WIEN / 18. Mai 2021

Stellungnahme

Zum Ministerialentwurf betreffend das Bundesgesetz, mit dem das Epidemiegesetz 1950 und das COVID-19-Maßnahmengesetz geändert werden

Für epicenter.works
Thomas Lohninger
Benedikt Gollatz
Manuel Jany

EPICENTER .WORKS
for digital rights

VORWORT UND KURZFASSUNG

Wir bedanken uns für die Möglichkeit zum vorliegenden Begutachtungsentwurf[1] Stellung zu nehmen. In diesem Zusammenhang wollen wir auf die Bedeutung des Begutachtungsverfahrens im demokratischen Prozess hinweisen. Mit einer öffentlichen Begutachtung können Expert*innen und unterschiedliche Interessensgruppen sich zu einem Gesetzesvorhaben positionieren, Verbesserungsvorschläge machen und insgesamt die Qualität der Gesetzgebung steigern. Es ist in einer modernen Demokratie essentiell, dass die Gesetze nicht nur von der Regierung ans Parlament "herabgereicht" werden oder mittels Initiativantrag wenige Tage vor der Beschlussfassung im Plenum der eigentliche Gesetzestext über Änderungsanträge im Ausschuss eingebracht wird. Demokratische Prozesse brauchen Zeit und Öffentlichkeit, sonst geht das Vertrauen der Bevölkerung verloren. Jene vier Gesetzesänderungen im Bereich des grünen Passes seit Februar 2021 erfüllten diese Anforderungen leider nicht.

Vor diesem Hintergrund bezieht sich diese Stellungnahme zum Teil auch auf Änderungen, die seit der letzten Begutachtung des Epidemiegesetzes ergangen sind, wo diese für den Kontext der Betrachtung der aktuellen Änderungen relevant sind.

Der vorliegende Entwurf geht aus unserer Sicht in eine gute Richtung. Es gibt jedoch mehrere große Datenschutzprobleme. Erstens sehen wir es als ein **großes Versäumnis, dass es keine Festschreibung der Unbeobachtbarkeit des Überprüfungsvorgangs von Zertifikaten gibt**. Wir begrüßen die Nutzung von quelloffener Software in diesem heiklen Bereich, haben diesbezüglich jedoch eine Empfehlung zur Steigerung der Rechtssicherheit und Vereinfachung der Bestimmungen. Neben einer Vielzahl von datenschutzrechtlichen Verbesserungsvorschlägen sehen wir die enorme Ausweitung der Datenspeicherung im Register der anzeigepflichtigen Krankheiten als ein fast nicht zu reparierendes Problem.

Die Verknüpfung von aktuellen und historischen Daten über das Erwerbsleben, das Einkommensniveau, etwaige Arbeitslosigkeiten, den Bildungsweg, etwaige Reha-Aufenthalte und Krankenstände aller geimpften oder genesenen Personen ist überschießend. Gerade im Hinblick auf die Übertragung aller Covid-19-Impfungen in dieses Register entsteht dadurch eine Datenbank über annähernd die gesamte Bevölkerung, welche sensible Gesundheitsdaten mit fast willkürlichen Lebensbereichen verknüpft. Angesichts dieser Datenfülle ist eine Pseudonymisierung gänzlich wirkungslos, da Menschen anhand der Kombination der Merkmale in dieser Datenbank eindeutig identifizierbar werden. Diese Datenverarbeitung ist weder durch den Zweck des Registers gedeckt, noch ist diese Verarbeitung verhältnismäßig. Sollte dies nicht korrigiert werden, überlegen wir, eine höchstgerichtliche Prüfung dieser Datenverarbeitung anzustreben.

Wir begrüßen, dass wesentliche neue Bestimmungen mit einer Außerkrafttretensklausel versehen sind.

1 https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00122/index.shtml

Inhaltsverzeichnis

EPIDEMIEGESETZ EPIG

Register der anzeigepflichtigen Krankheiten

Zu § 4 Abs 3a EpiG

Die Einführung des elektronischen Impfpasses liegt noch nicht lange zurück und wurde von mehreren Datenschutzorganisationen aufgrund des fehlenden opt-outs und seiner überschießenden Speicherverpflichtung von auch nicht-fremdgefährdenden Krankheiten kritisiert.[2] Mit dem vorliegenden Entwurf werden viele der damals geäußerten Befürchtungen leider bestätigt. Anstatt die Impfzertifikate einfach durch die ELGA GmbH ausstellen zu lassen, welche die Daten aller Covid-19 Schutzimpfungen unter hohen Datenschutzstandard bereits vorhält, werden diese Daten pauschal in ein anderes Register mit einer anderen Zweckmäßigkeit und niedrigeren Datenschutzstandards kopiert. Insbesondere da die erstellten Impfzertifikate gemäß § 4e wieder in das Impfregister der ELGA GmbH kopiert werden, muss diese gesamte Konstruktion im vorliegenden Entwurf gemäß dem Grundsatz der Datenminimierung nach Art 5 Abs 1 lit c DSGVO als unverhältnismäßig abgelehnt werden.

Eine Protokollierung ist beim Epidemiologischen Meldesystem (EMS) zwar vorgesehen, nur ist eine Einsicht nicht über den niederschwelligen Weg eines Onlineportals der ELGA, sondern lediglich durch eine jährliche Datenschutzauskunft möglich. Dieses Problem wird insofern gesteigert, da der Kreis der Zugriffsberechtigten und deren Zwecke im EMS um einiges größer ist (Kontaktpersonnachverfolgung). Die pauschale Weiterleitung der Daten hat demnach zur Folge, dass die Mehrzahl der Zugriffe auf die sensiblen Gesundheitsdaten über Impfungen außerhalb des strikteren Zugriffs- und Protokollregimes des eImpfpasses passieren.

Insbesondere da laut der Stellungnahme der ELGA GmbH bereits eine Portalverbundanwendung für die Kontaktverfolgung vorgesehen ist,[3] sollte zumindest dieser Zweck für die Verwendung im EMS gestrichen werden. Dadurch kann der Kreis der Zugriffsberechtigten drastisch reduziert werden.

Lösungsvorschlag:

Die Übertragung der Impfdaten an das EMS sollte gestrichen werden. Die Ausstellung der Zertifikate kann im Wirkungsbereich der ELGA GmbH erfolgen.

Alternativvorschlag:

Streichung der Kontaktverfolgung aus dem letzten Satz:

"Der für das Gesundheitswesen zuständige Bundesminister ist berechtigt, die ihm von der ELGA GmbH übermittelten Daten mit dem Register zu verknüpfen und, es dürfen diese Daten zum Zweck des Ausbruchs- und Krisenmanagements, wie etwa für die Ermittlung von Impfdurchbrüchen, ***oder*** *von Ausbruchsclustern* ***~~oder für die Kontaktpersonennachverfolgung~~****, verarbeitet werden."*

2 https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00009/index.shtml#tab-Stellungnahmen, https://epicenter.works/content/der-elektronische-impfpass-und-seine-schwachstellen und https://epicenter.works/content/e-impfpass-opt-out-moeglichkeit-haette-vertrauen-geschaffen

3 siehe Stellungnahme der ELGA GmbH zur Datenverwendung e-Impfpass (19.2.2021)

Zu § 4 Abs 8a EpiG

Der Umfang und die Bandbreite der personenbezogenen Daten im EMS hat inzwischen eine Eingriffstiefe erreicht, deren Verhältnismäßigkeit stark in Zweifel gezogen werden muss. Durch die Zusammenführung der Covid-19 Erkrankten mit den Geimpften wird in absehbarer Zeit fast die gesamte Bevölkerung in dieser Datenbank eingetragen sein. Durch die in Absatz 8a geplante Verbindung mit aktuellen und historischen Daten über das Erwerbsleben, das Einkommensniveau, etwaige Arbeitslosigkeiten, den Bildungsweg, etwaige Reha-Aufenthalte und Krankenstände der Person, werden fast alle Lebensbereiche in einer Datenbank durchleuchtet. Diese Eingriffstiefe in das Leben der beinahe gesamten Bevölkerung ist für den vorgeblichen Zweck "der Qualitätssicherung" und "des Monitorings der Wirksamkeit von Maßnahmen" überschießend.

Die Verwendung des bereichsspezifischen Personenkennzeichens (bPK) für diese Datenbank ist angesichts der kompletten Aufhebung der Trennung der Datenhaltungen verschiedenster Bereiche der öffentlichen Verwaltung schon fast süffisant. Das bPK sollte genau eine solche "Superdatenbank" verhindern. Die Pseudonymisierung ist angesichts dieser Datenfülle gänzlich zu vernachlässigen. Die Kombination aus Bildungsweg, Krankenständen, Berufswahl und Impf- oder Genesungszeitpunkt erlaubt es jede Person im Land eindeutig in dieser Datenbank zu identifizieren.

Vor diesem Hintergrund macht es auch keinerlei Unterschied, ob die Daten gemäß § 4 im EMS mit dem verschlüsselten bereichsspezifischen Personenkennzeichen Gesundheit (vbPK-GH) oder gemäß § 4a im Statistik-Register mit verschlüsselten bereichsspezifischen Personenkennzeichen Amtliche Statistik (vbPK-AS) gespeichert werden. Jedoch vergrößert sich aufgrund der Übertragung in das Statistik-Register der Kreis der Zugriffsberechtigten auf diesen enormen Datensatz, wodurch das Missbrauchspotential und sich die Gefahr eines Datenskandals im Einflussbereich des Gesundheitsministeriums ebenfalls vergrößert. Diese Bestimmung ist aus Datenschutzsicht eindeutig überschießend und muss ersatzlos gestrichen werden.

Lösungsvorschlag:

Ersatzlose Streichung von § 4 Abs 8a, 22, 23 und 24.

Überschießende Verordnungsermächtigungen

Die Novelle des Epidemiegesetzes enthält zahlreiche Verordnungsermächtigungen des für das Gesundheitswesen zuständigen Bundesministers. Gleichzeitig behandelt das Epidemiegesetz die Verarbeitung hochsensibler Gesundheitsdaten, deren Verarbeitung nach Art 9 DSGVO nur unter engen Grenzen zulässig ist, da sie irreversible Konsequenzen für die Grundrechte auf Privatsphäre und der Nichtdiskriminierung haben kann. Auch an das Bestimmtheitsgebot des Art 18 B-VG und die Determinierung gesetzlicher Grundlagen, die einen Eingriff in das Grundrecht auf Datenschutz und Privatsphäre erlauben, sind insbesondere dort hohe Anforderungen zu stellen, wo es sich um die Verarbeitung besonderer Kategorien personenbezogener Daten handelt, mit deren Verarbeitung hohe Risiken für die Rechte und Freiheiten Betroffener einhergehen. Die gesetzliche Regelung muss ausreichend präzise festlegen, also für den Normunterworfenen vorhersehbar regeln, unter welchen Voraussetzungen die Ermittlung bzw. Verwendung personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben erlaubt ist. Die Tragweite eines Eingriffs in die Grundrechte muss sich aus dem Normtext zweifelsfrei ergeben. Es obliegt somit dem Gesetzgeber, Normen hinreichend bestimmt und klar zu formulieren.[4]

4 Vgl *Thiele/Wagner*, Datenschutzrecht § 1 Rz 55 mwN; VfSlg 20.213/2017

Die Verordnungsermächtigungen des Bundesministers erscheinen dort sinnvoll und verhältnismäßig, wo auf Neuerungen rasch reagiert werden muss. In diesem Sinne normiert etwa § 4c Abs 4 EpiG, dass der Bundesminister aufgrund neuer wissenschaftlicher Erkenntnisse oder Festlegungen auf europäischer Ebene per Verordnung die Gültigkeitsdauer von Testzertifikaten sowie deren Berechnungsmethode ändern kann.

Es finden sich in der Novelle jedoch zahlreiche Ermächtigungen, die unter dem Gesichtspunkt der erforderlichen hinreichenden Bestimmtheit sowie der Verhältnismäßigkeit über die Stränge schlagen.

Zu § 4 Abs 8a EpiG

Nach dieser Bestimmung kann der für das Gesundheitswesen zuständige Bundesminister im Einvernehmen mit der jeweils zuständigen Bundesministerin oder dem jeweils zuständigen Bundesminister mit Verordnung weitere Register vorsehen, aus denen die jeweilige registerführende Stelle zum Zweck der epidemiologischen Überwachung sowie des Monitorings der Wirksamkeit der Maßnahmen im Zusammenhang mit dem Erreger SARS-CoV-2 Daten an den für das Gesundheitswesen zuständigen Bundesminister zu übermitteln hat. Diese Bestimmung erscheint uns völlig unterverhältnismäßig, da sie die zuständigen Bundesminister zu einer de facto grenzenlosen Schaffung neuer Register und damit zusammenhängenden Datenverarbeitungen ermächtigt. Sie steht damit im Widerspruch zu den Anforderungen an eine hinreichende gesetzliche Determinierung und ist aus diesem Grund abzulehnen.

Lösungsvorschlag:

Streichung der Verordnungsermächtigung im letzten Satz in § 4 Abs 8a weitere Register in das EMS zu überführen.

Zu § 4 Abs 3a EpiG

§ 4 Abs 3a EpiG sieht vor, dass die ELGA GmbH berechtigt ist, auf Anforderung des Bundesministers die im zentralen Impfregister gespeicherten Daten über COVID-19-Impfungen einschließlich des bPK-GH an ihn zu übermitteln. Welche personenbezogenen Daten aus dem möglichen Pool des § 24c Abs 2 Z 2 lit a bis c GTelG 2012 zu übermitteln sind, bestimmt der Bundesminister in seiner Anforderung. Die Festlegung der zu übermittelnden Daten durch den Bundesminister sollte unserer Ansicht nach entfallen, zumal es sich um sensible Gesundheitsdaten handelt. Es obliegt dem Gesetzgeber zu bestimmen, welche Daten zur Erreichung der Zwecke des Abs 3a unbedingt erforderlich sind und eine entsprechende Übermittlungsermächtigung gesetzlich zu formulieren. Dabei ist auf den Grundsatz der Datenminimierung nach Art 5 Abs 1 lit c DSGVO Bedacht zu nehmen, wonach nur jene personenbezogene Daten verarbeitet werden dürfen, die zur Erreichung des Zwecks unbedingt erforderlich sind. Die Festlegung welche Daten diese Anforderung erfüllen, sollte der Gesetzgeber treffen und zwar auch im Hinblick auf eine hinreichende Bestimmtheit der gesetzlichen Grundlage. Dies erscheint auch vor dem bereits erwähnten Hintergrund der zahlreichen Verordnungsermächtigungen des Bundesministers als erforderlich.

Datenschutz-Folgenabschätzung

Die dem Entwurf beigefügte Datenschutzfolgenabschätzung folgt dem Schema der Artikel-29-Arbeitsgruppe (WP 248 rev.01)[5], erweist sich aber als lückenhaft und teilweise nicht nachvollziehbar.

Das Schema sieht eine Diskussion der getroffenen Maßnahmen zur Wahrung der Betroffenenrechte vor. Die Datenschutzfolgenabschätzung spart aber die Diskussion der Rechte auf Auskunft, Berichtigung, Löschung, Widerspruch sowie Einschränkung der Verarbeitung aus. Dies ist insbesondere aufgrund der wiederkehrenden Übermittlung von personenbezogenen Daten aus mehreren Quellen in ein zentrales System unzufriedenstellend, da alleine dieser Vorgang eine unübersichtliche Lage für die Ausübung der Betroffenenrechte erzeugt und Fragen bezüglich der Datenkonsistenz zwischen verschiedenen Systemen einen wesentlichen Einfluss auf die Ausübung dieser Rechte haben.

Im Zusammenhang mit der Überprüfung der ausgestellten Zertifikate stützt die Datenschutzfolgenabschätzung ihre Bewertung darauf, dass eine Überprüfung der Zertifikate ausschließlich offline erfolgt. Diese Tatsache ist aber inkongruent mit dem Gesetzestext, der eine Offline-Überprüfung nicht vorschreibt und lediglich eine Authentifizierung von Überprüfenden ausschließt. Es ergibt sich also die Möglichkeit, dass Überprüfungsmechanismen zum Einsatz kommen, die den Bestimmungen des § 4f entsprechen, nicht aber der Datenschutzfolgenabschätzung. Dem Anspruch des § 4b Abs. 9, die vorgenommene Datenschutzfolgenabschätzung zu § 4f (u.a.) erübrige weitere Datenschutzfolgenabschätzungen aufgrund des Art. 35 Abs. 10 DSGVO, kann die vorliegende Datenschutzfolgenabschätzung damit nicht gerecht werden.

Die Bewertung der Schwere bestimmter Risiken erfolgt anhand eines nicht durch genaue Quellenangabe belegten Schemas der französischen Regulierungsbehörde CNIL. Mit den Veröffentlichungen der CNIL zu einem "Privacy Impact Assessment"[6] sind die getroffenen Einschätzungen aber nicht kongruent und erweisen sich als zu niedrig. So identifiziert die Datenschutzfolgenabschätzung etwa beim Eintreten bestimmter Risiken ein erschwertes Fortkommen auf dem Arbeitsmarkt für Betroffene, konstatiert aber in diesem Zusammenhang eine "eingeschränkte" Schwere. Gemäß der Veröffentlichung der CNIL müsste aber mindestens eine Einstufung als "significant" erfolgen ("Targeted, unique and non-recurring, lost opportunities (e.g. home loan, refusal of studies, internships or employment, examination ban)").

Konsultation der Datenschutzbehörde

Der Verantwortliche hat nach Art 36 DSGVO vor der Verarbeitung die Datenschutzbehörde zu konsultieren, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

Hochriskante Verarbeitungen, deren Risiken mithilfe geeigneter Abhilfemaßnahmen nicht auf ein geringes und erträgliches Risiko gesenkt werden können, sind vor der Durchführung der Datenschutzbehörde anzuzeigen. Die Behörde hat sodann die Möglichkeit, die geplante Datenverarbeitung zu prüfen und dem Verantwortlichen schriftliche Empfehlungen zu unterbreiten.

5 https://ec.europa.eu/newsroom/article29/items/611236

6 https://www.cnil.fr/en/PIA-privacy-impact-assessment-en

Außerdem kann sie von ihren Befugnissen nach Art 58 DSGVO Gebrauch machen, also unter anderem die Datenverarbeitung einschränken oder gar untersagen.

Das Ministerium kommt in seiner Folgenabschätzung zum Ergebnis, dass mit der Verarbeitung bloß geringe bzw. mittlere Risiken einhergehen, welche mit bestimmten Abhilfemaßnahmen hinreichend begegnet werden kann. Dem kann in Anbetracht der geplanten Datenverarbeitungen keinesfalls gefolgt werden. Die Verarbeitung birgt aus unserer Sicht ein hohes Risiko, da sie eine sehr hohe Anzahl von Personen mit ihren sensiblen Gesundheitsdaten betrifft und diese aufgrund der technischen Ausgestaltung der EU-konformen Zertifikate und deren Verwendung für private Eintrittstest zu Betriebsstätten auch von einem besonders großen Kreis an Organisationen verarbeitet werden.

Vor diesem Hintergrund sollten die Begleitmaterialien des Gesetzes dahingehend angepasst werden, das eine Einbeziehung der Datenschutzbehörde rechtlich erforderlich ist. Da es bereits gemeinsame Runden der Datenschutzbehörde mit dem Gesundheitsministerium und anderen Datenschutzexpert*innen gab, erscheint diese Klarstellung der Erforderlichkeit nur korrekt.

Zu § 4b Abs 9 EpiG

Art 35 Abs 10 DSGVO befreit den Verantwortlichen von der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung, wenn eine solche bereits im Zusammenhang mit dem Erlass der Rechtsgrundlage erfolgte. Ob die Ausnahmebestimmung Anwendung findet, richtet sich danach, ob eine Folgenabschätzung tatsächlich stattgefunden hat. Eine gesetzliche Verankerung ist nicht notwendig und erscheint unionsrechtswidrig.

Es wird bereits in den Erläuterungen auf die durchgeführte Folgenabschätzung hingewiesen. Wir empfehlen daher, den gegenständlichen Passus ersatzlos zu streichen. Damit wird auch das Problem gelöst, dass die Regelung im Abs 9, welcher in einem Satz zuvor die Verarbeitung zur Fehlersuche und statistischen Auswertung behandelt, völlig fehl am Platz ist.

Lösungsvorschlag:

Streichung des § 4b Abs 9.

Gemeinsame Verantwortlichkeit

Zu § 4c Abs 3 Z 3 lit a EpiG

Nach dieser Bestimmung sind Betroffene an den zuständigen Verantwortlichen zu verweisen, wenn sie unter Nachweis ihrer Identität ihre Betroffenenrechte gegenüber einem unzuständigen Verantwortlichen wahrnehmen.

Diese Regelung steht im direkten Konflikt zu Art 26 Abs 3 DSGVO, wonach ungeachtet der Einzelheiten der Vereinbarung der gemeinsam Verantwortlichen die betroffene Person ihre (Betroffenen-)Rechte bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen kann.

Ungeachtet der getroffenen Zuständigkeitsregelungen können Betroffene ihre Rechte folglich beliebig gegenüber jedem der gemeinsam Verantwortlichen ausüben. Die Vereinbarung entfaltet somit ausschließlich rechtliche Wirkungen im Innenverhältnis zwischen den Verantwortlichen.

Der in Anspruch genommene Verantwortliche ist für die fristgerechte und rechtskonforme Behandlung verantwortlich, was bedeutet, dass der den internen Vereinbarungen zufolge

Unzuständige die Begehren entgegenzunehmen und dem zuständigen Verantwortlichen weiterzuleiten hat. Die Entscheidungsfrist der Verantwortlichen wird durch die Weiterleitung nicht unterbrochen.

Lösungsvorschlag:

Da § 4c Abs 3 Z 3 lit a EpiG im direkten Widerspruch zum Unionsrecht steht, wird empfohlen, ihn gänzlich zu streichen. Da § 26 Abs 3 DSGVO unmittelbar anwendbar ist, bedarf es auch keiner gesonderten gesetzlichen Regelung.

Mehrfachspeicherung von Impfzertifikaten

Zu § 4e Abs 4 und 5 EpiG

Der für das Gesundheitswesen zuständige Bundesminister hat das Impfzertifikat der ELGA GmbH zur Speicherung im zentralen Impfregister zu übermitteln. Diese hat das Zertifikat im zentralen Impfregister zu speichern und jenen Personen, die zum Zeitpunkt des Inkrafttretens dieser Bestimmung die Voraussetzungen für die Ausstellung erfüllen, eine gedruckte Fassung zur Verfügung zu stellen.

Eine doppelte Speicherung der Impfzertifikate, also sowohl im EPI-System als auch im zentralen Impfregister, erscheint in Anbetracht des Grundsatzes der Datenminimierung nach Art 5 Abs 1 lit c DSGVO unverhältnismäßig.

Lösungsvorschlag:

Die Erstellung der Impfzertifikate sollte aus unserer Sicht dort erfolgen, wo die Daten bereits heute vorliegen. Wenn die ELGA GmbH die Zertifikate erstellt und dann im Impfregister speichert, entfällt die Notwendigkeit diese Daten gemäß § 4e Abs. 4 im EPI-System zu speichern und der Grundsatz der Datenminimierung würde nicht gebrochen. Das EU-System sieht eindeutig die Möglichkeit vor, in einem Land verschiedene Stellen zu haben, die Zertifikate ausstellen können[7].

Hinweis:

Ungeklärt erscheint uns in der aktuellen Konstruktion ebenfalls das Problem der Betroffenenrechte im Falle eines Widerspruches gemäß § 4b Abs 8. Durch die Kopie der Daten in den Wirkungsbereich der ELGA GmbH muss die Durchsetzung der Betroffenenrechte und die Wahrung der Korrektheit der Daten mit einem noch zu schaffenden Mechanismus sichergestellt werden.

Unbeobachtbarkeit der Zertifikatsprüfung

Zu § 4f Abs 1 EpiG

Wir begrüßen diese wichtige Klarstellung, dass eine Authentifizierung von Überprüfenden zu unterbleiben hat. Jedoch impliziert diese Formulierung, dass die Überprüfung in einer zentralen Infrastruktur erfolgen könnte (wo eine Authentifizierung stattfinden könnte). Anders als im Verhandlungsmandat des Parlaments zur EU-Verordnung fehlt im vorliegenden Entwurf die kritische Klarstellung, wie die Überprüfung zu erfolgen hat.

7 https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v1_en.pdf (Seite 11)

Sollte dies mittels einer Online-Verifikation (zentrales System) passieren, wäre schon über die IP-Adresse der Überprüfenden eine Zuordnung möglich. In diesem Fall fiele an einer zentralen Stelle die Information an, wer (personenbezogenes Zertifikat), wo (IP-Adresse des Überprüfenden), wann (Zeitpunkt der Überprüfung) war (mittels Zertifikat um Eintritt ersucht hat). Hierbei ist zu beachten, dass auch die IP-Adresse, von der aus die Online-Prüfung stattfindet, ein personenbezogenes Datum darstellt.[8]

Der europäische Gesetzgeber verhandelt zum Zeitpunkt dieser Begutachtung gerade die EU-Verordnung für das Digital-Green-Certificate-System, welches dem Vernehmen nach auch in Österreich zur Anwendung kommen soll. In der Verhandlungsposition des Europaparlaments und in den letzten drei Verhandlungsentwürfen der portugisischen Ratspräsidentschaft für die gerade laufenden Trilogverhandlungen ist eine klare Festschreibung einer Offlineverifikation zu finden. Nicht nur würde Österreich ohne eine derartige gesetzlichen Klarstellung hinter das Datenschutzniveau des EU-Systems zurückfallen, dies wäre auch vor dem Hintergrund der eingriffsintensiveren Verwendung des österreichischen Systems für Eintrittstestungen in Gastronomie, religiösen Einrichtungen, Kultur- und Sportstätten sachlich nicht gerechtfertigt.

Die Forderung nach einer klaren Festlegung, dass nur eine unbeobachtbare Lösung, also eine Offline-Verifikation von Zertifikaten, mit den Datenschutzstandards Österreichs vereinbar ist, findet sich darüber hinaus in den letzten zwei Stellungnahmen des Datenschutzrates[9], der Stellungnahme der Bioethikkommission[10] und einem Positionspapier von Ärztekammer, WKÖ UBIT, ÖG Telemed und der Fachverband der Elektroindustrie[11].

Die vorgeschlagene Regelung genügt diesem Anspruch nicht. Unsere zentrale Forderung ist daher eine gesetzliche Festschreibung der Unbeobachtbarkeit des Überprüfungsvorgangs von Zertifikaten in Anlehnung an den derzeitigen Verhandlungsstand der EU-Verordnung[12].

Lösungsvorschlag:

Ergänzung eines § 4f Abs 7:

"Die Überprüfung der Integrität und Authentizität von Zertifikaten basiert auf einer Public-Key-Infrastruktur. Die Überprüfung erfolgt vollständig auf dem Endgerät des Überprüfenden und ohne den Aussteller des Zertifikats über den Vorgang oder die überprüfende Stelle in Kenntnis zu setzen. Zur Verhinderung von Missbrauch und Fälschungen der Zertifikate wird eine Liste an eindeutigen Identifikatoren der widerrufenen Zertifikate bereitgestellt."

Zu § 4b Abs 8 EpiG

Die Anforderung der Unbeobachtbarkeit muss auch im Bezug auf die technische Umsetzung des Widerrufs von Zertifikaten zur Anwendung kommen. Auf EU-Ebene findet sich im aktuellen Kompromissvorschlag der portugiesischen Ratspräsidentschaft in Erwägungsgrund 39 dazu eine

8 Siehe Erwägungsgrund 30 DSGVO.
9 Siehe https://www.bmj.gv.at/dam/jcr:6f7811d7-854f-4052-bccb-d39691227497/Stellungnahme%20des%20DSR%20;%20Vorhaben%20Digitales%20Gr%C3%BCnes%20Zertifikat.pdf und https://www.bmj.gv.at/dam/jcr:8bb4a62c-d489-4a24-9a6f-dc6c7fc94538/Stellungnahme%20des%20Datenschutzrates%20Gr%C3%BCner%20Pass.pdf
10 https://www.bundeskanzleramt.gv.at/dam/jcr:ba1f33aa-9a50-4e4f-a7d0-2e58eef34c89/Stellungnahme_COVID_April_2021.pdf
11 https://www.aerztekammer.at/documents/261766/548282/Green+Pass+WKO+%C3%96%C3%84K+%C3%96GTelemed+2021.pdf/02cf32c7-3f29-c9c0-5bda-5b38b3f53e5a
12 Siehe Artikel 4 Absatz 1a des Verhandlungsstands vom 17. Mai 2021 im Trilog.

Passage, die dafür eine Liste der widerrufenen Zertifikate vorsieht. Um Kompatibilität mit dem EU-System zu erreichen und eine möglichst datenschutzfreundliche Lösung zu erzielen, sollte dieses Modell auch in Österreich eingesetzt werden.

Lösungsvorschlag:

Ergänzung am Ende von § 4b Abs 8:

"(8) Ein fehlerhaftes Genesungs- oder Impfzertifikat ist auf Grund einer Information der sie betreffenden Person von dem für das Gesundheitswesen zuständigen Bundesminister vor Ablauf seiner Gültigkeitsdauer zu widerrufen. Der für das Gesundheitswesen zuständige Bundesminister hat eine Stelle zu benennen, die Informationen über fehlerhafte Zertifikate entgegennimmt. Widerrufene Zertifikate sind unverzüglich im EPI-Service zu löschen. ***Eine Liste der eindeutigen Identifikatoren der widerrufenen Zertifikate ist für den Überprüfungsvorgang bereit zu stellen. Hierbei werden keine sonstigen personenbezogenen Informationen über das Zertifikat übertragen****."*

Hinweis

Die Formulierung "auf Grund einer Information der sie betreffenden Person" im ersten Satz des § 4b Abs 8 impliziert der Widerruf eines Zertifikats wäre immer in einem Zusammenhang mit einer Information der betroffenen Person. Ein Widerruf kann gemäß der EU-Verordnung jedoch auch aufgrund von neuen wissenschaftlichen Erkenntnissen oder durch den Widerruf von missbräuchlich ausgestellten Zertifikaten durch den ausstellenden Staat erfolgen. Diese Formulierung könnte missverständlich ausgelegt werden.

Quelloffene Zertifikatsprüfung

Zu § 4f Abs 5 EpiG

Wir begrüßen die Verwendung von quelloffenem Code, um das Vertrauen der Bevölkerung in dieses System zu bestärken. Jedoch wäre es gerade im Hinblick auf das Vertrauen in der Bevölkerung und die Steigerung der Qualität der Programmierung sinnvoll, auch die abgeleiteten Anwendungen anderer überprüfenden Stellen und den gesamten Code des Systems (inklusive der Erstellung der Zertifikate) öffentlich einsehbar zur Verfügung zu stellen. Die Entwicklung des EU-Systems geht hier bereits mit einem guten Beispiel voran.

Insbesondere da eine Weiterverwendung der Daten aus dem Überprüfungsvorgang gemäß § 4f Abs 6 ausgeschlossen ist, wäre es eine enorm vertrauensbildende Maßnahme, auch die Anbieter von alternativen Anwendungen zur Überprüfung von Zertifikaten dazu zu verpflichten, ihren Quellcode offen zu legen. Es sollte jedenfalls die Referenzimplementierung der österreichischen Überprüfungssoftware unter einer freien Softwarelizenz veröffentlicht werden, die auch abgeleitete Programme zu einer quelloffenen Veröffentlichung verpflichtet.

Die gewählte Formulierung lässt offen, welcher Quellcode als Referenz für die Implementierung der Überprüfung herangezogen werden soll. Auf EU-Ebene gibt es bereits jetzt zwei Repositories von Quellcode.[13] Im Sinne des Bestimmtheitsgebot sollte hier nachgebessert werden.

13 https://github.com/ehn-digital-green-development
https://github.com/eu-digital-green-certificates

Lösungsvorschlag

§ 4f Abs 5 sollte wie folgt geändert werden:

"*Sofern eine elektronische Anwendung zur Verifizierung von Zertifikaten* ***gemäß den Vorgaben dieses Bundesgesetzes oder des COVID-19-Maßnahmengesetz*** *zur Anwendung kommt****, ist deren Quellcode öffentlich zu machen****.* ~~***den quelloffenen Prüfmechanismus nicht unverändert verwendet, ist dem für das Gesundheitswesen zuständigen Bundesministers der geänderte Source Code offen zu legen.***~~ ***Vom für das Gesundheitswesen zuständigen Bundesminister*** *vorgefundene Mängel sind unverzüglich zu beheben. Der für das Gesundheitswesen zuständige Bundesminister hat* ***eine solche Anwendung als Referenzimplementierung unter einer Lizenz bereitzustellen, die die Veröffentlichung des Quellcodes abgeleiteter Werke notwendig macht*** ~~***den Zugang zum quelloffenen Code für die Verifizierung von Zertifikaten auf geeignete Weise zu veröffentlichen***~~*."*

Hinweis

Der letzte Satz in § 4f Abs 5 ist eine Tautologie. Einen "quelloffenen Code" muss man nicht veröffentlichen, da er per Definition[14] bereits veröffentlicht ist.

Hinweis

Die Formulierung "zeitlich gültiges […] Zertifikat" in § 4f Abs 4 Z 1 und Z 2 impliziert, die Gültigkeit sei immer abhängig von der Zeit. Sollte ein Zertifikat widerrufen worden sein, zB weil ein Mitgliedstaat es in die Liste an widerrufenen Zertifikaten einträgt, wäre dies nicht der Fall.

14 https://www.duden.de/rechtschreibung/quelloffen