Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

sozialministerium.at

Dr. Wolfgang Mückstein
Bundesminister

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2021-0.390.499

Wien, 15.7.2021

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 6779/J der Abgeordneten Douglas Hoyos-Trauttmansdorff, Mag. Gerald Loacker, Kolleginnen und Kollegen betreffend Datenschutz beim "Grünen Pass"** wie folgt:

Frage 1:

- *Wie weit ist die Entwicklung der WebApp fortgeschritten und wie sehen die weiteren Schritte aus?*
  - *a. Wer war bzw. ist für die Umsetzung der WebApp verantwortlich?*
  - *b. Wer war bzw. ist für den Datenschutz der WebApp verantwortlich?*

Die WebApp „GreenCheck“ wurde am 18. Juni 2021 in den Produktionsbetrieb übergeleitet. Sie wurde im Auftrag der Systempartner Bund, Länder und Sozialversicherung von der ITSV GmbH entwickelt. Das Projekt wird von einem Lenkungsausschuss, in dem alle Systempartner vertreten sind, gesteuert. Demnach wird

der Datenschutz sowohl seitens der Entwicklung als auch seitens der Steuerung wahrgenommen. Als datenschutzrechtlich Verantwortlicher für die WebApp „GreenCheck“ wurde der Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz festgelegt, die ITSV GmbH fungiert als Auftragsverarbeiter. Für die Nutzung der WebApp „GreenCheck“ ist die:der Überprüfende verantwortlich, da sowohl der Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz als der Auftragsverarbeiter keinen Einfluss auf die Verarbeitung der QR-Codes auf dem Endgerät haben.

Frage 2:

- *Wer ist in der Entwicklung des Gesamtprojekts "Grüner Pass" für den Datenschutz verantwortlich?*
    - *a. Wurden diesbezüglich auch externe Expert_innenmeinungen eingeholt?*
        - *i. Wenn ja, von wem?*
        - *ii. Wenn ja, wann?*
        - *iii. Wenn nein, warum nicht?*

Zur datenschutzrechtlichen Verantwortlichkeit wird auf die Antwort zu Frage 1 verwiesen. Betreffend Datenschutz waren in die Entwicklung zahlreiche Organisationen eingebunden, vorrangig die Stabsstelle Datenschutz im Bundesministerium für Justiz, der Datenschutzrat und die Datenschutzbehörde. Im Bereich des Datenschutzes tätige Non-Profit-Organisationen waren im Rahmen mehrerer Gespräche eingebunden, ihre Anmerkungen und Einwände wurden berücksichtigt.

Frage 3:

- *Sie sprechen auf Anfrage der ZiB2 Redaktion davon, nach "höchsten Sicherheits- und Datenschutzstandards" zu agieren. Was bedeutet das konkret?*

Die Entwicklung der WebApp erfolgte entsprechend dem aktuellsten Stand der Technik. Dabei wurden insbesondere auch die daraus resultierenden Anforderungen an die Datensicherheit berücksichtigt. Dasselbe gilt auch für den Applikationsbetrieb und die Weiterentwicklung. Bezüglich Datenschutz wurden alle Anforderungen, die im Vorfeld der gesetzlichen Regelung diskutiert wurden, umgesetzt. Die Offenlegung des Quellcodes – soweit davon nicht urheberrechtlich geschützte Fremdsoftware betroffen ist – wird derzeit vorbereitet.

Frage 4:

- *Aus welchem Grund wurde dann doch entschieden, die eCard nicht in den "Grünen Pass" miteinzubeziehen?*
    - *a. Wer hat diese Entscheidung getroffen?*
    - *b. Wann wurde diese Entscheidung getroffen?*
    - *c. Wurden hier schon im Vorfeld Bedenken geäußert?*
        - *i. Wenn ja, wann und durch wen?*

Konzeptionell war der von den europäischen Vorgaben geforderte niederschwellige Zugang für Bürgerinnen und Bürger zu ihren Zertifikaten durch die Einbeziehung der e-card intendiert. Auf Grund der geäußerten datenschutzrechtlichen Bedenken wurde von einer diesbezüglichen gesetzlichen Regelung, aber auch von der technischen Umsetzung im Auftrag des Lenkungsausschusses im Mai 2021, Abstand genommen. Die datenschutzrechtlichen Bedenken in diesem Zusammenhang bezogen sich unter anderem auf das Profiling (Erstellung von Bewegungs- oder Nutzungsprofilen), welches mit der ursprünglich beabsichtigten Lösung zwar technisch möglich, aber zu keinem Zeitpunkt angedacht war.

Fragen 5 und 7:

- *Auf welchen Grundlagen basiert die Idee, die Daten zentral abzuspeichern?*
    - *a. Welche anderen potenziellen Lösungen gäbe es für die Speicherung?*

b. Wird in Betracht gezogen, die Daten in der ELGA zu speichern?

i. Wenn nein, warum nicht?

c. Sämtliche Datenschützer/innen warnen diesbezüglich vor großen Sicherheitslücken. Wie wollen Sie diese umgehen?

d. Wie soll verhindert werden, dass auf die Daten zugegriffen und somit Bewegungsprofile erstellt werden können?

- *Mit der ELGA gibt es ein vorhandenes, sicheres System zur Datenspeicherung. Warum wird dieses nicht genutzt?*

a. Welche Maßnahmen werden gesetzt, um einen Datenschutz trotzdem gemäß dem Gesundheitstelematikgesetz zu garantieren?

b. Sollen dafür nur für die App eigene zu ELGA analoge Systeme geschaffen werden?

c. Um wie viel erhöhen sich dadurch die Kosten im Vergleich dazu, wenn man die Daten in der ELGA-Infrastruktur speichern würde?

Es war zu keinem Zeitpunkt angedacht, Daten in der WebApp zentral zu speichern, sondern – beim Einsatz der e-card als Zugangstoken – lediglich die durch das EPI-Service generierten Zertifikate direkt abzufragen. Dies hätte, wie zu Frage 4 ausgeführt, deshalb einen sehr niederschwelligen Zugang für Bürgerinnen und Bürger zu ihren Zertifikaten ermöglicht, weil bei diesem Lösungsansatz weder das Mitführen eines Papierausdrucks noch eines Smartphones erforderlich gewesen wäre. Tatsächlich umgesetzt wurde letztlich die auf europäischer Ebene skizzierte Lösung der ausschließlichen offline-Verifizierung von Zertifikaten. Demzufolge ist für das Gerät der/des Überprüfenden lediglich eine periodische Netzwerkverbindung innerhalb von maximal 48 Stunden erforderlich, um die im europäischen Gateway hinterlegten öffentlichen Schlüssel (der ausstellenden Behörden) sowie die Widerrufsliste für die Zertifikate zu aktualisieren.

Die Aus- und Bereitstellung der EU-konformen Test-, Genesungs- und Impfzertifikate erfolgt durch das sogenannte EPI-Service. Damit verbunden ist auch die Speicherung im auf das jeweilige Zertifikat bezogene unumgänglichen Ausmaß. Dies deshalb, weil davon

ausgegangen werden muss, dass die Zertifikate von den Betroffenen in hohem Ausmaß papiergestützt (gedruckt) verwendet werden und Ausdrucke verloren gehen oder unleserlich werden. Sie sind daher als Ersatz vorzuhalten, um eine aufwändige Neuausstellung (verbunden mit dem Widerruf) zu vermeiden. Die Löschung der Zertifikate erfolgt zeitnah bzw. gekoppelt an die jeweilige zeitliche Gültigkeitsdauer. Die für den Download der WebApp „GreenCheck“ durch Überprüfende aus technischen Gründen notwendige Verarbeitung der IP-Adresse wird unmittelbar nach Abschluss des Downloads automatisiert gelöscht.

Die Speicherung bzw. Bereitstellung von COVID-19-Zertifikaten in ELGA wurde aus mehreren Gründen nicht vorgesehen. Für ELGA ist nämlich ein sehr eingeschränktes Zugriffsregime auf Gesundheitsdaten festgelegt, das die Zugriffsrechte bezogen auf ELGA-Gesundheitsdiensteanbieter regelt. Auch weitere rechtliche Festlegungen, wie etwa der Widerspruch oder die Löschfristen, wären einer Einbettung von COVID-19-Zertifikaten in ELGA entgegengestanden. Die Verwendung der Zertifikate und der WebApp „GreenCheck“ erfolgt durch einen davon verschiedenen, jedenfalls nicht als ELGA-Gesundheitsdiensteanbieter geltenden Nutzerkreis. Mit der Umsetzung der COVID-19-Zertifikate in Form einer gesonderten Anwendung konnten die Hürden, die in massiven Änderungen des ELGA-Regelungsregime bestanden hätten, vermieden werden. Durch die strikte offline-Verifizierung werden keine Daten der Betroffenen zentral gespeichert, wodurch die Erstellung von Bewegungsprofilen nicht möglich ist.

Da es mit der gewählten technischen Lösung durch die Anwendung „GreenCheck“ zu keinem Transfer personenbezogener Gesundheitsdaten über das Netz kommt, werden auch die diesbezüglichen Datensicherheitsanforderungen des Gesundheitstelematik-gesetzes 2012 nicht tangiert. Selbst bei einer Integration der COVID-19-Zertifikate in ELGA hätte eine gesonderte Anwendung für die Verifizierung entwickelt werden müssen, da ELGA eine solche Funktionalität nicht enthält. Dem gegenüber hätte die Integration der Verifizierungssoftware in ELGA sehr weitreichende Eingriffe in den Softwarebestand mit nur schwer voraussehbaren oder durch Tests ausschließbaren Folgen nach sich gezogen.

Da dies zu keinem Zeitpunkt zur Diskussion stand und auch nicht gefordert wurde, konnten diesbezügliche Kostenschätzungen ebenfalls unterbleiben.

Frage 6:

- *Welche Maßnahmen sind als Sicherheitsmaßnahmen für die Abfrage vorgesehen?*
    a. *Wie wird garantiert, dass nur qualifizierte Verifier den Status abfragen können?*
    b. *Wie wird garantiert, dass durch die Qualifikation der Verifier keine Bewegungsprofile erstellt werden können?*

Durch die in den QR-Code integrierten Sicherheitsmechanismen wird sichergestellt, dass Manipulationen am QR-Code selbst (Integritätsverletzungen) festgestellt werden können. Durch die Rechtsvorschriften werden verschiedene Settings bestimmt, für die eine Beschränkung des Zugangs oder der Inanspruchnahme von Leistungen erfolgt ist. Für Betroffene, die verifizierbare (prüfbare) Nachweise vorlegen, entfallen diese Beschränkungen. Welche Personen konkret für die Verifizierung zum Einsatz gelangen, liegt nicht im Einflussbereich des Bereitstellers der Verifizierungssoftware. Für die Nutzung der Verifizierungssoftware ist keine besondere Qualifikation erforderlich, weshalb die Bereitstellung allgemeiner Anleitungen als ausreichend angesehen wurde.

Durch die ausschließliche offline-Verifizierung der Zertifikate ist die Erstellung von Bewegungsprofilen nicht möglich. Darüber hinaus hat eine Authentifizierung der/des Überprüfenden (§ 4f Abs. 1 EpiG) zu unterbleiben, weshalb auch die Erstellung von Nutzungsprofilen nicht möglich ist. Eine missbräuchliche Verwendung kann mit technischen Mitteln allein nicht verhindert werden, in rechtlicher Hinsicht wurde deshalb mit einem entsprechenden (Weiter-)Verarbeitungsverbot vorgesorgt.

Frage 8:

- *Welche Schritte wurden gesetzt, um den in der Begründung genannten Antrag (512/A(E)) umzusetzen?*
    - *a. Welche Schritte gedenken Sie in Zukunft in diese Richtung noch zu setzen?*
    - *b. Gibt es einen Zeitplan für die Umsetzung?*
        - *i. Warum nicht?*
    - *c. Falls noch keine Schritte gesetzt wurden: warum nicht?*

Zum Entschließungsantrag 512/A(E) in der Fassung der Entschließung des Nationalrats 53/E XXVII. GP ist festzuhalten, dass es – zumindest europaweit – noch keine akkordierte Vorgangsweise betreffend Antikörperbestimmungen gibt. Die unzureichende wissenschaftliche Evidenz dürfte nicht zuletzt auch Grund dafür gewesen sein, dass Antikörperbestimmungen und auf dieser Grundlage allenfalls ausgestellte Genesungszertifikate im Entwurf der Verordnung betreffend EU Digital COVID Certificate lediglich kursorisch angesprochen bzw. der Regelung durch einen delegierten Rechtsakt vorbehalten wurden. Mit den jüngst geschaffenen Bestimmungen im Epidemiegesetz 1950 (§§ 4b ff.) wurden erste Regelungen für eine innerstaatliche Verwendung von Antikörpertests geschaffen. Nach Vorliegen ausreichender wissenschaftlicher Evidenz bzw. eines delegierten Rechtsakts können diese Bestimmungen mit Verordnung konkretisiert werden.

Das Gesundheitstelematikgesetz 2012 bietet bereits derzeit die Möglichkeit (vgl. § 24c Abs. 2 Z 2 lit. c), Titerbestimmungen im elektronischen Impfpass (eImpfpass) zu erfassen und zwar unabhängig von COVID-19 für alle in Betracht kommenden Infektionskrankheiten. Für die Einbringung dieser Daten ist allerdings die Anbindung von Laboren an die eImpfpass-Anwendung notwendig, woran die ELGA GmbH als derzeit Verantwortliche für den eImpfpass intensiv arbeitet.

Frage 9:

- *Aus welchem Grund wird seitens der österreichischen Regierung nicht auf die Software-Angebote zurückgegriffen, die es auf EU-Ebene bereits gibt?*

Die Inhalte der Zertifikate (QR-Codes) werden auf EU-Ebene vorgegeben und wurden in das EpiG übernommen. Die nunmehr entwickelte WebApp „GreenCheck“ verwendet exakt jenen Prüf- bzw. Verifizierungsmechanismus, der im Rahmen der open source-Lösung auf europäischer Ebene entwickelt bzw. zur Verfügung gestellt wird. Lediglich die aus Sicht des Datenschutzes erforderliche eingeschränkte Auflösung des QR-Codes (text- und farbcodierte Präsentation des Verifizierungsergebnisses sowie das aus den nationalen Rechtsvorschriften resultierende Regelwerk für dessen Interpretation) und die für die Nutzung notwendige Oberfläche stellen Eigenentwicklungen dar, da diese Funktionalitäten von der europäischen open source-Lösung nicht abgedeckt werden.

Frage 10:

- *Wie hoch waren die bisherigen Gesamtkosten der Entwicklung des "Grünen Passes"? Bitte um Auflistung der Posten.*

Die Kosten für die Entwicklung des Grünen Passes (nunmehr EU Digital COVID Certificate) betragen ca. 1,9 Mio. Euro, wovon der überwiegende Anteil auf die Entwicklung des EPI-Service entfällt. Ein geringer Anteil dieser Kosten entfällt jeweils auf die Entwicklung der WebApp „GreenCheck“ sowie auf das Projektmanagement durch die ELGA GmbH. Anzumerken ist, dass der genannte Betrag eine Schätzung darstellt, da Abrechnungen naturgemäß noch nicht vorliegen.

Kostenaufgliederung:

Entwicklung EPI-Service: rd. 1,45 Mio. Euro
Entwicklung GreenCheck: rd. 180.000 Euro
Projektmanagement ELGA GmbH: max. 300.000 Euro

Fragen 11 und 12:

- *Die Umsetzung eines europäischen Passes ist sicher. Aus welchem Grund will man in Österreich hier vorgreifen?*
- *Wer trägt die Verantwortung dafür, dass die Umsetzung in Österreich schneller passieren muss?*

a. Gab es hier Überlegungen zu Alternativen? Wenn ja, welche?

Die Verwendung der auf der Grundlage der EU-Verordnung betreffend EU Digital COVID Certificate von den Mitgliedstaaten auszustellenden Zertifikate ist auf grenzüberschreitende Reisebewegungen eingeschränkt. Mit dieser wird aber für die Mitgliedstaaten die Möglichkeit eröffnet, die EU-konformen Zertifikate für andere (innerstaatliche) Zwecke zu verwenden, vorausgesetzt es werden die dafür notwendigen Rechtsgrundlagen geschaffen. Österreich hat sich dazu entschlossen, die EU-konformen Test-, Genesungs- und Impfzertifikate auch – aber nicht ausschließlich (vgl. § 4b Abs. 1 EpiG) – als Nachweise für den Zutritt zu bestimmten Settings/Veranstaltungen oder zur Inanspruchnahme bestimmter Dienstleistungen zu verwenden. Ziel war es, so weit wie möglich von Eigenentwicklungen abzusehen. Daher stellen die „österreichischen" Zertifikate keinen Vorgriff auf die ohnehin umzusetzenden EU-konformen Zertifikate dar und enthalten auch keine Abweichungen, sondern sind eine kostengünstige weitere Nutzungsmöglichkeit.

Die EU-Verordnung ist Anfang Juli 2021 in Kraft getreten und enthält eine sechswöchige Übergangsfrist. Da es erklärtes Ziel der EU-Verordnung ist, Reisen – insbesondere in den Sommermonaten – zu erleichtern und die Zertifikate daher bereits zu Beginn der Reisezeit verfügbar sein sollten, musste frühzeitig mit der Umsetzung begonnen werden. Diese Vorgangsweise unterscheidet sich nicht von anderen Mitgliedstaaten.

Die Alternative zu dieser Vorgangsweise wäre gewesen, das Inkrafttreten der EU-Verordnung abzuwarten und dann mit der Umsetzung zu beginnen. Dies hätte zu gravierenden Verzögerungen in der Verfügbarkeit von EU-konformen Zertifikaten, aber

auch zu Verzögerungen in der Verwendung dieser Zertifikate für innerstaatliche Zwecke geführt.

Frage 13:

- *Ist Ihnen die Umsetzung eines solchen Passes in den Niederlanden bekannt?*
  a. Wenn ja, was spricht dagegen, diese für Österreich zu übernehmen?

Mein Ressort steht, insbesondere über das eHealth Network, in regem Austausch mit den Mitgliedstaaten. Die von den Niederlanden gewählte Lösung entspricht weitgehend der österreichischen, allerdings wird für grenzüberschreitende Reisebewegungen eine separate Garnitur von Zertifikaten zur Verfügung gestellt. Einer direkten Übernahme der dortigen Lösung standen primär administrative und ökonomische Gründe entgegen, auf Unterschiede in den jeweiligen nationalen Rechtsordnungen hätte Bedacht genommen werden müssen. Auch die Akzeptanz der Betroffenen für unterschiedliche Zertifikatsgarnituren konnte a priori nicht angenommen werden.

Mit freundlichen Grüßen

Dr. Wolfgang Mückstein
Bundesminister

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR SOZIALES, GESUNDHEIT, PFLEGE UND KONSUMENTENSCHUTZ @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
	Datum/Zeit	2021-07-26T07:10:44+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	2098721075
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.sozialministerium.at/site/Ministerium/Willkommen_im_Ministerium/Amtssignatur/Amtssignatur	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2021-07-26T07:13:26+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.	