allen Fällen Identitätsregeln, Rollekonzepte, Vertraulichkeits- und Integritätsregeln, Vorgaben zu einem Berechtigungssystem und Protokollierungsverpflichtungen zu beachten.

- aktuelle Behandlung(en):
Hier ist sicher zu stellen, dass alle behandelnden Stellen alle unmittelbar zur Behandlung notwendigen Daten erhalten.
Eckpfeiler: gerichtete Kommunikation, Zustimmung erfolgt im Rahmen des Behandlungsverhältnisses, keine Ausnahmen bei den Daten, Daten sind personenbezogen (Patient und Arzt) zu verwenden, Datenverkehr hat verschlüsselt stattzufinden.

- Dokumentation von abgeschlossenen Behandlung(en), Beweissicherung:
Die Archivierung hat direkt bei jeder behandelnden Stelle zu erfolgen, die Ablage erfolgt dezentral und verschlüsselt, zentral ist - wenn überhaupt bloß

1 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)

ein Verweis auf Ort, Zeit und Umfang der Behandlung (z.B. auf die Entlassungsdiagnose) erforderlich ist.
Eckpfeiler: keine Zustimmung erforderlich, keine Ausnahmen bei den gesicherten Daten, Daten sind personenbezogen (Patient und Arzt) zu speichern.

- Patienteninformation:
Zusammenführung bisheriger Patientendaten zu einem Gesundheitsakt (die klassische ELGA-Aufgabe) für zukünftige Behandlungen.
Eckpfeiler: erfolgt auf freiwilliger Basis (auf Wunsch des Patienten), alle Daten werden in einen Akt übernommen, aber Patient kann Inhalt gestalten, z.B. Teile entfernen, Sperren usw. Die Speicherung erfolgt an einer Stelle, die der Patient vorgibt, Speicherung erfolgt verschlüsselt (Zugang nur für Patient + vom Patient nominierte Vertrauenspersonen), keine Ausnahmen bei den übernommenen Daten, aber Patient kann Unterlagen entfernen, kommentieren, aktualisieren. Daten sind personenbezogen (Patient und Arzt) zu speichern, Patient stellt bei nächster Behandlung Unterlagen dem Arzt zur Verfügung (in welcher technischen Form auch immer), technische Standards und Strukturierungen der Daten bzw. der Teilbereiche (Notfall, Medikation, ...) sollte Gesetz regeln.

- Qualitätssicherung, Planung, Optimierung:
Eigener strukturierter Datenbestand für Kontroll- und Planungsaufgaben
Eckpfeiler: Verpflichtend, aber bezüglich der Patienten nicht personenbezogen, enthält nicht alle Daten, sondern nur jene Diagnose-, Leistungs- und Verschreibungsdaten, die aufwands-, prüf- und ergebnisrelevant sind. Zentrale Speicherung, Grundlagen der Datenstrukturen und zulässige Auswertungen sollten per Gesetz geregelt werden, Details, abhängig von der medizinischen Entwicklung und den Erfahrungen, sollten in Verordnungen nachgebessert werden.

Diese vier Datenanwendungen sollten sowohl datenschutzrechtlich, als auch sicherheitstechnisch getrennt behandelt werden, dies insbesondere wegen:
- unterschiedlichem Datenumfang
- unterschiedlicher Zugriffserfordernisse
- unterschiedlicher rechtlicher Relevanz (Haftung)
- unterschiedlicher Sensitivität
- unterschiedlicher Speicherdauer
- unterschiedlicher Verfügungsrechte (Patient, GDA)
- ...

Erst eine klare Trennung der verschiedenen Verwendungszwecke von Gesundheitsdaten und eine unterschiedliche rechtliche Behandlung, lässt ein sinnvolles ELGA-Gesetz erwarten.

2. EINZELNE BESTIMMUNGEN IM ELGA-ENTWURF

(1) § 2 Z 1 "GESUNDHEITSDATEN", Z 9 "ELGA-GESUNDHEITSDATEN"

Weiterhin unbestimmte Formulierungen, wie "Erhebung der Ursachen für diese Befindlichkeiten" oder "Sicherung der Versorgungskontinuität ... wesentlich sein könnten"

"Sicherstellung der Behandlungsqualität für erforderlich erachtet"
Erfordert geradezu hellseherische Fähigkeiten beim GDA, was in Zukunft wesentlich sein wird.

Weiterhin unklarer Begriff "Geheimnisse": Was soll das sein? Daten? Informationen? Meinungen? ... DSG kennt nur Daten

(2) § 2 Z 11 "ELGA-Systempartner"

Definition der ELGA-Systempartner
Zwar für vieles zuständig, aber nicht im Sinne des DSG verantwortlich. Weiterhin keine Gesamtverantwortlichkeit ("Auftraggeber") für ELGA im Sinne des DSG definiert.

(3) § 3 Abs. 2 "Datensicherheit" - Ausnahme

".... wenn durch effektive und dem Stand der Technik entsprechende Datensicherheits- und Kontrollmaßnahmen unbefugte Dritte vom Zugriff auf Gesundheitsdaten und somit deren Kenntnisnahme ausgeschlossen werden können."
Bisher problematische Ausnahme wird noch mehr aufgeweitet. Was bedeutet "entsprechende"? Unklar, wie das "und" zu verstehen ist, können Kontrollmaßnahmen alternativ zu Sicherheitsmaßnahmen gesetzt werden oder müssen sie zussätzlich gesetzt werden? Was sollen diese sein?
Sinnvoller wäre es, die Verpflichtungen zum sicheren Datentransfer auch für die interne Datenspeicherung anzuwenden und beides praxisgerecht, aber ohne Ausnahmen zu formulieren.

(4) § 3 Abs. 3 "Datensicherheit"

"Die Zulässigkeit Gesundheitsdaten zu verwenden ist mittels Rollen abzubilden. Gesundheitsdiensteanbieter haben technisch zu gewährleisten, dass es keine Verwendung von Gesundheitsdaten außerhalb der zulässigen Rollen gibt."
Problematische Verpflichtung einer rein technischen Umsetzung der Zugriffsrechte auf Gesundheitsdaten. Gibt es in keiner betrieblichen IT-Praxis, realisiert wird immer Verbindung von technischen und organisatorischen Maßnahmen. Absatz steht im Widerspruch zu Abs. 2, der eben auch "Kontrollmaßnahmen" zulässt.

(5) § 4 Abs. 6 "Identität / bPK"

Verwendung des Gesundheits-bPKs für private GDAs
Es widerspricht dem Datenschutzkonzept des E-Gov-Gesetzes, wenn behördliche bPKs nunmehr auch für privatwirtschaftliche Aspekte verwendet werden. Damit wird das gesamte bPK-Konzept überflüssig.

(6) § 5 Rolle

Verordnungsermächtigung des BMG
Es fehlen gesetzlich formulierte Grundzüge, welche Art von Rollen per Verordnung festgelegt werden sollen.
Das Rollenkonzept ist zentral für den ELGA-Entwurf und definiert letztlich in welchem Umfang auf Patientendaten zugegriffen werden darf und wie weit das Arztgeheimnis und die Geheimhaltung nach § 1 DSG (Verfassungsbestimmung) letztlich durchlöchert wird. Das kann nicht komplett in eine Verordnungsermächtigung ausgelagert werden.

(7) § 6 Vertraulichkeit

Vertraulichkeit soll durch alternative Konzepte umgesetzt werden

Die in Abs. 1 Z 1 und Z 2 formulierten Vertraulichkeitsalternativen sind unnötig und führen letztlich zu Unklarheiten, welche Sicherheitstechniken tatsächlich angewandt wurden. Am Ende wird immer irgendeine Mischung von allem vorkommen. Die Unterscheidung ist zusätzlich problematisch, als für den GDA-internen Datenverkehr (§ 3 Abs. 2) der gesamte Abschnitt NICHT anzuwenden ist und damit nicht einmal die Minimalanforderung aus § 6 Abs. 1 Z 1 anzuwenden wäre.

(8) § 7 Abs. 2 Integrität - Ausnahmebestimmungen

keine Integritätsprüfung im Fall gesicherter Netzwerke

Auch hier sind die Ausnahmebestimmungen zur Integritätssicherung unverständlich und unnötig. Weiters ist darauf hinzweisen, dass sich auch in gesicherte Netzwerke (etwa bei einem größeren Spital) unbefugte Personen Zutritt und Zugriff verschaffen können, die dann überhaupt nicht mehr erkennbar wären. Besonders im Spitalsalltag mit hoher Besucherfrequenz ist es völlig unrealistisch alle Zugangsstellen wie in geschlossenen Betrieben abzusichern.

Hinzu kommt, dass GDA-intern der gesamte § 7 nicht gelten soll, also Ausnahmen von Ausnahmen gemacht werden. Bedenkt man, dass Gesundheitsdaten längere Zeit gesichert werden sollen und sich Netzwerktopologien ändern können, wäre nach einiger Zeit nicht mehr zuverlässig nachvollziehbar, unter welchen Bedingungen tatsächlich die Integrität einzelner Daten gesichert wurde.

Der durchgängige Schutz aller Gesundheitsdaten durch fortgeschrittene Signatur ist sowohl wirtschaftlich, als auch technisch leicht umzusetzen. Es sei nur daran erinnert, dass seit 1.1.2012 alle elektronischen Amtsschreiben mit einer fortgeschrittenen Signatur zu versehen sind. Dies muss umso mehr für sensible Daten gelten, die langfristige (haftungs)relevanz haben. Und selbstverständlich auch GDA-intern.

(9) § 8 Abs. 1 IT-Sicherheitskonzept

Verweis auf Sicherheit gemäß § 14 DSG 2000

Schon unter § 3 werden Sicherheitsgrundsätze angekündigt. Tatsächlich enthalten sie aber nur Sicherheitsausnahmen (siehe oben). Auch in § 8 finden sich weder Konzept noch Grundsätze, sondern bloß Verweise auf § 14 DSG 2000. Dieser Verweis ist jedoch überflüssig, da bestehende Gesetze sowieso einzuhalten sind.

Sinnvoll wären in diesem Abschnitt (a) klare Mindeststandards zur IT-Sicherheit inkl. Audit- und Prüfermächtigungen und (b) eine Verordnungsermächtigung, wie Dokumentationsformulare auszusehen haben, welche Sicherheitsstandards, Risikobewertungen und Maßnahmenkataloge diesen Mindeststandards entsprechen, auch welche Auditverfahren erforderlich sind usw.

(10) § 8 Abs 2 IT-Sicherheitskonzept / Standardformulare

Festlegung von Formularen durch Standesvertretungen

Die Ermächtigung einzelner Interessensvertreter zur Erstellung von Formularen mag zwar den Standesinteressen entgegen kommen, bringt diese aber auch in ein Dilemma. Die Standesvertretungen werden sich an möglichst einfachen Lösungen orientieren, diese müssen aber nicht sicherheitstechnisch optimal sein.

Es ist gerade die Aufgabe eines Gesetzgebers bei möglichen Interessenskonflikten durch klare Vorgaben gesellschaftspolitische richtige Weichen zu stellen. Genau diesen Anforderungen verweigert sich jedoch das BMG bzw. der Entwurf (siehe oben, § 8 Abs. 1 IT-Sicherheitskonzept).

(11) § 8 Abs 3 IT-Sicherheitskonzept / Dokumentation

Ist eigentlich eine Themenverfehlung, hier wäre festzulegen, wie und durch wen (in welcher Dichte) Zugriffe überprüft werden und welche Konsequenzen missbräuchliche Zugriffe nach sich ziehen.

(12) § 13 Abs 5 Allgemeine Bestimmungen

Hier wird auf "gebotene Sicherheitsanforderungen" verwiesen, die jedoch im gesamten Gesetz nicht definiert sind und die wenigen verstreuten Hinweise sind durch Ausnahmen und Alternativregelungen unklar formuliert.

(13) § 13 Abs 6 Allgemeine Bestimmungen / technische Parameter

"Die ELGA-Systempartner und die ELGA-Gesundheitsdiensteanbieter, gegebenenfalls vertreten durch die jeweilige gesetzliche Interessenvertretung, haben nach jeweiliger Betroffenheit, unter Beachtung der wirtschaftlichen Vertretbarkeit sowie dem Stand der Technik, Parameter, die für die Benutzer- und Anwenderfreundlichkeit von wesentlicher Bedeutung sind, gemeinsam festzulegen. ***Die dafür relevanten und technischen Fragen und Parameter sind vor der Festlegung mit der Wirtschaftskammer Österreich abzustimmen.****"*

Dass die Beteiligten miteinander reden ist wohl selbstverständlich, enthebt aber nicht den Gesetzgeber bzw. den Bundesminister am Ende klare System-Entscheidungen zu treffen. Dass de facto die WKO die Letztentscheidung zur Gestaltung des ELGA-Systems hat, ist geradezu grotesk.

(14) §16 Abs. 1 Z 2 lit a Rechte Teilnehmer/innen - Löschung

"... löschen; falls das Löschen auf Grund anderer gesetzlicher Dokumentationsverpflichtungen oder § 22 Abs. 5 Z 1 ausgeschlossen ist, sind die Verweise für ELGA unzugänglich zu machen, ..."

Unklare und widersprüchliche Löschungsverpflichtung. Kern des ELGA-Konzepts ist, dass es keine zentralen Gesundheitsdatenspeicher gibt, sondern nur Verweise darauf. Im Falle der eMedikation wird ein eigener zentraler Datenbestand aufgebaut, der aber keinen Einfluss auf die Behandlungsdokumentation beim GDA selbst hat. Es ist daher nicht nachvollziehbar, warum eine Löschung der ELGA-Verweise bzw. der zentralen Medikationsdaten nicht immer möglich sein soll.

Die Passage ist ein Musterbeispiel dafür, dass offensichtlich unterschiedlichste Verarbeitungszwecke miteinander vermengt und gemeinsam geregelt werden und damit keine klare Datenverwendungsstruktur möglich ist (Alternativlösung siehe Anmerkung zur Gesamtkonzeption von ELGA)

(15) § 16a e-Medikation

Zentrale Speicherung der E-Medikationsdaten

Da in dieser Datenbank auch nachvollziehbar bleiben muss, warum ein Medikament verschrieben wurde, obwohl Unverträglichkeiten festgestellt wurden, werden auch Diagnosen und Therapien aufgenommen werden müssen. Das sonstige ELGA-System ist als reines Verweissystem konzipiert. Die Abgrenzung welche Daten noch für die Nachvollziebarkeit der E-Medikation zentral übernommen werden müssen und welche nicht ist nicht geregelt und wird in der Praxis auch schwer zu treffen sein. Auch dieser Punkt ist ein Beispiel für die Fehlkonzeption des ELGA-Systems, das die verschiedenen Verwendungszwecke nicht korrekt trennt.

(16) § 18 Abs. 9 Löschung Daten Verstorbener

Löschung der Daten von Verstorbenen nach 10 Jahren
Die Frist von 10 Jahren ist völlig willkürlich gewählt. Entweder wird diese Frist klar begründet oder sie ist durch "unverzüglich" nach dem Tod des ELGA-Teilnehmers zu ersetzen.

(17) § 20 Abs. 1 Speicherung von ELGA-Gesundheitsdaten - Änderung

"Bereits gespeicherte ELGA-Gesundheitsdaten dürfen nicht geändert werden. Treten Umstände hervor, die eine maßgebliche Änderung des Behandlungsverlaufs bedingen können, ist zusätzlich eine aktualisierte Version zu speichern."
Diese Passage zeigt geradezu exemplarisch in welch ausweglose Situation sich die ELGA-Autoren manövriert haben. Für den einen Zweck ("Beweissicherung", Haftung) darf keinerlei nachträgliche Änderung stattfinden, für andere Zwecke (aktueller Überblick über die Patientengeschichte) sind Aktualisierungen geradezu unerlässlich.
Die von den Autoren vorgeschlagene Lösung, mehrere Versionen abzuspeichern bläht das System unnötig auf, macht Abfragen und Zugriffe schwieriger und bringt GDAs bei neuen Behandlungen in neue Haftungsprobleme (welche Version gilt tatsächlich?). Sinnvoller wäre eine klare Trennung zwischen Beweisdokumentation (nur bei der behandelnden Stelle aufbewahrt) und einer laufend aktualisierten Patienteninformation (nur bei einer vertrauenswürdigen zentralen Stelle aufbewahrt).

(18) § 20 Abs 3,4 Speicherung von ELGA-Gesundheitsdaten - Löschung

Einerseits werden starre Löschungsfristen vorgegeben und andererseits unverständliche Löschungsausnahmen definiert.
Die starren Löschungsfristen erscheinen angesichts der vielfältigen Krankheitsverläufe ziemlich praxisfern, zu den Löschungsausnahmen ist auf (siehe Anmerkungen zu §16 Abs. 1 Z 2 lit a Rechte Teilnehmer/innen - Löschung).

(19) § 21 Berechtigungssystem

Das Berechtigungssystem erlaubt individuelle Anpassungen (auch zeitlich begrenzt, auch begrenzt auf bestimmte GDAs) durch den ELGA-Teilnehmer.
Es ist jedoch fraglich, ob bei der sehr großen Zahl von ELGA-Teilnehmern, GDAs und Gesundheitsdokumenten und dem langen Zugriffszeiträumen eine sinnvolle, sichere und auch jederzeit nachvollziehbare Dokumentation, wer wann zu welchem Zweck auf Dokumente zugegriffen hat, welche tatsächlich freigegeben waren und welche sonstigen technischen Zugriffs/Zugangsbeschränkungen zu einem bestimmten Zeitpunkt existierten.
Weltweit ist kein sicheres System bekannt, dass diese komplexen Fragen zuverlässig über lange Zeiträume beantworten kann. Es ist eher zu befürchten, dass diese rechtliche Regelung - begründet mit technischen Machbarkeitsargumenten - schlicht nicht umgesetzt wird.
Die Berechtigungsfragen ließen sich wesentlich einfacher lösen, wenn dem ELGA-Teilnehmer ein eigenes ELGA-Informationssystem bereit gestellt wird, in dem er seine Gesundheitsdokumente in Form einer strukturierten Mappe zusammenstellen kann und bei dem er entscheidet, welcher GDA im Behandlungsfall tatsächlich zugreifen darf.

(20) § 22 Abs. 2 Protokollierungssystem

"*Jede Verwendung von ELGA-Gesundheitsdaten im Rahmen von ELGA ist gemäß § 14 DSG 2000 zu protokollieren mit: ...*".

Die Formulierung ist in sich widersprüchlich. "Jede Verwendung" würde bedeuten, dass jeder Zugriff (auch jedes Lesen) der ELGA-Daten protokolliert wird, "gemäß § 14 DSG 2000" - dieser besagt de facto das Gegenteil. § 14 verlangt eine Protokollierung nur insoweit, dass Verwendungen "im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können".

Der ELGA-Entwurf suggeriert, dass ein ELGA-Teilnehmer jede Verwendung nachvollziehen kann, also auch rechtmäßige Verwendungen, während die Protokollierungspflicht nach DSG 2000 § 14 bloß ein Schutz vor unrechtmäßiger Verwendung darstellt. Ist der Zugriff durch Zugriffsprofile von vornherein nur auf berechtigte Personen beschränkt, wäre eine Protokollierung nach § 14 DSG 2000 nicht erforderlich, aus Dokumentationsgründen für den ELGA-Teilnehmer jedoch sehr wohl.

(21) § 27 Abs. 10 Z 1-3 Übergangsbestimmungen - Identitätsfeststellungen

Zur Prüfung von Identität, Rollen oder Integrität soll es - bei mangelnder Infrastruktur - ausreichen, durch telefonischen, persönlichen oder vertraglichen Kontakt Zugang zu ELGA-Daten zu erhalten.

Diese Bestimmung ist in sich widersprüchlich. Fehlt eine geeignete technische Infrastruktur, dann gibt es auch keine Zugangsmöglichkeiten zu den ELGA-Gesundheitsdaten und die Ausnahmebestimmung erübrigt sich.

Diese Bestimmung ist geradezu eine Einladung ein Parallelsystem zu schaffen - wie es auch bisher trotz GTelG existiert - in der zwar die Gesundheitsdaten ausgetauscht werden, die erforderlichen technischen Grundlagen für Identitäts-, Rollen- oder Integritätsprüfung nicht umgesetzt werden. Damit besteht die Gefahr, dass an sich auszuschließende GDAs (weil Berechtigungsvoraussetzungen nicht mehr gegeben sind) über diesen Umweg weiter zugreifen können.

(22) § 27 Abs. 10 Z 4 Übergangsbestimmungen - Verzeichnisse

Zur Prüfung von Identität, Rollen oder Integrität sollen diverse Verzeichnisse herangezogen werden.

Identität, Rollen oder Integrität stellen die zentralen Eckpfeiler zu ELGA dar, diese absolut sicher zu gewährleisten ist entscheidend für das Funktionieren. Es wird jedoch nicht ausreichend klar festgehalten welche Verzeichnisse mit welchen Qualitäts- und Sicherheitsstandards tatsächlich herangezogen werden sollen.

Es muss ausdrücklich darauf hingewiesen werden, dass offenbar geplant ist, Verzeichnisse, die für andere Zwecke erstellt/verwendet wurden jetzt zu einem neuen Zweck (ELGA) zu verwenden. Dazu ist es aber notwendig die Anforderungen (etwa in Hinblick auf Aktualität) anzupassen.

So kann ein es ausreichend sein, dass ein Berufsverzeichnis, das zur Nachschau dient, ob jemand noch tätig ist, wöchentlich oder monatlich aktualisiert wird. Dasselbe Verzeichnis, das jedoch direkte Zugriffsrechte auf sensible Daten einräumt, muss jedoch sekundenaktuell zu einer Sperre führen, wenn jemand aus Datenmissbrauchsgründen vom Zugriff ausgeschlossen werden soll.

Sicherheitstechnisch sinnvolle Benutzerverzeichnisse können nur zentral geführt und gewartet werden.

3. ZUSAMMENFASSUNG DER DATENSCHUTZ- UND DATENSICHERHEITSASPEKTE

Der ELGA-Entwurf enthält zahlreiche Aspekte und Komponenten, die für ein sicheres IT-System wesentlich sind, u.a. Identitätsregeln, Rolle, Vertraulichkeits- und Integritätsregeln, Vorgaben zu einem Berechtigungssystem und Protokollierungsverpflichtungen.

Keine der Komponenten ist jedoch verbindlich für das Gesamtsystem festgelegt, es bestehen zu viele Ausnahmen. Zum Teil ist die Funktionalität der Komponenten widersprüchlich formuliert. Zum Teil werden durch "Übergangsbestimmungen" geradezu Umgehungskonzepte gesetzlich nahegelegt. Das Berechtigungssystem und die Protokollierungsverpflichtungen sind praxisfern und zu komplex formuliert.

Die Verweise auf die Sicherheitsbestimmungen des § 14 DSG 2000 bzw. die Abschnitte "Grundsätze der Datensicherheit" und "IT-Sicherheitskonzept" erschöpfen sich in Pauschalformulierungen und Leerformeln.

Der Entwurf lässt ein nachvollziehbares Gesamt-Sicherheitskonzept vermissen. Die wesentlichsten Gründe für diesen Mangel sind

(a) der Versuch unterschiedlichste Verwendungszwecke zu verknüpfen und gemeinsam zu regeln,
(b) die Weigerung der Gesetzes-Autoren einen für ELGA tatsächlich verantwortlichen Auftraggeber (im Sinne des DSG 2000) festzulegen und
(c) ein im Grundsatz missglücktes Datendesign, das zunehmend zu einer undurchschaubaren Vermischung zentraler und dezentraler Komponenten wird.