REPUBLIK ÖSTERREICH DATENSCHUTZRAT

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

Per E-Mail:
Vinzent.Rest@gesundheitsministerium.gv.at
Meinhild.Hausreither@gesundheitsministerium.gv.at
Engelbert.Prenner@gesundheitsministerium.gv.at

Geschäftszahl: 2021-0.332.347

BMJ - DSR (Geschäftsstelle des Datenschutzrates)
Kompetenzstelle GDSR
(Geschäftsstelle des Datenschutzrates)

dsr@bmj.gv.at
+43 1 52152 2918
Museumstraße 7, 1070 Wien

E-Mail-Antworten sind bitte unter Anführung der Geschäftszahl an dsr@bmj.gv.at zu richten.

GZ des Schreibens:
2021-0.323.900

Schreiben des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz betreffend Fragen von grundsätzlicher Bedeutung für den Datenschutz im Zusammenhang mit dem Grünen Pass; Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner fortgesetzten 257. Sitzung am 10. Mai 2021 **einstimmig beschlossen**, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Allgemeines

1 Das Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz hat dem Datenschutzrat mit Schreiben vom 5. Mai 2021 mitgeteilt, dass auf europäischer Ebene ein Legislativpaket der Europäischen Kommission betreffend den sogenannten „digitalen grünen Pass“ in Erarbeitung sei, das laut Zeitplan der Europäischen Kommission etwa Ende Juni 2021 in Kraft treten soll. Mit dieser EU-Verordnung soll ausschließlich die Rechtsgrundlage für die Erleichterung der Freizügigkeit („free movement“) geschaffen werden, allerdings sei in diesem Verordnungsentwurf ausdrücklich festgehalten, dass die in den Zertifikaten enthaltenen Daten zu anderen Zwecken verarbeitet werden dürfen, sofern es dafür im nationalen Recht eine hinreichend qualifizierte Rechtsgrundlage gibt.

2 In diesem Zusammenhang hat das Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz den Datenschutzrat unter Bezugnahme auf § 14 DSG um Befassung mit folgenden Fragen in der Sitzung am 6. Mai 2021 und Stellungnahme zu diesen Fragen ersucht:

1.) Im Hinblick auf die Gestaltung von Zertifikaten sowie die Ausgestaltung der Zugriffsmodalitäten stellt sich die Frage von grundsätzlicher Bedeutung für den Datenschutz, ob die im Schreiben des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz dargestellten Regelugen den datenschutzrechtlichen Anforderungen genügen.

2.) Im Hinblick auf die Überprüfung der Zertifikate, insbesondere auf die Zulässigkeit der Überprüfung mittels e-card, stellt sich die Frage von grundsätzlicher Bedeutung für den Datenschutz, ob die im Schreiben des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz dargestellten Regelugen den datenschutzrechtlichen Anforderungen genügen.

II. Datenschutzrechtliche Bemerkungen

A. Grundsätzliches

3 1. Vorweg wird festgehalten, dass das umfangreiche Schreiben des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz (mitsamt Auszügen von detaillierten Regelungen und Erklärungstext) erst am Tag vor der Sitzung am 6. Mai 2021 an den Datenschutzrat übermittelt wurde. Nachdem neben der inhaltlichen Prüfung des Vorhabens und der Erstellung einer diesbezüglichen Information auch den Mitgliedern des Datenschutzrates die Unterlagen entsprechend rechtzeitig für eine inhaltliche Durchsicht vor der Sitzung übermittelt werden müssen, kann eine seriöse vollständige, inhaltliche Prüfung der Fragestellungen anhand der komplexen datenschutzrechtlichen Regelungen in dieser Zeit nicht gewährleistet werden. Angesichts der komplexen technischen und rechtlichen Materie wäre eine Begutachtung im Gesetzgebungsverfahren angezeigt.

4 Der Datenschutzrat merkt weiters an, dass sich aus den übermittelten Gesetzestexten nicht unmittelbar ergibt, in welchem Gesetz die Änderungen erfolgen sollen. Der Datenschutzrat geht in der nachfolgenden Einschätzung davon aus, dass es sich um das Epidemiegesetz 1950 (EpiG) handelt.

5 2. Im Übrigen wird angemerkt, dass eine Prüfung der im Anhang im Rahmen des Erklärungstextes vorgelegten Datenschutz-Folgenabschätzung – sowohl aus Zeitgründen als auch mangels diesbezüglicher Fragestellungen – nicht durchgeführt wurde. Aus der Nichtprüfung der Datenschutz-Folgenabschätzung kann keine diesbezügliche inhaltliche Zustimmung des Datenschutzrates abgeleitet werden. Gleiches ist hinsichtlich des umfangreichen Erklärungstextes anzumerken.

6 Hinsichtlich der Datenschutz-Folgenabschätzung wird auf die Zuständigkeit der Datenschutzbehörde verwiesen.

7 3. Weiters stellt sich die grundsätzliche Frage nach dem Verhältnis der vorgelegten Regelungen zum auf Unionsebene in Vorbereitung befindlichen „digitalen grünen Pass“, der laut dem Schreiben des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz voraussichtlich etwa Ende Juni 2021 in Kraft treten soll. Hingewiesen wird idZ insbesondere auch darauf, dass auf Unionsebene ein dezentraler Ansatz verfolgt wird. Dies wäre in den vorliegenden Regelungen auch entsprechend zu berücksichtigen.

8 Unklar ist auch, wann die vorliegenden Regelungen in Kraft treten sollen. Jedenfalls wäre eine entsprechende „Sunset-Klausel“ vorzusehen.

9 Vor diesem Hintergrund stellt sich in Anbetracht der parallel stattfindenden Verhandlungen zu einer Verordnung auf Unionsebene, die bis Ende Juni auch grundlegende unionsweite Parameter für die Datenverarbeitungen festlegen wird, die grundsätzliche Frage, nach dem Grund und der Zweckmäßigkeit einer vorgezogenen Regelung auf nationaler Ebene in Unkenntnis der zeitnah zu erwartenden Unionsvorgaben.

10 4. Der Datenschutzrat merkt an, dass eine abschließende Gesamtbeurteilung der übermittelten Regelungen ausschließlich im Kontext eines Gesamtentwurfs erfolgen kann. Die Diskussion zu den gestellten Fragen wurde auf Montag, 10. Mai 2021, vertagt. Im Verlauf der fortgesetzten Sitzung wurden von den informierten Vertretern verschiedene Änderungen des zu den beiden Fragen vorgelegten Gesetzesentwurfes in Aussicht gestellt, insbesondere was den Entfall der e-card, die Verwendung der Sozialversicherungsnummer und die Kennnummer der e-card betrifft. Eine detaillierte Angabe der konkret angedachten Regelungen konnte nicht erfolgen. Die Grundlage für die nachfolgende Stellungnahme ist daher jener Gesetzesvorschlag, auf den sich die Fragen im Schreiben des BMSGPK vom 5. Mai 2021 beziehen.

B. Zur Frage 1.:

11 Allgemein stellt sich die grundlegende Frage, wie der Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz Daten aus dem Impfregister für die Ausstellung von Zertifikaten erhält.

12 Weiters ist unklar, wie ein niederschwelliger Zugang der betroffenen Personen zum einem Zertifikat in Papierform erfolgen kann.

Zu § 4b:

Zu Abs. 1:

13 Allgemein stellt sich in Bezug auf § 4b Abs. 1 die Frage, ob der Nachweis einer geringen epidemiologischen Gefahr in Bezug auf SARS-CoV-2 ausschließlich durch die in den §§ 4c bis 4e geregelten innerstaatlichen Zertifikate erfolgen kann oder auch ausländische Zertifikate bzw. sonstige Nachweise (zB internationaler Impfpass) verwendet werden dürfen (vgl. in diesem Zusammenhang § 4b Abs. 6, demzufolge die Ausstellung und Bereitstellung durch den für das Gesundheitswesen zuständigen Bundesminister zu erfolgen hat). Dies sollte in den Materialien ausdrücklich klargestellt werden. Eine Regelung über den Umgang mit im Ausland – auch außerhalb der EU – ausgestellten Nachweisen wäre auch im Rahmen der in den Unterlagen angesprochenen Übergangslösung bis zu einer allfälligen Regelung dieser Frage in unmittelbar anwendbarem Unionsrecht jedenfalls geboten. Dies gilt insbesondere auch für im Ausland verabreichte Impfungen, die – anders als ein Test – möglicherweise aus verschiedenen Gründen (medizinischer Natur, Verfügbarkeit udgl.) nicht ohne Weiteres im Inland wiederholt werden können.

14 Darüber hinaus stellt sich allgemein die Frage, ob für alle in Österreich (dauerhaft oder temporär) aufhältigen Personen die Möglichkeit der Ausstellung von Test-, Genesungs- oder Impfzertifikaten gesichert ist oder sich hier – insbesondere im Hinblick auf die in § 4c Abs. 2, § 4d Abs. 2 und § 4e Abs. 2 vorgesehenen Registerabfragen im Zusammenhang mit der Erstellung von Zertifikaten – Einschränkungen oder Zugangslücken ergeben können.

Zu Abs. 5:

15 Mit der Verordnungsermächtigung in § 4b Abs. 5 letzter Satz wird der für das Gesundheitswesen zuständige Bundesminister dazu ermächtigt, mit Verordnung Änderungen von Feldbezeichnungen vornehmen, Zusatzinformationen und nähere Vorgaben zur Gewährleistung der Barrierefreiheit festzulegen. Völlig unklar ist, was mit Änderungen von Feldbezeichnungen und welche Zusatzinformationen gemeint sind bzw. ob mit dieser

Verordnung (etwa im Wege der Änderung von Feldbezeichnungen) auch die Verarbeitung von (allenfalls zusätzlichen) personenbezogenen Daten vorgesehen ist.

16 Zur erforderlichen Vorhersehbarkeit der Verarbeitung von personenbezogenen Daten aus dem Gesetz wird neuerlich auf die Rechtsprechung des Verfassungsgerichtshofs zur Ermächtigungsnorm für Eingriffe in das Grundrecht auf Datenschutz im Sinne des § 1 Abs. 2 DSG hingewiesen, welche ausreichend präzise, also für jedermann vorhersehbar, bezeichnen muss, unter welchen Voraussetzungen die Ermittlung bzw. die Verarbeitung der Daten für die Wahrnehmung konkreter Verwaltungsaufgaben zulässig ist (VfSlg. 18.146/2007; 16.369/2001; zuletzt Erkenntnis vom 11.12.2019, G 72-74/2019 ua., Rz 64 ff).

Zu Abs. 6:

17 Aus der Regelung geht nicht hervor, wer für die Ausstellung der Zertifikate bzw. für die Bereitstellung derselben auf Aufforderung der sie betreffenden Person zuständig ist.

Zu Abs. 7:

18 In § 4b Abs. 7 wird hinsichtlich des Ausdruckens der Zertifikate durch die Gemeinden, die Bezirksverwaltungsbehörden und die ELGA-Ombudsstelle vorgesehen, dass diese Stellen als Verantwortlicher gemäß Art. 4 Z 7 DSGVO tätig werden. Vorweg sollte in diesem Zusammenhang geklärt werden, ob tatsächlich die „Gemeinde“ als juristische Person oder aber ein Organ der Gemeinde (zB der Bürgermeister) Verantwortlicher sein soll. Auch fehlen bei einer Verantwortlichkeit dieser Stellen entsprechende Vorgaben für die Löschung der erhobenen Daten. Insbesondere wäre dabei zu berücksichtigen, dass es sich um besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO handelt (etwa auch hinsichtlich der vom Verantwortlichen zu ergreifenden Datensicherheits-maßnahmen, damit nicht unbeteiligten Dritten zB am Gemeindeamt Kenntnis von dem Inhalt des Zertifikats erlangen).

19 Hinsichtlich der Bereitstellung einer Portalverbundanwendung – wird auf die für E-Government-Angelegenheiten zuständige Abteilung im Bundesministerium für Digitalisierung und Wirtschaftsstandort verwiesen.

Zu Abs. 8:

20 Im Zusammenhang mit dem in § 4b Abs. 8 vorgesehenen Widerruf von Zertifikaten stellt sich die Frage, welche Auswirkungen dies auf Papierausdrucke von Zertifikaten hat. Unklar ist auch, wie die betroffene Person vom Widerruf des Zertifikats Kenntnis erlangt und ob in diesem Zusammenhang allfällige Ansprüche entstehen können (wenn zB aufgrund des

nachträglichen Widerrufs der Zutritt zu einer Veranstaltung oder der Antritt einer Flugreise verwehrt wird). In diesem Zusammenhang erscheint eine möglichst zeitnahe aktive Information der betroffenen Person über den Widerruf eines zunächst gültigen Zertifikats (vgl. Art. 14 DSGVO) geboten. Die Bezugnahme auf die „diesbezügliche[n] Information der sie betreffenden Person" ist unverständlich und zweideutig (informiert die betreffende Person selbst oder wird sie informiert). Vor diesem Hintergrund sollte der erste Satz des Abs. 8 nochmals überarbeitet und klarer formuliert werden.

21 Völlig offen lässt Abs. 8, welche „Stelle" die Informationen über fehlerhafte Zertifikate entgegennimmt, ob und welche personenbezogenen Daten diese „Stelle" verarbeitet (und in welcher datenschutzrechtlichen Rolle diese „Stelle" diesfalls tätig wird) und in welcher rechtlichen Form (zB als Verordnung) der für das Gesundheitswesen zuständige Bundesminister die „Stelle" benennt. Weiters erscheint unklar, wer die Stelle von einem fehlerhaften Zertifikat informiert.

Zu Abs. 9:

22 Zu § 4b Abs. 9, demzufolge die auf Grundlage der §§ 4b bis 4f vorzunehmenden Datenverarbeitungen die Voraussetzungen des Art. 35 Abs. 10 DSGVO für den Entfall einer Datenschutz-Folgenabschätzung erfüllen, wird darauf hingewiesen, dass im Falle einer allfälligen Vorwegnahme der Datenschutz-Folgenabschätzung im Rahmen der allgemeinen Folgenabschätzung die Durchführung der Datenschutz-Folgenabschätzung gemäß den Vorgaben des Art. 35 Abs. 7 DSGVO in den Erläuterungen ausführlich dargelegt werden sollte. Inwiefern die Ausführungen in den Erläuterungen zur Datenschutz-Folgenabschätzung diesen Vorgaben entsprechen, kann in der vorgesehenen Begutachtungszeit für den Entwurf nicht geprüft werden. Eine normative Festlegung, dass die Voraussetzungen des Art. 35 Abs. 10 DSGVO erfüllt sind und die Datenschutz-Folgenabschätzung entfällt, ist mit dem Unionsrecht unvereinbar und kann im nationalen Recht jedenfalls nicht getroffen werden. Abs. 9 letzter Satz hat daher bei sonstiger Unionsrechtswidrigkeit ersatzlos zu entfallen.

23 Im Übrigen wird angemerkt, dass sich der inhaltliche Zusammenhang zwischen dem ersten und dem zweiten Satz des Abs. 9 nicht erschließt. Das Problem wäre durch den ohnedies gebotenen Entfall des zweiten Satzes des Abs. 9 jedoch gelöst.

Zu § 4c:

24 Zu § 4c Abs. 2 wird darauf hingewiesen, dass hinsichtlich der Einbindung der Stammzahlenregisterbehörde mit der E-Government-Abteilung im Bundesministerium für Digitalisierung und Wirtschaftsstandort in Kontakt getreten werden sollte.

25 Wie der Datenschutzrat bereits in mehreren Stellungnahmen (zB in der Stellungnahme vom 25. Februar 2010, GZ BKA-817.246/0002-DSR/2010) zur Verwendung der Sozialversicherungsnummer ausgeführt hat, ist die Verwendung der Sozialversicherungsnummer für Bereiche, die nicht in der Ingerenz der Sozialversicherung liegen, aus datenschutzrechtlicher Sicht abzulehnen und den E-Government-Lösungen des Bundes unter Gewähr der höchstmöglichen Datensicherheitsmaßnahmen der Vorzug zu geben. In den Materialien sollte daher dargelegt werden, inwiefern diesen Vorgaben des Datenschutzrates im Entwurf generell und im vorliegenden Kontext in § 4 Abs. 2 speziell entsprochen wird.

26 § 4c Abs. 3 legt eine gemeinsame Verantwortlichkeit des für das Gesundheitswesen zuständige Bundesministers und die übermittelnden Einrichtungen gemäß Art. 26 DSGVO fest. Fraglich ist vorweg, auf welche Regelung sich die Formulierung im Einleitungssatz („Im Anwendungsbereich dieser Bestimmung“) überhaupt bezieht. Zudem stellt sich die Frage, wie (bzw. in welcher Datenbank oder in welchem Register) diese Daten „gemeinsam“ verarbeitet werden oder um welche gemeinsame Datenverarbeitung es sich überhaupt handeln soll, zumal offenbar nur der Bundesminister gemäß Abs. 3 Z 1 Verantwortlicher für das das EPI-Service ist und die übermittelnden Einrichtungen keine Daten im EPI-Service verarbeiten, sondern diese wohl nur Daten an den Bundesminister als Verantwortlichen des EPI-Service übermitteln. Im Ergebnis scheint die Einordnung als gemeinsam für die Verarbeitung Verantwortliche gemäß Art. 26 DSGVO nicht der realen Rollenverteilung zu entsprechen und sollte nochmals geprüft werden.

27 Im Übrigen wird im Hinblick auf die Verteilung der Pflichten der gemeinsam für die Verarbeitung Verantwortlichen darauf hingewiesen, dass gemäß Art. 26 Abs. 3 DSGVO die betroffene Person ihre Rechte im Rahmen der DSGVO auch bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen kann. Die Erfüllung sämtlicher dieser Rechte muss unabhängig von der gewählten Pflichtenverteilung für alle Bestandteile der Datenverarbeitung sichergestellt werden. Die Pflichtenverteilung sollte dahingehend nochmals geprüft werden.

28 Hinsichtlich der in Abs. 4 vorgesehenen Verordnungsermächtigung wird auf die obigen Anmerkungen zur Vorhersehbarkeit und zur Rechtsprechung des Verfassungsgerichtshofes verwiesen. Dies sollte entsprechend geprüft werden.

Zu § 4d:

29 Zur in § 4d Abs. 2 vorgesehenen Ermittlung des bPK-GH mittels Abfrage des Zentralen Melderegisters im Wege der Stammzahlregisterbehörde sowie zur Verwendung der

Sozialversicherungsnummer wird auf die diesbezüglichen Anmerkungen zu § 4c Abs. 2 verwiesen.

30 Es stellt sich die Frage, weshalb nicht für das Genesungszertifikat eine Abfrage des Bundesministers für das Impfregister vorgesehen wird. Unklar ist jedoch, wie oder von wem die sonstigen für das Genesungszertifikat erforderlichen Daten an den Bundesminister übermittelt werden. Zudem sollte die „Schnittstellendefinition“ ausführlicher geregelt werden, dies vor allem vor dem Hintergrund, dass es sich um besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO handelt.

31 Hinsichtlich der Verordnungsermächtigung in Abs. 3 wird auf die obigen Anmerkungen zur Vorhersehbarkeit und zur Rechtsprechung des Verfassungsgerichtshofes verwiesen. Dies sollte entsprechend geprüft werden.

Zu § 4e:

32 Es wird angeregt, den Ablauf der Erstellung der Impfzertifikate zu prüfen. Nach dem vorgeschlagenen § 4e werden zunächst personenbezogene Daten aus dem zentralen Impfregister (§ 24c GTelG 2012) von der ELGA GmbH an den für das Gesundheitswesen zuständigen Bundesminister übermittelt (Abs. 2); in der Folge erstellt dieser die Impfzertifikate (Abs. 3), die danach wiederum der ELGA-GmbH zur Speicherung im zentralen Impfregister übermittelt werden (Abs. 4).

33 Im Hinblick darauf, dass der für das Gesundheitswesen zuständige Bundesminister im Zusammenhang mit dem zentralen Impfregister gemeinsam Verantwortlicher im Sinne des Art. 26 DSGVO ist (vgl. § 24c Abs. 3a GTelG 2012), stellt sich die Frage, warum die Erstellung der Impfzertifikate nicht unmittelbar aus dem zentralen Impfregister erfolgen kann, womit nur eine Datenübermittlung (aus dem zentralen Impfregister in das EPI-Service) erforderlich wäre.

34 Unbeschadet dessen ist – insbesondere vor dem Hintergrund des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) – auch die parallele Speicherung des Impfzertifikats in verschiedenen Registern (einerseits im EPI-Service und andererseits im Impfregister) kritisch zu hinterfragen. Soweit es um die Abrufbarkeit geht, könnte dies durch entsprechende Zugriffsmöglichkeiten von Gesundheitsdiensteanbietern auf das EPI-Service erfolgen. Der Abruf von Impfzertifikaten aus dem Impfregister wäre zwar grundsätzlich systemkonform, entspricht aber nicht dem – aus datenschutzrechtlicher Sicht keinesfalls wünschenswerten, aber im EpiG gewählten – Ansatz, ein zentrales Register für Test-, Genesungs- und Impfzertifikate zu schaffen, in dem die Daten aus

verschiedenen Registern zusammengeführt werden. Durch die Duplizierung von Daten aus dem EPI-Service in den ursprünglichen Registern wird dies noch weiter verschärft.

35 Die Verordnungsermächtigung in Abs. 3 sieht für den für das Gesundheitswesen zuständigen Bundesminister die Möglichkeit der Festlegung eines abweichenden Ausstellungszeitpunkts für das Impfzertifikat vor. Soweit ersichtlich wird in § 4c jedoch überhaupt kein Ausstellungszeitpunkt festgelegt, von dem abgewichen werden könnte.

36 Im Hinblick auf Abs. 4 ist fraglich, in welcher datenschutzrechtliche Rollen die Impfstellen das Zertifikat ausdrucken. Dies sollte ergänzt werden.

37 Zu § 4e Abs. 6 wird angeregt, hinsichtlich des Ablaufs der Speicherfrist im EPI-Service an das Ende der Geltungsdauer (und nicht an den Zeitpunkt der Übermittlung des Impfzertifikats an das zentrale Impfregister) anzuknüpfen.

C. Zur Frage 2.:

Zu § 4f:

38 Die vorgeschlagene Variante des Abrufs des Zertifikats mittels e-card würde bedeuten, dass der COVID-Status aller in Österreich Sozialversicherten – laut § 4f Abs. 6 des Entwurfs bestehend aus der Information „gültig“, wenn ein zeitlich gültiges Test-, Genesungs- oder ein Impfzertifikat verfügbar ist, oder „abgelaufen“ (rot oder grün), sowie Vorname, Nachname und Geburtsdatum – öffentlich von jedermann abgerufen werden kann. Die Abrufmöglichkeit bestünde unabhängig davon, ob sich ein Betroffener dafür entscheidet, von der Nachweismöglichkeit mittels e-card überhaupt Gebrauch zu machen.

39 Es ist darauf hinzuweisen, dass es sich beim Status „gültig“ oder „abgelaufen“ um Gesundheitsdaten und somit um besondere Kategorien personenbezogener Daten iSd Art. 9 Abs. 1 DSGVO handelt, da sich der Status „gültig“ oder „abgelaufen“ auf die körperliche Gesundheit einer natürlichen Person bezieht und daraus an sich bereits Informationen über den Gesundheitszustand hervorgehen, nämlich insbesondere aus dem Status „gültig“ die Information, dass der Betroffene aktuell nicht an COVID-19 erkrankt ist, und damit die Definition des Art. 4 Z 15 DSGVO erfüllt ist. Überdies beziehen sich auch alle drei möglichen Datenquellen (Test-, Genesungs- oder Impfzertifikat) auf die körperliche oder geistige Gesundheit einer natürlichen Person und es gehen daraus Informationen über den Gesundheitszustand hervor.

40 Der Umstand, dass der Zugang nur mittels der Kennnummer der e-card des Betroffenen möglich ist, stellt keine ausreichende Hürde dar, um Missbrauch zu verhindern. Es ist nicht davon auszugehen, dass Betroffene ihre Kennnummer der e-card bzw. Scans oder Fotokopien ihrer e-card bisher noch nie Dritten preisgegeben haben. Ein besonderer Anreiz, diese geheim zu halten, bestand bisher nicht, sondern entsteht erst mit dem hier vorgeschlagenen System. So ist die Kennnummer der e-card beispielsweise in bestimmen Steuerangelegenheiten erforderlich und es ist in der Unternehmenspraxis durchaus üblich, Scans bzw. Fotokopien der e-card im Zuge der Aufnahme von Mitarbeitern zu verarbeiten und zum Teil sogar zu archivieren. Unabhängig von der Frage der Rechtmäßigkeit dieses Vorgehens ist darauf hinzuweisen, dass Betroffene in der Praxis häufig keine Wahl haben, ob sie diese Daten preisgeben.

41 Darüber hinaus besteht ein Missbrauchspotenzial durch automatisierten massenhaften Abruf der Daten: Da die ersten zehn Stellen der Kennnummer der e-card stets gleich und damit nur neun Stellen der Kennnummer der e-card variabel sind, ist es einem Angreifer sehr leicht möglich, Software zu erstellen, die den Abruf der Daten für alle theoretisch möglichen Kennnummern der e-card der Reihe nach durchprobiert und auf diese Weise die oben genannten Gesundheitsdaten aller in Österreich Sozialversicherten inkl. Vorname, Nachname und Geburtsdatum abruft. Durch mehrfachen Abruf zu verschiedenen Zeitpunkten könnte sogar darauf geschlossen werden, ob der Status von einem Test herrührt oder von einer Immunität. Es gibt Mechanismen, einen solchen massenhaften Abruf zu erschweren oder zu verhindern, insbesondere Rate Limiting, sogenannte Captchas oder das Erfordernis eines Log-in. Davon abgesehen, dass ein Log-in das aufgrund der zentralen Verifikation vorhandene Datenschutzproblem der Beobachtbarkeit des Verhaltens der Betroffenen weiter erhöhen würde (siehe dazu unten), würden alle diese Mechanismen im vorliegenden Fall auch die zweckkonforme Verwendung des vorgeschlagenen Systems erschweren oder verhindern, man denke zB an die Einlasskontrolle bei einem großen Stadion, die eine rasche Abwicklung erfordert. Es ist daher zu bezweifeln, dass dem hier beschriebenen Missbrauchsszenario durch solche Maßnahmen wirksam begegnet werden kann, ohne das System für solche Anwendungsfälle faktisch unbrauchbar zu machen. Die vorgeschlagene Variante des Abrufs des Zertifikats mittels e-card stellt daher einen weitreichenden Eingriff in das Grundrecht auf Datenschutz des § 1 Abs. 1 DSG dar, für den eine Rechtfertigung weder dargelegt wurde noch ersichtlich ist, und weist weitreichende Datenschutzrisiken auf.

42 Mit der Verifizierung des Zertifikats mittels QR-Code liegt bereits eine Variante zur Erreichung des verfolgten Zwecks vor, welche die soeben beschriebenen Datenschutz-probleme nicht aufweist und daher im Vergleich zur Variante mittels e-card das gelindere

Mittel darstellt. Aus diesem Umstand, sowie aus dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO und insbesondere mangels einer Rechtfertigung für den damit einhergehenden weitreichenden Grundrechtseingriff spricht sich der Datenschutzrat gegen die vorgeschlagene Variante des Abrufs des Zertifikats mittels e-card aus.

43 Das in § 4f Abs. 1 letzter Satz ausdrücklich vorgesehene Unterbleiben der Authentifizierung des Überprüfenden hat Auswirkungen auf das Auskunftsrecht der betroffenen Person, da damit eine Beauskunftung der Identität von Empfängern im Rahmen des datenschutzrechtlichen Auskunftsrechts (vgl. Art. 15 Abs. 1 lit. c DSGVO) in Bezug auf die Überprüfer des Zertifikats wohl verunmöglicht wird. Es wird darauf hingewiesen, dass gesetzliche Beschränkungen der datenschutzrechtlichen Betroffenenrechte nur im Rahmen der Vorgaben des Art. 23 DSGVO zulässig sind, die vorliegend nicht erfüllt zu sein scheinen.

44 Vom informierten Vertreter des BMSGPK wurde in der Sitzung des Datenschutzrates am 6. Mai 2021 ausgeführt, dass die Sozialversicherungsnummer für die Abfrage der Zertifikate nicht mehr genutzt werden soll. Für den Fall, dass die Sozialversicherungsnummer doch beibehalten werden sollte, merkt der Datenschutzrat Folgendes an: In § 4f Abs. 5 ist unklar, wie die Sozialversicherungsnummer überhaupt ermittelt wird („abgelesen“ wird offenbar nur die Kennnummer der e-card) und von wem die Kartennummer bzw. die Sozialversicherungsnummer wo „eingegeben“ werden soll.

45 Weiters erscheint zweifelhaft, ob das Ablesen der Kennnummer von der e-card – im Sinne einer optischen Prüfung – tatsächlich auf eine Wahrnehmung nur dieser einen hier relevanten darauf abgedruckter Informationen beschränkt werden kann. Die – grundsätzlich rechtlich in sehr engem Rahmen geregelte – Verwendung der e-card bzw. im Falle der Verwendung der Sozialversicherungsnummer im vorliegenden Kontext (etwa Prüfung durch den Gastwirt beim Betreten eines Lokals) zum Zweck der Konsumation erscheint völlig systemfremd. Darüber hinaus eröffnet die Verwendung der Sozialversicherungsnummer bzw. der e-card die Gefahr, dass der Gesundheitsstatus von Betroffenen (zB am Arbeitsplatz, im Gesundheitswesen etc.) ohne deren Wissen und Zutun überprüft werden kann, indem Stellen, die bereits über die jeweiligen Sozialversicherungsnummern verfügen, diese unzulässigerweise für entsprechende Abfragen verwenden. Zur Verwendung der e-card und allfällig der Sozialversicherungsnummer wird daher erneut auf die diesbezügliche Anmerkung zu § 4c Abs. 2 verwiesen.

46 Vom informierten Vertreter des Dachverbandes der Sozialversicherungsträger wurde in der Sitzung des Datenschutzrates am 6. Mai 2021 ausgeführt, dass für die Abfrage der Zertifikate mittels „Green Check“ eine Web-App verwendet werden soll.

47 Im Übrigen wird auf die einstimmig beschlossene Stellungnahme des Datenschutzrates vom 2. April 2021 verwiesen, wonach für die österreichische Implementierung der Unionsvorgaben für ein Digitales Grünes Zertifikat bzw. für eine entsprechende österreichische Übergangslösung nur eine dezentrale Verifikation vorgesehen werden soll. Die in § 4f Abs. 5 vorgesehene Möglichkeit des Abrufs des Zertifikats mittels e-card erfüllt diese Voraussetzung nicht. Im Sinne der Datenminimierung wäre es geboten, dass die betreffende Information nur am jeweiligen Endgerät gespeichert ist. Hingewiesen wird auch darauf, dass auf Unionsebene (Digital Green Certificate) ein dezentraler Ansatz verfolgt wird.

48 Allgemein stellt sich auch die Frage, weshalb für den Nachweis der Identität nicht auf die E-ID (bzw. die Handy-Signatur), sondern auf die nur für Zwecke der Sozialversicherung geschaffene e-card zurückgegriffen wird. Diesbezüglich wird auf die für E-Government-Angelegenheiten zuständige Abteilung im Bundesministerium für Digitalisierung und Wirtschaftsstandort verwiesen.

49 Soweit ersichtlich, überlässt es § 4f Abs. 8 zur Gänze dem für das Gesundheitswesen zuständigen Bundesminister, mit Verordnung „die Anforderungen für die Freischaltung des Abrufs von Zertifikaten aus dem EPI-Service für private und öffentliche Anbieter von Anwendungen für Bürgerinnen und Bürger“ festzulegen. Im Hinblick darauf, dass es sich um personenbezogene Daten aus dem Bereich der Hoheitsverwaltung handelt und die Zertifikate besondere Kategorien personenbezogener Daten (Information über den Immunitätsstatus) beinhalten, sollten vor dem Hintergrund der Vorgaben des § 1 Abs. 2 DSG betreffend Eingriffe in das Grundrecht auf Datenschutz die datenschutzrechtlich gebotenen Vorgaben für den Zugriff im Wege von Anwendungen Dritter auf gesetzlicher Ebene näher determiniert werden. Ebenfalls in Erwägung zu ziehen wäre allfällige vergaberechtliche Implikationen.

D. Empfehlungen

50 Zur geplanten Anwendung (Web-App) zur Verifizierung durch Auslesen des QR-Codes spricht sich der Datenschutzrat dafür aus, diese so zu implementieren, dass die Verifizierung auf dem Client erfolgt, sodass keinerlei Information zur Identität der betroffenen Person an einen Server übertragen wird, um die Anforderungen der

einstimmig beschlossenen Stellungnahme des Datenschutzrates vom 2. April 2021 hinsichtlich Unbeobachtbarkeit und Offline-Verifikation zu erfüllen, was laut den Ausführungen der informierten Vertreter technisch möglich ist. Der Datenschutzrat empfiehlt darüber hinaus, den Quellcode der Anwendung zu veröffentlichen, was dem Datenschutzrat in der Sitzung am 10. Mai seitens der informierten Vertreter bereits in Aussicht gestellt wurde, damit nachvollzogen werden kann, ob die Implementierung dieser Vorgabe und weiteren Datenschutz-Anforderungen entspricht. Aus diesem Grund sollte im Gesetz geregelt werden, dass die Verifizierung durch auslesen des QR-Codes auf dem Client zu erfolgen hat und keine personenbezogenen Daten an den Server übertragen werden.

51 Ein informierter Vertreter wies auf das Vorhaben der Einrichtung einer Ansprechstelle hin, an die sich Betroffene im Falle unrichtiger Daten bzw. falsch ausgestellter Zertifikate wenden können. Die Rechtsqualität der Zertifikate und die damit verbundenen Rechtschutzmöglichkeiten sind somit noch nicht hinreichend geklärt. Der Datenschutzrat ersucht um entsprechende Klarstellungen.

52 Der Datenschutzrat empfiehlt, die Notwendigkeit einer Befassung der Datenschutzbehörde nach Art. 36 Abs. 1 DSGVO im Rahmen der Datenschutz-Folgenabschätzung vertieft zu prüfen und gegebenenfalls die Nichtbefassung der Datenschutzbehörde weiter zu begründen, ebenso die Hinweise zu den Risikomitigierungsstrategien in der Datenschutz-Folgenabschätzung.

Für den Datenschutzrat
Der Vorsitzende:
OFENAUER
10. Mai 2021

Elektronisch gefertigt