MINISTERIUM FRAUEN GESUNDHEIT

Dr.in Pamela Rendi-Wagner, MSc
Bundesministerin

Frau
Präsidentin des Nationalrates
Doris Bures
Parlament
1017 Wien

GZ: BMGF-11001/0197-I/A/5/2017

Wien, am 28. Juni 2017

Sehr geehrte Frau Präsidentin!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 12993/J der Abgeordneten Ing. Norbert Hofer, Dr. Dagmar Belakowitsch-Jenewein und weiterer Abgeordneter** nach den mir vorliegenden Informationen wie folgt:

Eingangs ist festzuhalten, dass zur gegenständlichen parlamentarischen Anfrage eine Stellungnahme der ELGA GmbH eingeholt wurde.

Frage 1:

- *Wieso wurde keine zentrale Benutzerverwaltung für alle ELGA-berechtigten Anwender eingeführt?*

Das ELGA-Berechtigungssystem ist ein zentraler Baustein von ELGA. Jeglicher Zugriff auf die elektronische Gesundheitsakte ELGA kann nur nach Prüfung im ELGA-Berechtigungssystem erfolgen. Hierbei erfolgt auch ein Abgleich der verwendeten Identität mit dem zentralen Gesundheitsdiensteanbieter-Index (§ 19 GTelG 2012). Die Organisation der konkreten Benutzerverwaltung setzt aus Gründen der Zweckmäßigkeit und Wirtschaftlichkeit auf bereits bestehenden Strukturen auf (§ 10 GTelG 2012). Die in § 22 GTelG 2012 festgelegte Pflicht zur Protokollierung des Namens der natürlichen Person, die die ELGA-Gesundheitsdaten tatsächlich verwendet hat, ist zudem als wesentliche Maßnahme der Datensicherheit zu betrachten, da sie eine inhärent präventiv-abschreckende Wirkung hat.

Fragen 2, 3 und 5:

- *Weshalb wurde bisher keine verpflichtende separate Authentifizierung beim Einstieg in ELGA durch jeden ELGA-User eingeführt?*
- *Warum wurde bisher keine starke Zweifaktor-Authentifizierung, z. B. über die Verwendung von Hardware-Token plus PIN, verwendet?*
- *Warum werden Kontaktbestätigungen nicht nur nach erfolgter Zweifaktor-Authentifizierung angelegt?*

Laut GTelG 2012 muss jeder Zugriff auf ELGA-Gesundheitsdaten personenbezogen, zuordenbar und nachvollziehbar erfolgen. Bereits dieses Faktum erhöht die Datensicherheit in Spitälern massiv: Bisher vereinzelt verwendete „Sammeluser", wie etwa „Chirurgie" für das gesamte chirurgische Team, sind dank ELGA nicht mehr zulässig. Eine Zwei-Faktor-Authentifizierung – analog zur Authentifizierung der Bürgerin bzw. des Bürgers am ELGA-Portal mittels Bürgerkarte/Handysignatur – wäre prinzipiell auch seitens der ELGA-Gesundheitsdiensteanbieter möglich, ihre Umsetzung ist jedoch mit beachtlichen Aufwänden und Eingriffen in die etablierten Prozesse verbunden. Die Verantwortung für die Einführung einer Zwei-Faktor-Authentifizierung obliegt daher dem betreffenden ELGA-Gesundheitsdiensteanbieter bzw. dessen Rechtsträger (z. B. Spitalsbetreiber). Zur Gewährleistung des geforderten Sicherheitsniveaus wurde demzufolge entschieden, zumindest durch entsprechende Vorgaben beim Passwort-Login die Sicherheit weiter zu erhöhen.

Frage 4:

- *Warum gibt es bisher keine Autorisierung von Batch-Jobs durch eine natürliche Person mittels Zweifaktor-Authentifizierung?*

Diese Frage ist in sich widersprüchlich, da es die Intention bei der Einrichtung eines „Batch-Jobs" ist, diesen automatisiert durchzuführen. Die Einrichtung von Batch-Jobs ist ausschließlich durch dafür autorisierte und persönlich identifizierte Administrator/inn/en möglich und zulässig.

Frage 6:

- *Wäre das Stecken der e-Card nicht auch bei Ombudsstellen notwendig?*

Wie im ELGA-Gesetz (§ 17 Abs. 4 GTelG 2012) und den diesbezüglichen Erläuterungen festgelegt ist, kommen bei der ELGA-Ombudsstelle die Mechanismen gemäß § 5 Abs. 3 E-Government-Gesetz zur Anwendung. Das bedeutet, dass bei der ELGA-Ombudsstelle eine Zweifaktor-Authentifizierung mittels Bürgerkartenfunktionalität verwendet wird.

Frage 7:

- *Warum wurde bisher keine flächendeckende digitale Signatur von Gesundheitsdokumenten eingeführt?*

Durch die Einführung von ELGA wurden die Voraussetzungen für das digitale Signieren von Gesundheitsdokumenten wesentlich vorangetrieben. Es dürfen nur ärztlich vidierte/validierte Befunde in ELGA registriert werden. Für ein korrektes ELGA-Gesundheitsdokument, das die Anforderungen der Clinical Document Architecture (CDA) erfüllt, ist die Angabe einer/eines inhaltlich Verantwortlichen zwingend erforderlich, diese Informationen sind auch in ELGA enthalten. Die Umsetzung der konkreten Berechtigung für das Vidieren liegt – wie schon bisher – in der Verantwortung der einzelnen Krankenanstalt bzw. des einzelnen Labor- und Röntgeninstitutes. Die Einführung einer flächendeckenden elektronischen Signatur für alle Gesundheitsdokumente würde jedenfalls für den niedergelassenen Bereich die Ausstattung mit den im Signatur- und Vertrauensdienstegesetz (SVG) vorgesehenen Einrichtungen erforderlich machen. Seitens der ELGA GmbH wurde und wird in diesem Zusammenhang auf die bisherigen guten Erfahrungen mit der schrittweisen Einführung von ELGA und dem damit einhergehenden Austausch von best practice-Modellen unter den anwendenden Einrichtungen hingewiesen. Solche Maßnahmen erfordern zumeist auch eine Anpassung (Integration) vorhandener Softwareprodukte, die schon aus ökonomischen Gründen mit der Weiterentwicklung des Produkts selbst einhergehen sollte. Eine ähnliche Herangehensweise wird auch für die flächendeckende Einführung der digitalen Signatur von Gesundheitsdokumenten empfohlen.

Fragen 8 und 9:

- *Ist eine regelmäßige Information an Patienten über sie gespeicherte Daten und deren Abrufe (z. B. über e-Mail oder SMS ("Push Service")) künftig vorgesehen?*
- *Ist es vorgesehen künftig Informationen an Patienten über erfolgte Kontaktbestätigungen (z. B. über e-Mail oder SMS ("Push Service")) weiter zu geben?*

ELGA bietet jeder Patientin/jedem Patienten die Möglichkeit, jederzeit im Wege des ELGA-Portals einfach und sicher Kenntnis davon zu erlangen, welche ELGA-Gesundheitsdaten (z. B. ärztlicher Entlassungsbrief) in ELGA zur Verfügung gestellt wurden und wer wann darauf zugegriffen hat. Ersatzweise wird dies den Betroffenen, die über keine entsprechende technische Ausstattung oder Kenntnisse verfügen, über die ELGA-Ombudsstelle ermöglicht. Die Errichtung eines „Push-Services“ wäre technisch möglich, wenngleich finanziell und organisatorisch aufwändig (z. B. Pflege der Kontaktdaten). Es wurde daher davon Abstand genommen, weil etwa chronisch kranke Personen, für die häufiger ELGA-Dokumente entstehen bzw. auf deren ELGA-Dokumente unterschiedliche behandelnde ELGA-GDA zugreifen, dann von Push-Nachrichten „überschwemmt“ würden.

Fragen 10 und 11:

- *Werden im gesamten Projekt ELGA Dienstleistungen an externe Unternehmen ausgeschrieben und vergeben?*
- *Wenn ja zu Frage 10. Welche Dienstleistungen im Projekt ELGA wurden seit dem Projektstart an welche externen Dienstleister ausgeschrieben und vergeben?*

Für Beschaffungen im Rahmen von ELGA gilt das Vergaberechtsregime, sofern hierfür kein Ausnahmetatbestand des BVergG (z. B. bei Inhouse-Vergaben) zur Anwendung gelangt. Gemäß BVergG wurde etwa das ELGA-Berechtigungssystem öffentlich ausgeschrieben und vergeben. Einige Leistungen, wie z. B Softwaretests, wurden und werden aus dem Warenkorb der Bundesbeschaffung GmbH (BBG) abgerufen.

Frage 12:

- *Wer wurde per Gesetz für den zukünftigen Betrieb des ELGA Berechtigungssystems (BeS) nominiert?*

Gemäß § 20 ELGA-Verordnung 2015 wird das ELGA-Berechtigungssystem und das ELGA-Protokollierungssystem von der Bundesrechenzentrum GmbH im Sinne des § 28 Abs. 2 Z 11 GTelG 2012 betrieben.

Frage 13:

- *Wer wurde für die technische Umsetzung und den Betrieb des Gesundheitsportals (Zugriff ELGA möglich) beauftragt?*

Im Öffentlichen Gesundheitsportal, das gemäß § 23 Abs. 2 GTelG 2012 auch das Zugangsportal für ELGA ist, erfolgt die Überprüfung der eindeutigen Identität der ELGA-Teilnehmer/innen. Die dahinterliegenden Funktionen des ELGA-Portals, das die ELGA-Funktionalitäten für die Wahrung der Teilnehmer/innen/rechte bereitstellt, z. B. den Zugang zu den persönlichen ELGA-Gesundheitsdaten, werden vom Hauptverband der österreichischen Sozialversicherungsträger im übertragenen Wirkungsbereich zur Verfügung gestellt.

Fragen 14 und 15:

- *Wer ist für den Gesundheitsdienstanbieter-Index (GDA-I) zuständig?*
- *Ist durch die Betreiber des Gesundheitsdienstanbieter-Index (GDA-I) eine eindeutige Identifizierung und Authentifizierung der Gesundheitsdienstanbieter möglich?*

Gemäß § 19 GTelG 2012 hat das Bundesministerium für Gesundheit und Frauen (BMGF) zur Überprüfung der Identität von ELGA-Gesundheitsdiensteanbietern und der ELGA-Ombudsstelle den Gesundheitsdiensteanbieter-Index (GDAI) einzurichten. Die in den GDAI aufzunehmenden Daten sind aus dem eHealth-Verzeichnisdienst (eHVD) zu ermitteln und umfassen die Angaben gemäß § 10 Abs. 1 Z 1 bis 8 GTelG 2012. Technischer Betreiber des GDAI im Auftrag des Bundesministeriums für Gesundheit und Frauen ist die Bundesrechenzentrum GmbH.
Die eindeutige Identifikation von ELGA-Gesundheitsdiensteanbietern erfolgt auf die im GTelG 2012 genannten Arten durch Abgleich dieser Daten mit dem Datenbestand des GDAI (§ 19 Abs. 2 iVm Abs. 3).

Fragen 16 und 17:

- *Wer ist für den Patienten-Index (Z-PI) zuständig?*
- *Ist durch die Betreiber des Patienten-Index (Z-PI) eine eindeutige Identifizierung und Authentifizierung der Zugriffsberechtigten möglich?*

Der Zentrale Patientenindex (ZPI) ist ein Verzeichnis aller Patientinnen und Patienten und enthält grundlegende demografische Angaben zu einer Person. Der ZPI ist notwendig, um die ELGA-Gesundheitsdaten eindeutig einer Person zuzuordnen. Gleichzeitig ist der ZPI eine wesentliche Voraussetzung dafür, Patientinnen und Patienten den elektronischen Zugriff auf die eigenen ELGA-Gesundheitsdaten zu ermöglichen. Der Zentrale Patientenindex wird von den Daten der Sozialversicherung abgeleitet und in einem Clearingverfahren mit den Daten von Stammzahl- und Ergänzungsregister abgeglichen. Eingerichtet und betrieben wird der Zentrale Patientenindex gemäß § 18 GTelG 2012 vom Hauptverband der österreichischen Sozialversicherungsträger im übertragenen Wirkungsbereich.
Entsprechend dem E-Government-Gesetz ist die eindeutige Identifikation der Bürgerin/des Bürgers im Zentralen Patientenindex (ZPI) durch die Verwendung des bereichspezifischen Personenkennzeichens Gesundheit (bPK-GH) sichergestellt.

Frage 18:

- *Werden Sie die Studie "Analyse des Systems Elektronische Gesundheitsakte ELGA" von Dr. Granig und Dr. Stubbings an den Datenschutzrat zur datenschutzrechtlichen Überprüfung vorlegen?*

Das Bundesministerium für Gesundheit und Frauen ist weder Auftraggeber der Studie, noch sind ihm die Inhalte vollumfänglich bekannt. Die Vorlage der Studie an den Datenschutzrat könnte daher nur durch den/die Auftraggeber/in selbst erfolgen.

Frage 19:

- *In der 218. Sitzung des Datenschutzrates wurde die Umsetzung von ELGA einstimmig gefasst, obwohl es dem Datenschutzrat weder fachlich noch technisch möglich war die damals vorgelegten Implementierungsleitfäden zu ELGA (600 Seiten) ordnungsgemäß zu prüfen. Der Datenschutzrat ging damals von der "Annahme" aus, dass eine entsprechende Überprüfung hinsichtlich der gesetzlichen Rechtsgrundlagen und der datenschutzrechtlichen Vorgaben durch das Bundesministerium für Gesundheit erfolgt ist. Der Datenschutzrat ordnete in weiterer Folge die Prüfung der Implementierungsleitfäden durch das Gesundheitsministerium an.*
  Wurden die Implementierungsleitfäden in Ihrem Ministerium datenschutzrechtlich geprüft und liegt dazu ein datenschutzrechtliches Gutachten Ihrer Rechtsabteilung vor?

Die Ergebnisse der (datenschutz-)rechtlichen Prüfung der Implementierungsleitfäden wurden nicht zuletzt mit der Ausführungsbestimmung in § 16 ELGA-VO 2015 umgesetzt. Ein diesbezüglich gesondertes Gutachten wurde nicht erstellt.

Fragen 20 und 21:

- *Planen Sie die Durchführung eines Audits der zentralen und Betreiber-Systeme auf Basis der bestehenden Detaildokumente, Interviews mit Key Stakeholdern sowie den Ergebnissen der bisherigen Penetration Tests?*
- *Wenn nein, warum nicht?*

Ja, solche Audits werden als Initialaudits bereits durchgeführt und können im Rahmen der Gesamtbetriebsführung von ELGA auch künftig durchgeführt werden.

Frage 22:

- *Die A1 Telekom Austria AG bietet Gesundheitsdienstanbietern (GDA) ein A1 ELGA Service (genannt LB A 1 ELGA Service) an. Gibt es zu diesen Dienstleistungen der A1 Telekom Austria AG Verträge mit der ELGA-GmbH und dem Gesundheitsministerium?*
  Quelle: https://cdn2.a1.neUfinal/de/media/pdf/LB A1 ELGApdf

Betreiberinnen und Betreiber von Datenspeichern und Verweisregistern – so wie A1 – haben seit der ELGA-Verordnungsnovelle 2015 vor der Aufnahme des Betriebs eine Meldung zu erstatten. Diese Meldepflicht gemäß § 17k der ELGA-VO 2015 besteht gegenüber der Bundesministerin für Gesundheit und Frauen. Gesonderte Verträge sind dafür nicht erforderlich.

Frage 23:

- *Sind solche Dienstleistungen externer Dienstleister an Gesundheitsdienstanbieter (GDA) durch die ELGA-GmbH oder das Gesundheitsministerium an die Datenschutzkommission gemeldet worden?*

Die Bundesministerin für Gesundheit und Frauen hat in der Vergangenheit gem. § 14 Abs. 5 GTelG 2012 in Vertretung für die ELGA-Gesundheitsdiensteanbieter die Meldepflicht gemäß §17 DSG 2000 wahrgenommen. Die ELGA GmbH hatte in diesem Zusammenhang zu keinem Zeitpunkt eine Meldeverpflichtung.

Frage 24:

- *Wird der betroffene Patient über den jeweiligen Gesundheitsdienstanbieter (GDA) darüber informiert, wenn seine Befunde und Patientendaten nicht beim GDA selbst, sondern über einen Vertrag bei einem externen Dienstleister, zum Beispiel auf Servern der A1 Telekom AG liegen?*

Eine Informationspflicht des ELGA-GDA gegenüber den Betroffenen über die von ihm herangezogenen Auftragsverarbeiter/innen besteht im Rahmen von ELGA nicht. Die Erteilung von diesbezüglichen Auskünften der Auftraggeber/innen (ELGA-GDA) richtet sich nach dem Datenschutzgesetz - DSG 2000.

Frage 25:

- *Welche weiteren externen Dienstleister für Gesundheitsdienstanbieter (GDA) außer der A1 Telekom AG sind Ihnen bekannt?*

Neben den öffentlich-rechtlichen und konfessionellen Anbietern für Betriebsdienstleistungen für Datenspeicher und Verweisregister sind derzeit – über die Fragestellung hinausgehend – zwei weitere private Anbieter bekannt.

Frage 26:
Haben alle derzeit registrierten Gesundheitsdienstanbieter (GDA) ein gem. § 8 GTelG gefordertes IT-Sicherheitskonzept vorgelegt?

Alle Betreiberinnen und Betreiber von Datenspeichern und Verweisregistern, die den Betrieb ab Inkrafttreten der Novelle der ELGA-VO 2015 aufgenommen haben, haben der diesbezüglichen Meldung das Sicherheitskonzept angeschlossen (§ 17k Abs. 2 ELGA-VO 2015).

Dr.in Pamela Rendi-Wagner, MSc

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR GESUNDHEIT UND FRAUEN @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Gesundheit und Frauen
	Datum/Zeit	2017-06-28T15:48:44+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1610631462
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2017-06-28T15:53:14+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	