

An das
Bundesministerium für Soziales,
Gesundheit, Pflege, und
Konsumentenschutz

Per Mail:

Engelbert.Prenner@gesundheitsmi
nisterium.gv.at

begutachtungVIII4@gesundheitsm
inisterium.at

Regierungsvorlage zum Bundesgesetz, mit dem das Gesundheitstelematikgesetz 2012 geändert wird (Anhörung des Datenschutzrates gemäß § 31a Abs. 4 ASVG)

Der Datenschutzrat hat in seiner **250. Sitzung am 14. Juli 2020 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines

Gemäß der Parlamentshomepage wurde am 16. Juni 2020 die **Regierungsvorlage** zur Änderung des **Gesundheitstelematikgesetzes 2012 (GTelG)** eingebracht.

Zum zugehörigen Ministerialentwurf wurde im Jänner 2020 im Begutachtungsverfahren vom Datenschutzrat – nach Anhörung informierter Vertreter aus dem Bundesministerium für Soziales, Gesundheit, Pflege, und Konsumentenschutz (BMSGPK) – eine umfassende Stellungnahme aus datenschutzrechtlicher Sicht abgegeben (siehe Beilage).

2) Datenschutzrechtliche Anmerkungen

Die Anmerkungen und Fragestellungen aus der Stellungnahme des Datenschutzrates zum Ministerialentwurf wurden vom BMSGPK in der Regierungsvorlage zum GTelG weitgehend nicht oder nur unzureichend berücksichtigt. Gleiches gilt nach Auskunft der Datenschutzbehörde für die von der Datenschutzbehörde abgegebenen Stellungnahme. Der Datenschutzrat verweist deshalb erneut auf die beiliegende Stellungnahme zum

Ministerialentwurf, die vollinhaltlich aufrecht bleibt. Beispielhaft wird auf folgende Aspekte aus der Stellungnahme des Datenschutzrates hingewiesen:

- Vor dem Hintergrund des Verhältnismäßigkeitsgrundsatzes wurde die in der Stellungnahme des Datenschutzrates aufgeworfene zentrale Frage der Zielerreichung mit gelinderen Mitteln nicht behandelt. Es bleibt somit die Frage bestehen, ob bei der Verarbeitung der personenbezogenen Daten für den **Elektronischen Impfpass bzw. das zentrale Impfbregister überhaupt ein direkter Personenbezug** zur Erreichung der angestrebten Ziele erforderlich ist oder ob auch **(nur) mit bereichsspezifischen Personenkennzeichen (bPK)** (ohne Namen) bzw. überhaupt bloß mit **statistischer Erfassung ohne jeglichen Personenbezug** (zB zur Erhebung der Durchimpfungsrate) das Auslagen gefunden werden kann.
- Der **Entfall des Widerspruchsrechtes** der Bürger in § 24b für die **lückenlose, verpflichtende Erfassung** von Durchimpfungsraten im Elektronischer Impfpass ist geblieben. Die datenschutzrechtliche Anregung der unterschiedlichen Behandlung der jeweiligen Impfungen aufgrund der **unterschiedlichen Ansteckungsgefahren und den drohenden gesundheitlichen Folgen einer Ansteckung**, die sich in der **Regelung der Verpflichtung** zur Speicherung der personenbezogenen Impfdaten widerspiegeln sollten, wurde **nicht** berücksichtigt.
- Die Frage, wie die Daten von jenen Personen verarbeitet werden, die **nicht ELGA-Teilnehmer** sind bzw. **einer Teilnahme an ELGA widersprochen haben**, zumal für die eHealth-Anwendung „Elektronischer Impfpass“ gemäß § 24f auch **ELGA-Komponenten** genutzt werden, wurde nicht geklärt. Dies hätte offenbar auch zur Folge, dass Einrichtungen, die bislang nicht zur Abfrage von ELGA-Daten berechtigt waren, nun **(einzelne) Komponenten von ELGA** nutzen und Daten daraus verarbeiten dürfen. Ebenso fehlt die nähere Darlegung, ob damit etwa für den Landeshauptmann, die Bezirksverwaltungsbehörden und den für das Gesundheitswesen zuständigen Bundesminister unter Umständen ersichtlich werden kann, **wer der Teilnahme an ELGA widersprochen hat**.
- Der in der Begutachtung geäußerten Ansicht, dass die **Zugriffsberechtigung für Apotheken entfallen** sollte, da diese zur Zielerreichung nicht erforderlich erscheint, wurde **nicht gefolgt**. Vielmehr wurde in der **Regierungsvorlage zusätzlich** vorgesehen, dass hinsichtlich der Nutzung von ELGA-Komponenten nunmehr auch die **Apotheken** in § 24f Abs. 4 Z 2 eine **spezifische Zugriffsberechtigung im Berechtigungssystem** (§ 21) auf die zusammenfassende Darstellung der im zentralen Impfbregister gespeicherten Daten gemäß § 24d Abs. 2 Z 1 und auf die auf Basis dokumentierter Impfungen und des jeweils aktuellen Impfplans Österreich erstellten **persönlichen Impfkalender** gemäß § 24d Abs. 2 Z 2 haben.

- Die Anmerkung in der Begutachtung zum in § 27 Abs. 17 geregelten „**Pilotbetrieb**“, dass für eine **Datenverarbeitung mit „Echtdaten“** im Rahmen einer „Pilotierung“ **keine Sonderregelungen in der DSGVO vorgesehen** sind, bleibt aufrecht. **Die Vorgaben der DSGVO für Datenverarbeitungen sind in einem solchen Fall auch vollinhaltlich auf die „Pilotierung“ anzuwenden.** In diesem Zusammenhang wird insbesondere auf die Bedeutung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen hingewiesen.
- Der Datenschutzrat hat bereits wiederholt eine ablehnende Haltung zur **Verwendung der Sozialversicherungsnummer** für Bereiche, die nicht der Ingerenz der Sozialversicherung unterliegen – quasi als „**Personenkennzeichen**“ – vertreten (vgl. etwa GZ BKA-817.246/0004-DSR/2010). Die Verwendung der Sozialversicherungsnummer als universelles „Personenkennzeichen“ widerspricht der E-Government-Strategie des Bundes. Es sollte daher stattdessen das bereichsspezifische Personenkennzeichen (bPK) verwendet werden.

Zusätzlich zu diesen beispielhaft aufgezählten, nicht gelösten datenschutzrechtlichen Problemstellungen aus dem Begutachtungsverfahren wurde nunmehr folgende Regelung nachträglich in die Regierungsvorlage aufgenommen:

Z 36. Dem § 18 Abs. 4 wird folgende Z 5 angefügt:

„5. Auslesen von Daten der e-card oder eines amtlichen Lichtbildausweises im Format ID-1 mittels geeigneter Technologie, wobei als amtlicher Lichtbildausweis in diesem Sinne von einer staatlichen Behörde ausgestellte Dokumente, die mit einem nicht austauschbaren erkennbaren Kopfbild der betreffenden Person versehen sind, und den Namen, das Geschlecht, das Geburtsdatum und die Unterschrift der Person sowie die ausstellende Behörde enthalten, gelten,“

Erläuterungen:

Zu Z 35 und Z 36 (§ 18 Abs. 4 Z 4 und Z 5):

„Vor dem Hintergrund der COVID-19-Pandemie soll die vorgeschlagene Bestimmung dem Umstand Rechnung tragen, dass eine niederschwelle Möglichkeit zur sicheren und eindeutigen Identifizierung der Bürger/innen durch die Gesundheitsdienstleister geschaffen wird: Mittels einer speziellen App können Identitätsdaten von der e-card oder einem amtlichen Lichtbildausweisen im Scheckkartenformat (ID-1-Format) extrahiert und dann mit dem Patientenindex oder dem Stammzahlenregister abgeglichen werden. Die App hat den Vorgaben der DSGVO und anderen einschlägigen Gesetzen hinsichtlich Datenschutz und Datensicherheit zu entsprechen, insbesondere dürfen die Identitätsdaten nicht über die Dauer des Abgleiches mit dem Patientenindex hinaus gespeichert werden. Durch die Verwendung eines amtlichen Lichtbildausweises wird potentieller Missbrauch verhindert; die Definition des

amtlichen Lichtbildausweises orientiert sich an derjenigen in § 6 Abs. 2 Z 1 Finanzmarkt-Geldwäschegesetz – FMGwG, BGBl. I Nr. 118/2016.“

Der Datenschutzrat merkt aus datenschutzrechtlicher Sicht dazu Folgendes an:

- Die in der Regierungsvorlage hinzugefügte Bestimmung (§ 18 Abs. 4 Z 5) war nicht Teil des Ministerialentwurfs und wurde somit **keiner Begutachtung zugeführt**. Im Rahmen einer nachträglichen Sitzung des Datenschutzrates am 14. Juli 2020 wurden informierte Vertreter des BMSGPK dazu befragt.
- Diese Bestimmung **ändert** soweit ersichtlich das **Grundkonzept der Authentifizierung für ELGA** (bisher war die Authentifizierung ausschließlich über das Stecken der eCard möglich und zulässig; ohne eCard kein Zugang zu den Gesundheitsdaten).
- Gemäß § 31a Abs. 4 ASVG dürfen Bestandteile des ELSY für andere als Sozialversicherungszwecke nur mit bundesgesetzlicher Ermächtigung und nur so weit verarbeitet werden, als dies mit dem **Zweck des ELSY nicht unvereinbar** (Art. 5 Abs. 1 lit. b DSGVO) ist.
- Zu Fragen der Unvereinbarkeit neuer Verarbeitungszwecke sowie zu Fragen der Speicherung von personenbezogenen Daten auf den innerhalb des ELSY zu verwendenden Chipkarten **ist der Datenschutzrat** unter Setzung einer angemessenen Frist **anzuhören**. **Der Datenschutzrat wurde zu dieser Bestimmung im Vorfeld nicht gehört.**
- Die Ergänzung dieser Regelung im Vergleich zum Ministerialentwurf wird mit der **COVID-19-Krise** begründet. Dieser Zusammenhang wird allerdings nicht entsprechend nachvollziehbar begründet.
- Die vorgesehene Regelung ist im Lichte der Judikatur des VfGH betreffend die Kriterien für einen Eingriff in das Grundrecht auf Datenschutz **unterdeterminiert**.
- Völlig **offen** bleibt die **Frage der Verhältnismäßigkeit**: Die eCard wurde mit dem Argument der Betrugsverhinderung rezent mit einem Foto ausgestattet. Unbeschadet der Frage, ob überhaupt das Auslesen der eCard im vorliegenden Kontext zulässig sein könnte, ist nicht nachvollziehbar, **weshalb nunmehr zur Identitätsprüfung offenbar jeder amtliche Lichtbildausweis im Scheckkartenformat von allen Gesundheitsdiensteanbietern ausgelesen werden können soll**. Es wirft die Frage auf, inwiefern die Identität – so wie bisher – nicht mit dem gelinderen Mittel iSd § 1 Abs. 2 DSG ausschließlich unter Nutzung der eCard festgestellt werden kann. **Des Weiteren wäre zu klären, wie bei Verwendung amtlicher Lichtbildausweise die eindeutige Zuordnung der Impfdaten bei Datenwilligen sichergestellt werden kann**. Fraglich ist auch, weshalb insbesondere die Datenarten Unterschrift, Geschlecht und ausstellende Behörde aus einem amtlichen Lichtbildausweis ausgelesen werden.

- Zudem ist in der vorgesehenen Bestimmung völlig unklar, **wie die elektronische Schnittstelle ausgestaltet** werden soll. Es müsste **auf gesetzlicher Ebene** (auch im Sinne der zu setzenden Datensicherheitsmaßnahmen) festgelegt werden, über welchen konkreten technischen Weg die personenbezogenen Daten übermittelt werden. Gemäß den Erläuterungen soll das Auslesen über eine App funktionieren; allerdings fehlen dazu jegliche Details und Spezifikationen. Insbesondere wäre konkret zu regeln, ob Dienstleister eingesetzt werden, ob eine Cloud-Lösung angedacht ist und ob über die App-Nutzung auch eine Datenverarbeitung im Ausland erfolgen soll.
- Zur Verhinderung von Missbrauch wird angeregt, ein Sicherheitskonzept zu erstellen, das regelmäßig evaluiert wird. Ebenso wird angeregt für die Kontrolle der Sicherheitsmaßnahmen zu sorgen.
- Generell müsste geklärt werden, wie die **datenschutzrechtliche Rollenverteilung für die App** aussieht und wie in diesem Zusammenhang **Betroffenenrechte** wahrgenommen werden können.
- Ergänzend weist der Datenschutzrat darauf hin, dass die Speicherung personenbezogener Gesundheitsdaten im Impfreister zu Zwecken der Erfüllung der berufsrechtlichen Dokumentationspflichten (§ 24c Abs. 2 letzter Satz) sowie die in den Erläuterungen dargestellte Erhebung von Impfdaten durch Gesundheitsdiensteanbieter aus dem Impfreister von der abschließenden Aufzählung der zulässigen Verarbeitungszwecke des § 24d Abs. 2 nicht umfasst sind und die Verantwortung für die genannte Erhebung nicht nur in den Erläuterungen sondern im Gesetz abzubilden ist.

Darüber hinaus gelten für diese Zwecke auch deutlich andere Anforderungen an Zugriffsbeschränkungen und Speicherdauern der betreffenden Daten (zB § 51 Abs. 2 Ärztegesetz), als für die übrigen Zwecke der Verarbeitung vorgesehen sind. Diesbezüglich wäre somit sicherzustellen, dass die Einhaltung der berufsrechtlichen Anforderungen an die Auskunftserteilung und Speicherdauer der Daten zu jedem Zeitpunkt gewährleistet ist und es nicht zur Offenlegung von Daten an unberechtigte Personengruppen oder zu unzulässigen Speicherdauern kommen kann.

Zur Sicherstellung der Integrität der medizinischen Dokumentation sollten allfällige Eingriffe von Bezirksverwaltungsbehörden in die medizinische Dokumentation praktizierender Gesundheitsdiensteanbieter vermieden werden. Im Sinne der Verfügbarkeit wäre angesichts der geltenden Zugriffsvoraussetzungen zu prüfen, inwiefern die im Impfreister gespeicherte medizinische Dokumentation für den jeweiligen Gesundheitsdiensteanbieter im erforderlichen Umfang überhaupt zugänglich ist, sollten die betroffenen Personen – etwa im Zuge der Abwehr derer Rechtsansprüche – an diesem Zugriff nicht mitwirken.

Zusammenfassend weist der Datenschutzrat **neuerlich** auf die schon aus dem Begutachtungsverfahren stammenden **Defizite bei der Berücksichtigung datenschutzrechtlicher**

Anmerkungen hin. Die **Dringlichkeit für die nun in die Regierungsvorlage neu aufgenommene Bestimmung** (§ 18 Abs. 4 Z 5), mit der offenbar das gesamte Berechtigungssystem/Authentifizierungssystem im Hinblick auf den Zugang zu Gesundheitsdaten geändert und erweitert werden soll, **kann in dieser Form nicht nachvollzogen werden**. Ein unmittelbarer Zusammenhang mit der **COVID-19-Krise ist aus Sicht des Datenschutzrates nicht erkennbar**. Die dazu **vorgesehene verpflichtende Anhörung des Datenschutzrates** hat im Vorfeld nicht stattgefunden. Zudem sollte die Einhaltung der berufsrechtlichen Anforderungen an die Dokumentationspflichten im Rahmen des Impfreisters geprüft werden.

Beilage

16. Juli 2020
Für den Datenschutzrat
Der Vorsitzende:
OFENAUER

Elektronisch gefertigt