

Frau
Präsidentin des Nationalrates
Doris Bures
Parlament
1017 Wien

GZ: BMGF-11001/0221-I/A/5/2016

Wien, am 8. September 2016

Sehr geehrte Frau Präsidentin!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 9879/J der Abg. Eva Mückstein, Albert Steinhauser, Freundinnen und Freunde** nach den mir vorliegenden Informationen wie folgt:

Einleitend darf festgehalten werden, dass zur vorliegenden Anfrage eine Stellungnahme der ELGA GmbH eingeholt wurde, die in den nachstehenden Ausführungen berücksichtigt wurde.

Fragen 1 und 2:

- *Wie viele Fälle von missbräuchlichen Zugriffen auf PatientInnendaten sind mittlerweile bekannt?*
- *Wo ist es zu derartigen Vorfällen gekommen?*

Seit Inbetriebnahme der ELGA am 09.12.2015 sind keine missbräuchlichen Zugriffe auf Patientinnen- bzw. Patientendaten bekannt geworden.

Frage 3:

- *Werden Sie die Zugriffsberechtigung so gestalten, dass die zugreifende Person nur Einblick in jene Daten erhält, die für die Erfüllung ihrer Aufgaben berufsgruppenspezifisch erforderlich sind?*

Die Zugriffsrechte auf ELGA-Gesundheitsdaten sind umfassend im Gesundheitstelematikgesetz 2012 geregelt. Der Umfang und die Dauer der Zugriffsberechtigungen sind differenziert nach ELGA-Gesundheitsdiensteanbietern

und nach der Art der ELGA-Gesundheitsdaten festgelegt, die Zugriffsberechtigung ist prinzipiell auf einen konkreten Behandlungsfall eingeschränkt. Diese gesetzlichen Vorgaben wurden entsprechend technisch umgesetzt. Die Steuerung der Zugriffe erfolgt über das ELGA-Berechtigungssystem, das – insbesondere bei ELGA-Gesundheitsdiensteanbietern in Form von Organisationen – durch das vorhandene organisationsinterne Berechtigungssystem ergänzt wird. Letzteres stellt etwa bei Krankenhausinformationssystemen sicher, dass nur jene Personen auf ELGA-Gesundheitsdaten einer Patientin bzw. eines Patienten Zugriff haben, die in das Behandlungsgeschehen eingebunden sind.

Frage 4:

- *Werden Sie Zugriffskontrollen einführen, so dass sichtbar wird, wer aus einem Personenkreis von nicht weniger als 1000 Personen auf die Krankenakte zugegriffen hat?*

Jeder Zugriff auf ELGA-Gesundheitsdaten wird protokolliert. Diese Protokollierung im Rahmen des ELGA-Berechtigungssystems kann technisch nicht umgangen werden. Darüber hinaus werden solche Zugriffe auch in den lokalen IT-Systemen (etwa Krankenhausinformationssystemen) mitprotokolliert, sodass für Zugriffe jederzeit nachvollziehbar ist, wer wann und in welche ELGA-Gesundheitsdaten Einsicht genommen hat. Die Protokolldaten des ELGA-Berechtigungssystems können von Patientinnen und Patienten jederzeit eingesehen werden und werden auch dafür verwendet, um Auffälligkeiten im Zugriffsverhalten feststellen zu können. Daneben ist auf die allgemeinen Vorgaben des Datenschutzgesetzes 2000 hinzuweisen, wonach die Betreiber von Datenanwendungen angehalten sind, die Einhaltung der Zugriffsberechtigungen zu überwachen. Die Kontrollmöglichkeiten von Zugriffen sind somit deutlich höher, als in der Frage ausgeführt.

Frage 5:

- *Gibt es technische Lösungen für Zugriffseinschränkungen und -kontrollen? Wenn ja, welche?*

Zugriffe auf ELGA-Gesundheitsdaten von ELGA-Gesundheitsdiensteanbietern im niedergelassenen Bereich sind nur durch vorheriges Stecken der e-card möglich. Eine weitere technische Voraussetzung für ELGA-Zugriffe ist, dass der betreffende Gesundheitsdiensteanbieter in den GDA-Index eingetragen ist. Ist dies nicht der Fall, werden Zugriffsversuche vom ELGA-Berechtigungssystem verhindert. Eine weitere technische Zugriffsschranke besteht darin, dass Zugriffe nur in einem bestimmten Zeitraum möglich sind und inhaltlich entsprechend den gesetzlichen Vorgaben eingeschränkt sind. Beispielsweise dürfen/können Apotheken nur e-Medikationsdaten einsehen, der Zugriff auf Befunde und Entlassungsbriefe ist technisch nicht möglich.

Frage 6:

- *Wie werden Sie sicherstellen, dass Personen von missbräuchlichen Zugriffen auf ihre Krankenakte erfahren, die nicht selbst Einsicht in ihre Krankenakte nehmen (können)?*

In der Fragestellung wird nicht unterschieden, ob der (missbräuchliche) Zugriff auf die lokale Dokumentation (Krankengeschichte) oder auf ELGA-Gesundheitsdaten erfolgt ist. Missbräuchliche Zugriffe auf die Krankengeschichte sind durch geeignete Vorkehrungen des Betreibers zu verhindern. Sofern ELGA-Gesundheitsdaten bzw. ELGA von solchen Zugriffen betroffen wären, könnten dies jene Bürgerinnen und Bürger, die nicht selbst via Zugangportal in die Protokollierung Einsicht nehmen können, im Wege der ELGA-Ombudsstelle tun. Die regionalen Standorte der ELGA-Ombudsstellen bei den Patientenanwaltschaften unterstützen die Betroffenen dabei und beraten sie auch in sonstigen datenschutzrechtlichen Fragen.

Frage 7:

- *Mit welchen sonstigen Mitteln werden Sie sicherstellen, dass persönliche Gesundheitsdaten nicht aus Neugier oder anderen Gründen in die falschen Hände kommen?*

Soweit sich die Frage auf ELGA bezieht, darf auf die umfassenden rechtlichen Vorgaben verwiesen werden. Verwaltungsstrafbestimmungen sowie die Erweiterung der gerichtlich strafbaren Tatbestände in Bezug auf ELGA entfalten die notwendige Präventivwirkung. Um interne unberechtigte Zugriffe zu verhindern, müssen die technischen Vorkehrungen durch intensive und laufende Schulungen des Personals ergänzt werden, worauf gerade bei der Einführung von ELGA besonders geachtet wurde. ELGA selbst wird in Bezug auf externe unberechtigte Zugriffe, aber auch in Bezug auf sonstige Auffälligkeiten überwacht (siehe Antwort zu Frage 4). Insbesondere die Verbesserung und Erweiterung der Sicherheitsvorkehrungen sind ein Schwerpunkt der Weiterentwicklung, wodurch angestrebt und sichergestellt werden soll, dass die Sicherheit der ELGA-Gesundheitsdaten jederzeit entsprechend dem Stand der Technik gewährleistet ist. Demzufolge ist auch der Zugang der Bürgerinnen und Bürger zu ihren ELGA-Gesundheitsdaten über das Portal nur auf Basis der Bürgerkartenidentifizierung und –authentifizierung möglich.

Frage 8:

- *Wird das System ELGA aufgrund dieser alarmierenden Vorfälle grundlegend überarbeitet und werden die Empfehlungen von Datenschutz-ExpertInnen berücksichtigt, wonach die elektronische Gesundheitsakte bzw. persönliche Gesundheitsdaten ausschließlich in die Hände der PatientInnen zu legen sind?*

Vorfälle wie jene, die offenbar Anlass für die parlamentarische Anfrage waren, können nicht im Zusammenhang mit ELGA stehen, zumal im Burgenland eine Inbetriebnahme von ELGA bislang noch nicht erfolgt ist. Weder die ELGA-Systempartner noch ich sehen derzeit einen Anlass, ELGA aufgrund solcher

Vorkommnisse grundlegend zu überarbeiten. Wie bereits zu Frage 7 ausgeführt, bildet die technische Weiterentwicklung der Datensicherheit einen Schwerpunkt der bisherigen und auch der künftigen Arbeiten. Dabei werden nicht nur die Empfehlungen von Datenschutzexpert/inn/en berücksichtigt, sondern auch Sicherheitsexpert/inn/en einbezogen. Die in der Präambel angesprochenen Möglichkeiten, etwa die Speicherung von Gesundheitsdaten auf persönlichen USB-Sticks, stellen allerdings nach einhelliger Meinung aller Expert/inn/en keine gangbare Alternative in Bezug auf (Daten-)Sicherheitsaspekte dar. Dies gilt auch für die Vorstellung, alternativ bei der bisherigen analogen/papiergestützten Datenhaltung zu bleiben, da diese weder per se sicherer ist noch einer modernen Gesundheitsversorgung entspricht. Darüber hinaus darf angemerkt werden, dass es Bürgerinnen und Bürgern ohnehin freisteht, ihre Gesundheitsdaten elektronisch im Web bzw. auf einem Medium ihrer Wahl zu speichern oder in Papierform zu Hause aufzubewahren.

Dr.ⁱⁿ Sabine Oberhauser

