1 von 33

Gemäß § 53 Abs. 4 GOG
an die Abgeordneten verteilt

(Pös. Sobotka)

Abänderungsantrag

der Abgeordneten Gabriela Schwarz, Ralph Schallmeiner,

zum Antrag der Abgeordneten Dr. Josef Smolle, Ralph Schallmeiner, Kolleginnen und Kollegen betreffend ein Bundesgesetz, mit dem das Epidemiegesetz 1950 und das COVID-19-Maßnahmengesetz geändert werden (1572/A)

Der Nationalrat wolle in zweiter Lesung beschließen:

Der eingangs genannte Gesetzesantrag wird wie folgt geändert:

a) In Artikel 1 erhält die Novellierungsanordnung die „Z 1"; folgende Z 2 bis 22 werden angefügt:

2. In § 4 Abs. 1 entfällt die Wortfolge ‚sowie zu Impfdaten aus dem zentralen Impfregister'.

3. § 4 Abs. 3a lautet:

‚(3a) Die ELGA GmbH ist berechtigt, auf Anforderung des für das Gesundheitswesen zuständigen Bundesministers die im zentralen Impfregister gespeicherten Daten über COVID-19-Impfungen einschließlich des bPK-GH an ihn zu übermitteln. Für die Übermittlung dieser Daten gilt § 6 des Gesundheitstelematikgesetzes 2012 – GTelG 2012, BGBl. I Nr. 111/2012. Die Anforderung des für das Gesundheitswesen zuständigen Bundesministers hat zu enthalten:

1. die Konkretisierung, welche der in § 24c Abs. 2 Z 2 lit a bis c GTelG 2012 bezeichneten Daten(kategorien) zu übermitteln sind,
2. die Angabe, ob und gegebenenfalls welche zielgruppenspezifische, altersgruppenspezifische oder geografische Einschränkung der zu übermittelnden Daten vorzunehmen ist und
3. die Periodizität der Datenübermittlung.

Der für das Gesundheitswesen zuständige Bundesminister ist berechtigt, die ihm von der ELGA GmbH übermittelten Daten mit dem Register zu verknüpfen und dürfen diese Daten zum Zweck des Ausbruchs- und Krisenmanagements, wie etwa für die Ermittlung von Impfdurchbrüchen, von Ausbruchsclustern oder für die Kontaktpersonennachverfolgung, verarbeitet werden. Die betroffenen Personen haben nach Maßgabe der technischen Verfügbarkeit das Recht, elektronisch im Wege des Zugangsportals (§ 23 GTelG 2012) Auskunft (Art. 15 DSGVO) über die sie betreffenden Protokolldaten (Abs. 9) zu erhalten. Das Auskunftsrecht kann durch die betroffenen Personen hinsichtlich der sie betreffenden Protokolldaten auch zumindest monatlich gegenüber dem für das Gesundheitswesen zuständigen Bundesminister geltend gemacht werden.'

4. In § 4 Abs. 4 Z 3 entfällt der zweite Beistrich am Ende der Ziffer.

5. § 4 Abs. 6 lautet:

‚(6) Jede Verarbeitung der im Register gespeicherten Daten darf nur in Vollziehung dieses Bundesgesetzes, in Vollziehung des Tuberkulosegesetzes sowie in Vollziehung des Zoonosengesetzes, BGBl. I Nr. 128/2005, erfolgen. Eine Übermittlung der nach den Bestimmungen dieses Bundesgesetzes verarbeiteten personenbezogenen Daten an Dritte und eine Weiterverarbeitung der personenbezogenen Daten zu anderen Zwecken ist nicht zulässig, soweit nicht in diesem Bundesgesetz ausdrücklich anderes bestimmt ist.'

6. § 4 Abs. 7 vorletzter Satz entfällt.

7. § 4 Abs. 18 bis 24 entfällt.

8. In § 4a Abs. 1 wird nach der Wort- und Zeichenfolge ‚§ 4 Abs. 3' *die Wort- und Zeichenfolge* „ und Abs. 3a' *eingefügt.*

9. In § 4a Abs. 6 wird nach der Wort- und Zeichenfolge „„Statistik Österreich"' *der Klammerausdruck* ‚(Bundesanstalt)' *eingefügt und folgender Satz angefügt:*

‚Der für das Gesundheitswesen zuständige Bundesminister ist berechtigt, die mit dem vbPK-AS versehenen COVID-19-bezogenen Daten des Statistik-Registers zum Zweck der Erstellung von Statistiken im Zusammenhang mit der epidemiologischen Überwachung sowie dem Monitoring der Wirksamkeit der Maßnahmen in Bezug auf die Bekämpfung von COVID-19 mit einem konkreten, näher zu bezeichnenden

Auftrag an die Bundesanstalt zu übermitteln und die Bundesanstalt erstellt aus den ihr übermittelten Daten die Statistik (§ 4 in Verbindung mit § 23 Abs. 1 Z 1 des Bundesstatistikgesetzes 2000, BGBl. I Nr. 163/1999). ‘

10. § 4b samt Überschrift lautet:

‚Zertifikate im Zusammenhang mit SARS-CoV-2

§ 4b. (1) Zum Nachweis der Durchführung eines Tests auf eine Infektion mit SARS-CoV-2, einer überstandenen Infektion mit SARS-CoV-2 und einer empfangenen Schutzimpfung gegen COVID-19 können folgende Zertifikate herangezogen werden:

1. ein Testzertifikat (§ 4c) über ein mittels NAAT- oder RAT-Test ermitteltes negatives SARS-CoV-2-Testergebnis oder
2. ein Genesungszertifikat (§ 4d) über den Umstand, dass die Person von einer mittels NAAT-Test oder mittels einer gemäß § 4d Abs. 4 festgelegten Testmethode nachgewiesenen SARS-CoV-2-Infektion genesen ist oder
3. ein Impfzertifikat (§ 4e) über eine erfolgte COVID-19-Schutzimpfung.

(2) Im Sinne des Abs. 1 Z 1 und 2 ist

1. „NAAT-Test“ ein molekularer Nukleinsäure-Amplifikationstest, insbesondere Verfahren der Reverse-Transkriptase-Polymerase-Kettenreaktion (RT-PCR), der schleifenvermittelten isothermalen Amplifikation (LAMP) und der transkriptionsvermittelten Amplifikation (TMA), die zum Nachweis des Vorhandenseins der SARS-CoV-2-Ribonukleinsäure (RNS) verwendet werden;
2. „RAT-Test“ ein Antigen-Schnelltest, nämlich Verfahren, die auf dem Nachweis viraler Proteine (Antigene) unter Verwendung eines Immuntests mit Seitenstrom-Immunoassay beruhen und in weniger als 30 Minuten zu einem Ergebnis führen; der für das Gesundheitswesen zuständige Bundesminister hat die jeweils aktuelle Liste der anerkannten Testmethoden bzw. -produkte auf der Webseite des Ressorts zu veröffentlichen;
3. „Antikörpertest“ ein laborgestützter Test, der an Blutproben (Serum, Plasma oder Vollblut) durchgeführt wird und darauf abzielt festzustellen, ob eine Person Antikörper gegen SARS-CoV-2 entwickelt hat, unabhängig davon, ob sie Symptome aufwies oder nicht; Der für das Gesundheitswesen zuständige Bundesminister hat die jeweils aktuelle Liste der anerkannten Testmethoden bzw. -produkte auf der Webseite des Ressorts zu veröffentlichen.

(3) Zum Zweck der Ausstellung und der Bereitstellung von Zertifikaten gemäß Abs. 1 hat der für das Gesundheitswesen zuständige Bundesminister als datenschutzrechtlich Verantwortlicher (Art. 4 Z 7 DSGVO) ein elektronisches Service („EPI-Service“) einzurichten und zu betreiben. Er kann sich dazu eines Auftragsverarbeiters bedienen.

(4) Die Ausstellung der Zertifikate hat nach Maßgabe der technischen Verfügbarkeit des EPI-Service und der dafür erforderlichen Daten in Form eines QR-Codes zu erfolgen, der

1. die jeweils notwendigen Daten nach den §§ 4c Abs. 1, 4d Abs. 1 oder 4e Abs. 1 enthält,
2. mit den auf europäischer Ebene allenfalls festgelegten inhaltlichen und technischen Vorgaben interoperabel ist und
3. die Überprüfung von Authentizität, Gültigkeit und Integrität des Zertifikats ermöglicht.

(5) Die Bereitstellung der Zertifikate hat mittels QR-Code und im PDF-Format zu erfolgen, wobei das PDF-Format neben dem QR-Code alle Daten des QR-Codes in menschenlesbarer Form zu enthalten hat. Die Feldbezeichnungen der Daten und allfällige Zusatzinformationen sind in deutscher und englischer Sprache anzugeben. Der für das Gesundheitswesen zuständige Bundesminister kann mit Verordnung Änderungen von Feldbezeichnungen vornehmen und nähere Vorgaben zur Gewährleistung der Barrierefreiheit festlegen.

(6) Die Ausstellung der Zertifikate und die Bereitstellung hat für die sie betreffende Person oder für ihre Vertretung kostenlos zu erfolgen. Dies gilt auch für die Bereitstellung von gedruckten Zertifikaten durch berechtigte Stellen.

(7) Der für das Gesundheitswesen zuständige Bundesminister hat:

1. den Landeshauptleuten als datenschutzrechtlich Verantwortliche (Art. 4 Z 7 DSGVO) den Abruf von Zertifikaten oder von Verweisen auf Zertifikate aus dem EPI-Service zum Zweck der elektronischen Weitergabe an die betroffenen Personen zu ermöglichen, wobei Abrufe

ausschließlich mittels bereichsspezifischem Personenkennzeichen Gesundheit (bPK-GH) und über ein gesichertes Netzwerk erfolgen dürfen. Jede über das für die elektronische Weitergabe von Zertifikaten oder Verweisen an Betroffene unbedingt erforderliche Ausmaß hinausgehende Verarbeitung von Daten ist unzulässig.

2. eine Portalverbundanwendung bereitzustellen, die es
   a) Gemeinden, Bezirksverwaltungsbehörden und der ELGA-Ombudsstelle als datenschutzrechtlich Verantwortliche (Art. 4 Z 7 DSGVO) ermöglicht, einer anfordernden Person Zertifikate (Abs. 1)) sowie
   b) den Kundenservicestellen der Österreichischen Gesundheitskasse als datenschutzrechtlich Verantwortliche (Art. 4 Z 7 DSGVO) ermöglicht, einer anfordernden Person das Impfzertifikat (Abs. 1 Z 3)

   in gedruckter Form zur Verfügung zu stellen. Zertifikate dürfen in gedruckter Form und auf Anforderung auch an die Vertretung der betroffenen Person ausgefolgt werden. Jede über das für den Druck von Zertifikaten unbedingt erforderliche Ausmaß hinausgehende Verarbeitung von Daten ist unzulssig.
3. für Bürgerinnen und Bürger die Möglichkeit zur Einsichtnahme, zum Druck und zum Download von Zertifikaten im Wege des Zugangsportals (§ 23 GTelG 2012) zu schaffen; Die Authentifizierung der Bürgerinnen und Bürger hat gemäß § 3 E-GovG zu erfolgen.

(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. Die benannte Stelle hat die Art des Fehlers zu erheben, für die Behebung des Fehlers zu sorgen und gegebenenfalls die Neuausstellung und Bereitstellung des Zertifikats binnen fünf Arbeitstagen an die betroffene Person zu veranlassen. Widerrufene Zertifikate sind unverzüglich im EPI-Service zu löschen.

(9) Die Verarbeitung von Daten gemäß Abs. 1 durch den für das Gesundheitswesen zuständigen Bundesminister ist außer zu den in den §§ 4b bis 4f genannten Zwecken, ausschließlich zur Fehlersuche und Fehlerbehebung sowie für statistische Auswertungen zulässig.

(10) Die für die Umsetzung der §§ 4b bis 4e erforderlichen Mittel sind den genannten Rechtsträgern aus dem COVID-19-Krisenbewältigungsfonds zu ersetzen.'

11. § 4c samt Überschrift lautet:

‚Testzertifikat

§ 4c. (1) Das Testzertifikat hat folgende Daten zu enthalten:

1. Nachname(n) und Vorname(n) der getesteten Person, in dieser Reihenfolge,
2. Geburtsdatum der getesteten Person,
3. Zielkrankheit oder -erreger, auf die oder den die Person getestet wurde, ausschließlich lautend auf „COVID-19“ (umfasst auch „SARS-CoV-2“ oder dessen Varianten),
4. Art des Tests,
5. Bezeichnung des Tests (optional bei NAAT-Tests),
6. Bezeichnung des Herstellers des Tests (optional bei NAAT-Tests),
7. Datum und Uhrzeit der Probenahme,
8. Testergebnis,
9. Bezeichnung des Testzentrums oder der testenden Einrichtung (optional bei RAT-Tests),
10. Bezeichnung des Staates, in dem der Test durchgeführt wurde,
11. Bezeichnung des Ausstellers des Testzertifikats,
12. eindeutige Kennung des Testzertifikats.

(2) Die Daten gemäß Abs. 1 Z 1 bis 9 sowie – falls verfügbar – die Sozialversicherungsnummer der getesteten Person sind von den Einrichtungen, die SARS-CoV-2-Tests im Sinne des § 4b Abs. 2 auswerten, das sind insbesondere Teststellen und Labore, unter Einhaltung des § 6 GTelG 2012 elektronisch in standardisierter Form an den für das Gesundheitswesen zuständigen Bundesminister zu übermitteln. Dabei sind die in § 4 Abs. 12 bis 14 vorgesehenen Datensicherheitsmaßnahmen zu ergreifen. Der für das Gesundheitswesen zuständige Bundesminister ermittelt aus den übermittelten Daten im Wege der Abfrage des Patientenindex (§ 4 in Verbindung mit § 18 GTelG 2012) oder – im Falle des Fehlens der Sozialversicherungsnummer – im Wege der Stammzahlenregisterbehörde das bereichsspezifische Personenkennzeichen Gesundheit (bPK-GH) und erstellt das Testzertifikat. Das Testzertifikat in den gemäß

§ 4b Abs. 5 festgelegten Formaten sowie das bPK-GH sind im EPI-Service zu speichern. Teststellen dürfen das Testzertifikat für die getestete Person ausdrucken; zu diesem Zweck darf ihnen das Testzertifikat vom für das Gesundheitswesen zuständigen Bundesminister übermittelt werden. Die Teststellen sind berechtigt, das Testzertifikat zu diesem Zweck in personenbezogener Form zu verarbeiten.

(3) Im Anwendungsbereich des § 4c sind der für das Gesundheitswesen zuständige Bundesminister und die übermittelnden Einrichtungen gemeinsam Verantwortliche im Sinne des Art. 4 Z 7 in Verbindung mit Art. 26 DSGVO:

1. Der für das Gesundheitswesen zuständige Bundesminister ist verantwortlich für die Einrichtung und den Betrieb des EPI-Service (§ 4b Abs. 3) und für die Ausstellung und Bereitstellung der Testzertifikate gemäß § 4b Abs. 1 Z 1. Ihm obliegen folgende aus der DSGVO resultierende Pflichten:
   a) Wahrnehmung von Anträgen gemäß Art. 15 DSGVO, sofern sie das EPI-Service betreffen;
   b) Sicherstellung der Datensicherheit hinsichtlich des EPI-Service;
   c) Wahrnehmung der Meldepflicht gemäß Art. 33 DSGVO sowie Benachrichtigung der betroffenen Personen gemäß Art. 34 DSGVO, sofern die Verletzung des Schutzes personenbezogener Daten im EPI-Service aufgetreten ist;
   d) Zurverfügungstellung des wesentlichen Inhalts der Pflichtenaufteilung in geeigneter Weise.
2. Die Einrichtungen, die SARS-CoV-2-Tests im Sinne des § 4b Abs. 2 auswerten, sind verantwortlich für die Ermittlung und Übermittlung der Testergebnisse. Ihnen obliegen folgende aus der DSGVO resultierende Pflichten:
   a) Information der betroffenen Personen gemäß Art. 13 DSGVO in geeigneter Weise;
   b) Wahrnehmung von Anträgen auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) und Einschränkung der Verarbeitung (Art. 18 DSGVO) hinsichtlich jener Daten, die von der jeweiligen Einrichtung verarbeitet werden;
   c) unverzügliche Benachrichtigung des für das Gesundheitswesen zuständigen Bundesministers über jede erfolgte Berichtigung oder Löschung oder Einschränkung der Verarbeitung (Art. 19 DSGVO) hinsichtlich jener Daten, die von der jeweiligen Einrichtung verarbeitet werden;
   d) Sicherstellung der Datensicherheit hinsichtlich der Ermittlung und Übermittlung der Daten, die die jeweilige Einrichtung verarbeitet;
   e) Wahrnehmung der Meldepflicht gemäß Art. 33 DSGVO sowie Benachrichtigung der betroffenen Personen gemäß Art. 34 DSGVO, sofern die Verletzung des Schutzes personenbezogener Daten bei der Ermittlung oder Übermittlung der Daten aufgetreten ist.
3. Sowohl dem für das Gesundheitswesen zuständigen Bundesminister als auch den Einrichtungen, die SARS-CoV-2-Tests im Sinne des § 4b Abs. 2 auswerten, obliegen folgende aus der DSGVO resultierende Pflichten:
   a) Verweis an den zuständigen Verantwortlichen, wenn eine betroffene Person unter Nachweis ihrer Identität ein Recht nach der DSGVO gegenüber einem unzuständigen Verantwortlichen wahrnimmt, wobei die betroffene Person entsprechend anzuleiten ist;
   b) Information der betroffenen Personen gemäß Art. 12 Abs. 4 DSGVO, wenn aufgrund von deren Anträgen kein Tätigwerden erfolgt;
   c) Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO sowie
   d) Zusammenarbeit mit der Aufsichtsbehörde gemäß Art. 31 DSGVO.

(4) Der für das Gesundheitswesen zuständige Bundesminister kann auf Grund neuer wissenschaftlicher Erkenntnisse oder Festlegungen auf europäischer Ebene mit Verordnung die Gültigkeitsdauer von Testzertifikaten gemäß Abs. 1 sowie deren Berechnungsmethode festlegen oder ändern.

(5) Sämtliche Daten im EPI-Service sind eine Woche ab dem Datum der Probenahme zu löschen.‘

12. Nach § 4c werden folgende §§ 4d bis 4f samt Überschriften eingefügt:

‚Genesungszertifikat

§ 4d. (1) Das Genesungszertifikat hat folgende Daten zu enthalten:

1. Nachname(n) und Vorname(n) der getesteten Person, in dieser Reihenfolge,
2. Geburtsdatum der getesteten Person,
3. Krankheit oder Erreger, von der oder dem die Person genesen ist, ausschließlich lautend auf „COVID-19“ (umfasst auch „SARS-CoV-2“ oder dessen Varianten),

4. Datum des ersten positiven NAAT-Testergebnisses,
5. Bezeichnung des Staates, in dem der Test durchgeführt wurde,
6. Bezeichnung des Ausstellers des Genesungszertifikats,
7. Gültigkeitsbeginn des Genesungszertifikats,
8. Gültigkeitsende des Genesungszertifikats,
9. eindeutige Kennung des Genesungszertifikats.

(2) Der für das Gesundheitswesen zuständige Bundesminister hat die Daten gemäß Abs. 1 Z 1 bis 4 sowie die Sozialversicherungsnummer aus dem Register gemäß § 4 und das bereichsspezifische Personenkennzeichen Gesundheit (bPK-GH) im Wege der Abfrage des Patientenindex (§ 4 in Verbindung mit § 18 GTelG 2012) oder – im Falle des Fehlens der Sozialversicherung – im Wege der Stammzahlenregisterbehörde zu ermitteln. Die ELGA GmbH hat für den Fall, dass Antikörpertests als Grundlage für die Ausstellung von Genesungszertifikaten festgelegt werden (Abs. 4), die für die Ausstellung von Genesungszertifikaten erforderlichen Daten gemäß Abs. 1 Z 1 bis 3 und 5 sowie das bPK-GH aus dem zentralen Impfregister (§ 24c GTelG 2012) zu ermitteln und dem für das Gesundheitswesen zuständigen Bundesminister unter Einhaltung des § 6 GTelG 2012 sowie der technisch-organisatorischen Vorgaben (Schnittstellendefinition) zu übermitteln. Genesungszertifikate sind vom für das Gesundheitswesen zuständigen Bundesminister auf Anforderung von Betroffenen auszustellen.

(3) Das Genesungszertifikat darf frühestens am elften Tag ab dem Datum des ersten positiven NAAT-Testergebnisses ausgestellt werden, seine Gültigkeitsdauer darf 180 Tage, gerechnet ab dem Datum des ersten positiven NAAT-Testergebnisses, nicht übersteigen.

(4) Mit Verordnung kann der für das Gesundheitswesen zuständige Bundesminister auf Grund neuer wissenschaftlicher Erkenntnisse oder diesbezüglicher Festlegungen auf europäischer Ebene bestimmen:

1. abweichende Ausstellungsfristen bzw. Gültigkeitsdauern,
2. dass, gegebenenfalls ab welchem Zeitpunkt und unter welchen Voraussetzungen weitere Testmethoden, insbesondere Antikörpertests, als Grundlage für die Ausstellung von Genesungszertifikaten verwendet werden dürfen.

(5) Das Genesungszertifikat in den gemäß § 4b Abs. 5 festgelegten Formaten sowie das bPK-GH sind im EPI-Service zu speichern.

(6) Sämtliche Daten im EPI-Service sind eine Woche nach Gültigkeitsende des Genesungszertifikats zu löschen.

Impfzertifikat

§ 4e. (1) Das Impfzertifikat hat folgende Daten zu enthalten:

1. Nachname(n) und Vorname(n) der geimpften Person in dieser Reihenfolge,
2. Geburtsdatum der geimpften Person,
3. Krankheit oder Erreger, gegen die oder den die Person geimpft ist, ausschließlich lautend auf „COVID-19“ (umfasst auch „SARS-CoV-2“ oder dessen Varianten),
4. Impfstoff/Prophylaxe (generische Beschreibung des Impfstoffs oder seiner Komponenten),
5. Impfarzneimittel (Bezeichnung des Impfstoffs gemäß Zulassung),
6. Zulassungsinhaber oder Hersteller des Impfstoffs,
7. Nummer der Impfdosis und die Gesamtanzahl der Impfdosen einer Impfserie,
8. Datum der letzten Impfung der Impfserie,
9. Bezeichnung des Staates, in dem die Impfung durchgeführt wurde,
10. Bezeichnung des Ausstellers des Impfzertifikats,
11. eindeutige Kennung des Impfzertifikats.

(2) Die ELGA GmbH hat die für die Ausstellung von Impfzertifikaten erforderlichen Daten gemäß Abs. 1 Z 1 bis 8, die Chargennummer des verabreichten Impfstoffs sowie das bPK-GH aus dem zentralen Impfregister (§ 24c GTelG 2012) zu ermitteln und dem für das Gesundheitswesen zuständigen Bundesminister unter Einhaltung des § 6 GTelG 2012 sowie der technisch-organisatorischen Vorgaben (Schnittstellendefinition) zu übermitteln.

(3) Mit Verordnung kann der für das Gesundheitswesen zuständige Bundesminister auf Grund neuer wissenschaftlicher Erkenntnisse oder diesbezüglicher Festlegungen auf europäischer Ebene einen abweichenden Ausstellungszeitpunkt oder die Gültigkeitsdauer und deren Berechnungsmethode für Impfzertifikate festlegen.

(4) Das Impfzertifikat in den gemäß § 4b Abs. 5 festgelegten Formaten sowie das bPK-GH werden im EPI-Service gespeichert. Impfstellen dürfen einer geimpften Person das Impfzertifikat ausdrucken, wofür ihnen das Impfzertifikat vom für das Gesundheitswesen zuständigen Bundesminister übermittelt werden darf. Zu diesem Zweck sind die Impfstellen berechtigt, das Impfzertifikat in personenbezogener Form zu verarbeiten.

(5) Der für das Gesundheitswesen zuständige Bundesminister hat das Impfzertifikat im PDF-Format samt bPK-GH der ELGA GmbH zur Speicherung im zentralen Impfregister zu übermitteln. Die ELGA GmbH hat das Impfzertifikat im zentralen Impfregister zu speichern und jenen Personen, bei denen zum Zeitpunkt des Inkrafttretens dieser Bestimmung die Impfserie abgeschlossen wurde, eine gedruckte Fassung des Impfzertifikats (PDF-Format) zur Verfügung zu stellen. Die ELGA GmbH hat eine für die Speicherung des Impfzertifikats im zentralen Impfregister sowie für den Druck und Versand von Impfzertifikaten beschränkte spezifische Zugriffsberechtigung im Sinne des § 24f Abs. 4 GTelG 2012.

(6) Bürgerinnen und Bürger können auf das Impfzertifikat auch im Wege des § 24e Abs. 1 Z 1 GTelG 2012 zugreifen. Niedergelassene Ärztinnen und Ärzte im Sinne des § 24c Abs. 2 Z 1 GTelG 2012, sowie Apotheken gemäß § 1 Apothekengesetz, RGBl. Nr. 5/1907, dürfen die im zentralen Impfregister verfügbar gemachten Impfzertifikate für die Bürgerinnen und Bürger ausdrucken und haben hierfür eine spezifische Zugriffsberechtigung im Sinne des § 24f Abs. 4 GTelG 2012.

(7) Sämtliche Daten im EPI-Service sind ein Jahr nach Übermittlung des Impfzertifikats an das zentrale Impfregister zu löschen.

Verarbeitung der Nachweise durch Überprüfende

§ 4f. (1) Überprüfende (§ 1 Abs. 5b Z 1 bis 3 des COVID-19-Maßnahmengesetzes – COVID-19-MG, BGBl. I Nr. 12/2020) dürfen Zertifikate gemäß § 4b Abs. 1 zum Zweck ihrer Verifizierung verarbeiten. Die Authentifizierung der Überprüfenden hat zu unterbleiben.

(2) Die Identifizierung einer Person durch Überprüfende hat anhand eines amtlichen Lichtbildausweises oder einer elektronischen Vorzeigemethode, die jedenfalls das kryptographisch gesicherte Bild aus einem amtlichen Lichtbildausweis der Person zu enthalten hat, zu erfolgen.

(3) Die Verifizierung von Zertifikaten durch Überprüfende darf ausschließlich auf dem Endgerät des Überprüfenden („offline") erfolgen und hat die Signaturprüfung, aus der die syntaktische und inhaltliche Korrektheit sowie die zeitliche Gültigkeit hervorzugehen hat, zu umfassen.

(4) Elektronische Anwendungen zur Verifizierung von Zertifikaten gemäß §§ 4c bis 4e haben – ausgenommen bei ihrer Verwendung beim Grenzübertritt – die bereitgestellten Zertifikatsdaten für Überprüfende eingeschränkt darzustellen, nämlich mit Nachname(n), Vorname(n) und dem Geburtsdatum der Person, für die das Zertifikat ausgestellt wurde, sowie text- und farbcodiert entweder mit

1. „gültig" (grün hinterlegt), wenn ein zeitlich gültiges Test-, Genesungs- oder ein Impfzertifikat verfügbar ist, oder
2. „ungültig" (rot hinterlegt), wenn kein zeitlich gültiges oder kein verifizierbares Zertifikat verfügbar ist.

(5) Elektronische Anwendungen zur Verifizierung von Zertifikaten dürfen folgende zusätzliche Informationen über die Ursache des Rückgabewerts „ungültig" (rot hinterlegt) der/dem Überprüfenden bereitstellen:

1. „Gültigkeitsdauer abgelaufen",
2. „QR-Code fehlerhaft",
3. „Signaturprüfung fehlgeschlagen".

(6) Sofern eine elektronische Anwendung zur Verifizierung von Zertifikaten den quelloffenen Prüfmechanismus nicht unverändert verwendet, ist dem für das Gesundheitswesen zuständigen Bundesminister der geänderte Source Code offen zu legen. Vorgefundene Mängel sind unverzüglich zu beheben. Der für das Gesundheitswesen zuständige Bundesminister hat den Zugang zum quelloffenen Code für die Verifizierung von Zertifikaten auf geeignete Weise zu veröffentlichen.

(7) Jede über das für die Verifizierung von Zertifikaten unbedingt erforderliche Ausmaß hinausgehende Verarbeitung von Daten durch Überprüfende ist unzulässig.'

13. In § 5 Abs. 4 wird vor der Zeichenfolge ‚(5)' *ein Absatz eingefügt.*

14. In § 5a Abs. 1 wird nach der Wortfolge ‚kann der Landeshauptmann' *die Wortfolge* ‚als datenschutzrechtlicher Verantwortlicher (Art. 4 Z 7 DSGVO)' *eingefügt.*

15. Der Klammerausdruck in § 5a Abs. 2 Z 1 lautet:

‚(Vor- und Zuname, Geschlecht, Geburtsdatum; die Sozialversicherungsnummer, falls verfügbar)'

16. § 5a Abs. 7 und 8 lauten:

‚(7) Screeningprogramme gemäß Abs. 1 können auch zum Zweck der Erlangung eines Testergebnisses durchgeführt werden, um die auf Grund dieses Bundesgesetzes oder des COVID-19-MG verordneten Voraussetzungen oder Auflagen zu erfüllen.

(8) Der Durchführende des Screeningprogramms hat der betroffenen Person einen Nachweis über das Ergebnis des Tests auszustellen. Dieser Nachweis ist der betroffenen Person entweder in gedruckter oder in elektronischer Form – sofern möglich unverzüglich – zur Verfügung zu stellen. Wird dieser Nachweis nicht in Form eines Testzertifikats (§ 4c) bereitgestellt, kann der für das Gesundheitswesen zuständige Bundesminister mit Verordnung nähere Bestimmungen über Form und Inhalt festlegen. In dieser Verordnung sind jedenfalls die in den Nachweis aufzunehmenden Daten anhand der Datenkategorien gemäß § 5b Abs. 3 zu konkretisieren. Die Daten sind vom Durchführenden des Screeningprogramms unverzüglich nach Bereitstellung des Nachweises für die betroffene Person zu löschen. Gesetzlich vorgesehene Aufbewahrungs- bzw. Dokumentationspflichten bleiben davon unberührt. Die Verarbeitung der Daten zu anderen Zwecken als zur Erstellung und Bereitstellung des Testzertifikats oder des Testnachweises ist unzulässig.'

17. § 25a Abs. 2 Z 3 lautet:

‚3. Wohn- und Aufenthaltsadresse, falls zutreffend,'

18. § 25a Abs. 2 Z 10 lautet:

‚10. Vorliegen eines ärztlichen Zeugnisses oder eines der in § 4b genannten Zertifikate.'

19. § 28a Abs. 1 wird folgender Satz angefügt:

‚Organe nach § des 12b Grenzkontrollgesetzes – GrekoG, BGBl. Nr. 435/1996, haben bei der Ausübung der ihnen nach § 12a GrekoG zukommenden Befugnisse die nach diesem Bundesgesetz zuständigen Behörden und Organe über deren Ersuchen bei der Ausübung ihrer gemäß § 25 beschriebenen Aufgaben zu unterstützen.'

20. In § 28d Abs. 1 Z 5 entfällt das Wort „und"*, in Z 6 wird nach der Zeichenfolge* „BGBl. I Nr. 96/1998," *das Wort* „ und" *eingefügt und nach Z 6 folgende Z 7 angefügt:*

‚7. Angehörige des tierärztlichen Berufes gemäß dem Bundesgesetz über den Tierarzt und seine berufliche Vertretung (Tierärztegesetz), BGBl. Nr. 16/1975,'

21. Dem § 28d Abs. 1 wird folgender Satz angefügt:

‚Die nach dieser Bestimmung tätigen Personen sind unbeschadet sonstiger Verschwiegenheitspflichten zur Verschwiegenheit über die im Rahmen ihrer Tätigkeit anvertrauten oder bekannt gewordenen Geheimnisse verpflichtet.'

22. Dem § 50 wird folgender Abs. 23 angefügt:

‚(23) Die Überschrift zu § 2, § 4 Abs. 1, Abs. 4 Z 3, Abs. 6 und Abs. 7, § 4a Abs. 1 und Abs. 6, § 5 Abs. 4, § 5a Abs. 1, Abs. 2 Z 1, Abs. 7 und Abs. 8, § 25a Abs. 2 Z 3 und Z 10, § 28a Abs. 1 sowie § 28d Abs. 1 in der Fassung des Bundesgesetzes BGBl. I Nr. xxx/2021 treten mit dem der Kundmachung folgenden Tag in Kraft; gleichzeitig tritt § 4 Abs. 18 bis 24 außer Kraft. § 4 Abs. 3a sowie §§ 4b bis 4f samt Überschriften treten mit 4. Juni 2021 in Kraft. §§ 4b bis 4f samt Überschriften treten mit Ablauf des 30. Juni 2022 außer Kraft.'"

b) in Artikel 2 erhält die Novellierungsanordnung die Z 11; folgende Z 1 bis 10 werden vorangestellt:

1. In § 1 entfällt Abs. 5b und die bisherigen Abs. 5c bis 5f erhalten die Absatzbezeichnungen ‚(5b)' *bis* ‚(5e)'.

2. In § 1 Abs. 5b (neu) wird die Wortfolge ‚einen Testnachweis gemäß Abs. 5b' *durch die Wortfolge* ‚ein Testzertifikat nach § 4c des Epidemiegesetzes 1950' *ersetzt.*

3. Dem § 1 Abs. 5b (neu) wird folgender Satz angefügt:

‚Dies gilt auch für Zertifikate nach § 4b Abs. 1 des Epidemiegesetzes 1950, BGBl. I Nr. 186/1950.'

4. § 1 Abs. 5c (neu) wird in Z 1 der Beistrich durch das Wort ‚oder' *ersetzt; die Z 3 enfällt und die Z 2 lautet:*

„2. einer überstandenen Infektion mit SARS-CoV-2,"

5. In § 1 Abs. 5d (neu) wird die Wortfolge ‚grundsätzlich geeignet sind, eine Gleichstellung im Sinne von Abs. 5d zu rechtfertigen.' *durch die Wortfolge* ‚geeignet sind, eine grundsätzliche Gleichstellung im Sinne von Abs. 5c zu rechtfertigen.' *ersetzt.*

6. In § 1 Abs. 5d (neu) wird folgender dritter Satz eingefügt:

‚Bei Vorliegen einer ärztlichen Bestätigung über eine überstandene Infektion mit SARS-CoV-2, eines Absonderungsbescheides, der wegen einer Infektion des Bescheidadressaten mit SARS-CoV-2 erlassen wurde oder eines durchgeführten Tests, der das Vorhandensein von Antikörpern gegen eine Infektion mit SARS-CoV-2 bestätigt, ist von einer grundsätzlichen Gleichstellung auszugehen.'

7. In § 1 Abs. 5d (neu) wird die Wort- und Zeichenfolge ‚Abs. 5c' *durch die Wort- und Zeichenfolge* ‚Abs. 5b' *ersetzt.*

8. In § 1 Abs. 5e (neu) wird die Wort- und Zeichenfolge ‚Abs. 5d' *durch die Wort- und Zeichenfolge* ‚Abs. 5c' *und die Wort- und Zeichenfolge* ‚Abs. 5e' *durch die Wort- und Zeichenfolge* ‚Abs. 5d' *ersetzt.*

9. In § 1 werden nach Abs. 5e (neu) folgende Abs. 5f (neu) und 5g angefügt:

‚(5f) Die in § 4b Abs. 1 Z 1 bis 3 des Epidemiegesetzes 1950 genannten Zertifikate können als Nachweis eines negativen Tests auf SARS-CoV-2, einer Schutzimpfung gegen COVID-19 oder einer überstandenen Infektion mit SARS-CoV-2 herangezogen werden.

(5g) Der für das Gesundheitswesen zuständige Bundesminister kann durch Verordnung nähere Vorschriften über die Form des Nachweises eines negativen Tests auf SARS-CoV-2, einer Schutzimpfung gegen COVID-19 oder einer überstandenen Infektion mit SARS-CoV-2 erlassen. Der Nachweis darf die in § 4c Abs. 1, § 4d Abs. 1 und § 4e Abs. 1 des Epidemiegesetzes 1950 genannten Daten enthalten.'

10. Dem § 9 wird folgender Abs. 3 angefügt:

‚(3) Aufsichtsorgane gemäß §§ 24ff des Lebensmittelsicherheits- und Verbraucherschutzgesetzes – LMSVG, BGBl. I Nr. 151/2005, Organe der zur Vollziehung der gewerberechtlichen Vorschiften zuständigen Behörden und Organe der Arbeitsinspektion sind im Rahmen ihrer dienstlichen Aufgaben zur Überprüfung von in einer Verordnung nach diesem Bundesgesetz als Auflage oder Voraussetzung vorgesehenen Präventionskonzepten, vor Ort, berechtigt.'"

c) In Artikel 2 wird folgende Z 12 angefügt:

12. Dem § 13 wird folgender Abs. 12 angefügt:

‚(12) § 1 Abs. 5a bis 5g, § 9 sowie § 11 Abs. 3 in der Fassung des Bundesgesetzes BGBl. I Nr. xxx/2021 treten mit dem der Kundmachung folgenden Tag in Kraft.'"

Begründung

I. Allgemeiner Teil

Der vorliegende Abänderungsantrag geht von jener Rechtslage aus, wie sie sich nach Inkrafttreten des Gesetzesbeschlusses des Nationalrats vom 25. März (757 der Beilagen XXVII. GP) darstellen wird. Die darin enthaltenen Regelungen sehen zwar Testnachweise, nicht jedoch Genesungs- oder Impfnachweise vor. Der nun vorliegende Text berücksichtigt aus Gründen der Gleichwertigkeit auch diese beiden Nachweise.

Auf europäischer Ebene ist ein Legislativpaket der Europäischen Kommission betreffend den sogenannten „digitalen grünen Pass" in Erarbeitung, das laut Zeitplan der Europäischen Kommission etwa Ende Juni 2021 in Kraft treten soll.

Der Entwurf der Europäischen Kommission für einen digitalen grünen Pass enthält zwei Verordnungen, wobei im Folgenden auf den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von Impfungen, Tests und der Genesung mit der Zielsetzung der Erleichterung der Freizügigkeit während der COVID-19-Pandemie (digitaler grüner Pass), COM(2021) 130 final vom 17. März 2021, näher einzugehen ist. Sofern nicht anders angegeben, wird auf die Fassung des Ausschusses der Ständigen Vertreter verwiesen.

Mit dem Vorschlag der Europäischen Kommission wird ausschließlich die Rechtsgrundlage für die Verwendung des grünen Passes zur Erleichterung der Freizügigkeit (free movement) geschaffen. Von vielen Mitgliedstaaten wurden zur Bekämpfung der Pandemie Restriktionen für die Einreise oder sonstige Beschränkungen für grenzüberschreitend Reisende (Quarantäne) geschaffen, die mit zunehmender Entspannung der Situation – auch auf Grund der Fortschritte bei den Schutzimpfungen – wieder zurückgenommen werden können. Um eine einheitliche Vorgangsweise der Mitgliedstaaten und eine wechselseitige Anerkennung der dafür vorgesehenen Bescheinigungen sicherzustellen, aber auch um mögliche Fälschungen der in Verwendung befindlichen Bescheinigungen hintanzuhalten, wurden im Rahmen des eHealth Netzwerks, in dem Österreich vertreten ist, Arbeiten zur Konzeption interoperabler Bescheinigungen durchgeführt und in Form von Leitlinien veröffentlicht. Diese Leitlinien sehen einen normierten Mindestdatensatz für die Bescheinigungen sowie einen eindeutigen Identifikator vor. Sie sollen digital von der ausstellenden Behörde signiert werden, der dafür notwendige gemeinsame Vertrauensrahmen ist ebenfalls Bestandteil der vom eHeath Netzwerk geleisteten Vorarbeiten.

Der Vorschlag der Kommission baut auf diesen Vorarbeiten auf und umfasst im Wesentlichen die folgenden Regelungen:

- grundsätzliche bzw. gemeinsame Bestimmungen über die drei Zertifikatsarten, die im Rahmen des grünen Passes ausgestellt werden bzw. Verwendung finden (Art. 3): Test-, Genesungs- und Impfzertifikat,
- interoperabler Vertrauensrahmen (Art. 4),
- die Art. 5 bis 7 gehen auf die einzelnen Zertifikatsarten näher ein,
- mit Art. 8 wird die Europäische Kommission ermächtigt, die erforderlichen technischen Spezifikationen für den Vertrauensrahmen zu erlassen und
- Art. 9 enthält die Vorschriften zum Datenschutz.

Über den Vorschlag wurde im Trilog Einigung erzielt, weitere Änderungen sind daher nicht mehr zu erwarten.

Wie bereits ausgeführt und von der Europäischen Kommission auch ausdrücklich festgehalten, wird die Verordnung lediglich die (auch datenschutzrechtliche) Rechtsgrundlage für grenzüberschreitende Reisebewegungen, insbesondere von und zu Arbeitsstätten, aber auch für touristische Zwecke, bieten. Die Europäische Kommission führt daher auch aus, dass Mitgliedstaaten, wenn sie innerstaatlich die von ihnen auszustellenden Zertifikate für andere Zwecke verwenden wollen, die notwendigen Rechtsgrundlagen dafür selbst schaffen müssen. In Österreich werden bereits derzeit ähnliche Nachweise – auch in elektronischer Form – beispielweise für Eintrittstests und Ausreisetests aus Hochrisikoregionen verwendet. Aus praktischen und ökonomischen Gründen erscheint es daher zweckmäßig, diese Nachweise durch die auf Grundlage des Vorschlags der Kommission auszustellenden Zertifikate zu ersetzen, weil ansonsten administrativ aufwändige und kostenmäßig belastende Doppelgleisigkeiten entstünden. Obwohl die endgültige Fassung der Verordnung noch nicht vorliegt und auch die endgültigen technischen Spezifikationen noch nicht abschließend verfügbar sind, orientiert sich das vorliegende Gesetzesvorhaben sehr eng an den Inhalten des Kommissionsvorschlags bzw. an den Vorarbeiten des eHealth Netzwerks. Ziel dabei ist, ein Set von Zertifikaten sowie Vorgaben für Anwendungen für ihre Überprüfung (Verifizierung)

bereitzustellen, die sowohl konform zu den EU-Vorgaben sind, als auch den innerstaatlichen Bedarf abdecken.

Ein wesentliches Ziel für die Ausstellung und Verifizierung der Zertifikate ist, sie soweit wie möglich interoperabel zu gestalten, das minimum data set wurde daher unverändert aus dem Entwurf übernommen. Damit wird sichergestellt, dass „österreichische" Zertifikate in anderen Mitgliedstaaten gelesen werden können. Sofern andere Mitgliedstaaten ihre Zertifikate ebenso EU-konform ausstellen, ist auch sichergestellt, dass diese Zertifikate, etwa bei der Verifizierung durch die heimische Gastronomie Veranstalter oder durch touristische Einrichtungen aufgelöst („gelesen") werden können.

Der einleitend zitierte Gesetzesbeschluss enthielt auf Grund eines vordringlichen Bedarfs lediglich erste Regelungen für die Testnachweise und ein elektronisches Werkzeug für ihre Überprüfung. Für Genesungs- und Impfzertifikate wurden lediglich rudimentäre Vorgaben in verschiedenen Stellen des Epidemiegesetzes aufgenommen. Diese zum Teil verstreuten Bestimmungen werden durch das gegenständliche Gesetzesvorhaben aufgehoben und durch eine zusammenhängende und möglichst kompakte Regelung ersetzt. Verordnungsermächtigungen sind nur dann vorgesehen, um verbliebene Unwägbarkeiten des Gesetzgebungsprozesses auf europäischer Ebene abzufangen oder – und dies kommt auch im Vorschlag der Europäischen Kommission deutlich zum Ausdruck – um aktuell noch nicht vorliegende wissenschaftliche Erkenntnisse möglichst rasch ab ihrer Verfügbarkeit in die Rechtsgrundlagen integrieren zu können. Letztere betreffen unter anderem bestimmte Testmethoden (z. B. Antikörpertests) oder neue Erkenntnisse über die Dauer der Immunisierung durch Schutzimpfungen.

II. Besonderer Teil

Zu Artikel 1 (Epidemiegesetz 1950)

Zu Z 2 (§ 4 Abs. 1) und Z 7 (§ 4 Abs. 18 bis 24):

Infolge der Neuregelung der Nachweise (Zertifikate) über eine epidemiologisch geringe Gefahr in Form des „digitalen grünen Passes" werden entgegenstehende bzw. unsystematische Bestimmungen oder Teile davon aufgehoben.

Zu Z 3 (§ 4 Abs. 3a):

Das Gesundheitswesen verfügt zunehmend über Hinweise auf sogenannte „Impfdurchbrüche", das sind neuerliche Infektionen bereits genesener oder geimpfter Personen überwiegend mit Varianten (Mutationen) des COVID-19-Erregers oder über „Ausbruchscluster", die mit den verfügbaren Daten nicht nachvollzogen bzw. aufgeklärt werden können. Um valide Anhaltspunkte über die tatsächliche Anzahl von Reinfektionen, die gesundheitsbezogenen Determinanten (z. B. Vorerkrankungen) der neuerlich infizierten Personen und der diesbezüglich im Rahmen des Ausbruchs- und Krisenmanagements zu setzenden Maßnahmen zu gewinnen (etwa die Bestellung zusätzlicher Impfstoffe für den betroffenen Personenkreis), ist eine Übermittlung von Daten aus dem zentralen Impfregister und deren Verschneidung mit den Daten des Registers gemäß § 4 (EMS) unumgänglich. Es ist darauf hinzuweisen, dass der Umfang dieser Datenübermittlung jenen der Übermittlung an das EPI-Service gemäß § 4e Abs. 2 für die Ausstellung von Impfzertifikaten übersteigt. Die Übermittlung der Daten erfolgt auf Anforderung, die entsprechend den angeführten Kriterien zu konkretisieren ist.

Das im Bereich der Epidemiologie führende IT-System ist das Epidemiologische Meldesystem (EMS), das für die Gesundheitsbehörden entwickelt wurde und Standardworkflows in Bezug auf die verschiedenen Erreger abbildet. Es ist jedoch nicht auf die Pandemiebekämpfung ausgerichtet, weshalb diesbezügliche Anpassungen bereits vorbereitet werden. Ausbruchscluster oder auch Impfdurchbrüche stellen somit eine neue Anforderung dar, denen mit dem im EMS (Register gemäß § 4) verfügbaren Daten alleine nicht entsprochen werden kann. Solche Konstellationen sind aber auch weder zeitlich noch regional vorhersehbar, weshalb es nicht möglich ist, Art und Umfang jener Daten, die zusätzlich benötigt werden, vorab zu definieren. Daten aus dem zentralen Impfregister, für das im Vollbetrieb der für das Gesundheitswesen zuständige Bundesminister und im Pilotbetrieb die ELGA GmbH der datenschutzrechtlich Verantwortliche (Art. 4 Z 7 DSGVO) ist, bilden eine wesentliche Grundlage für gesundheitsbehördliche Analysen und die daraus abzuleitenden Maßnahmen, sie müssen aber im Hinblick auf die genannten Unwägbarkeiten für den konkreten Bedarf (fallbezogen) festgelegt bzw. angefordert werden, um dem datenschutzrechtlich gebotenen Grundsatz der Datenminimierung Rechnung tragen zu können. Eine Anforderung ist deshalb nötig, weil sich die eHealth-Anwendung „Elektronischer Impfpass" noch im Pilotbetrieb befindet und die ELGA GmbH die datenschutzrechtliche Verantwortliche ist (vgl. auch § 4b Abs. 1 der eHealth-Verordnung, BGBl. II Nr. 449/2020). Die Berechtigung der ELGA GmbH zur Übermittelung von Daten wird durch die Anforderung konkretisiert. Klarerweise werden bei

Mehrfachübermittlungen zu derselben Anforderung die Folgeübermittlungen auf die bis zum Zeitpunkt der Folgeübermittlung eingetretenen Änderungen (Delta) eingeschränkt.

Gesundheitsbehördliche Maßnahmen im Kontext der Kontaktnachverfolgung sind ganz wesentlich dadurch bestimmt, dass sie – um Wirksamkeit zu entfalten – in einem engen Zeitfenster (maximal 72 Stunden) gesetzt werden müssen. Weder das Umfeld (regional, zielgruppenspezifisch) noch der Personenkreis, der in die Kontaktpersonennachverfolgung einzubeziehen ist, sind vorab bekannt, sondern ergeben sich erst durch die diesbezüglichen behördlichen Tätigkeiten. Zu bedenken ist auch, dass sich die Kontaktpersonennachverfolgung gerade nicht auf bereits erkrankte Personen beschränken darf, sondern die Personen im Umfeld einer erkrankten Person im Fokus hat. Festzustellen, welcher konkrete Personenkreis betroffen ist, ist somit eine der Kernaufgaben in diesem Zusammenhang, Informationen über bereits erfolgte Impfungen tragen dazu bei, die zu setzenden Maßnahmen, die meist mit Eingriffen in Persönlichkeitsrechte verbunden sind, aber auch den Aufwand dafür, auf das notwendige Ausmaß einzuschränken. Bewusst ist, dass die Kontaktpersonennachverfolgung mittels Einzelabfragen des zentralen Impfregisters durch Gesundheitsbehörden erfolgen können. Dafür wäre aber in der Regel ein permanenter Applikationswechsel vom EMS als führendem System zum zentralen Impfregister erforderlich, Einzelabfragen können zu Fehlern führen. Angesichts des gegebenen Zeitdrucks und des damit verbundenen Aufwands wären Einzelabfragen des zentralen Impfregisters für die Gesundheitsbehörden somit eine zusätzliche, jedoch vermeidbare Belastung.

Die Daten, die gemäß dieser Bestimmung in Register gemäß § 4 übernommen werden, stehen den auf das Register Zugriffsberechtigten und somit auch den Gesundheitsbehörden in den Ländern zur Verfügung bzw. dürfen die Daten von den Gesundheitsbehörden entsprechend den Vorgaben verarbeiten.

Die in § 4 normierten angemessenen und spezifischen Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, wie das Weiterverarbeitungsverbot zu anderen Zwecken (siehe den vorgeschlagenen Abs. 6) und die Pflicht zur Protokollierung eines jeden Verarbeitungsvorgangs (siehe den geltenden Abs. 9) finden auch auf den vorgeschlagenen Abs. 3a Anwendung. Gemäß ErwG 63 der DSGVO sollte der Verantwortliche nach Möglichkeit einen Fernzugang zu einem sicheren System bereitstellen, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglicht. Den betroffenen Personen soll ein solcher Fernzugang über das Zugangsportal (§ 23 GTelG 2012) bereitgestellt werden, damit sie unkompliziert und zu jeder Zeit Auskunft über die sie betreffenden Protokolldaten erhalten Bei Inkrafttreten der Bestimmung ist die technische Umsetzung noch nicht abgeschlossen, jedoch wird eine zeitnahe Umsetzung angestrebt. Da für den Zugriff über das Zugangsportal eine Handysignatur notwendig ist, soll durch die vorgeschlagene Bestimmung auch die Klarstellung erfolgen, dass das Auskunftsrecht weiterhin gegenüber dem für das Gesundheitswesen zuständigen Bundesminister ausgeübt werden kann. Da sich gemäß Art. 12 Abs. 5 DSGVO der Verantwortliche weigern kann, bei häufigen Wiederholungen tätig zu werden, erfolgt durch die vorgeschlagene Bestimmung auch die Klarstellung, dass eine Geltendmachung des Auskunftsrechts hinsichtlich der Protokolldaten mindestens monatlich keine „häufige Wiederholung“ ist. Durch die Verwendung des Begriffs „monatlich“ statt „einmal im Monat“ wird klargestellt, dass auf eine Zeitspanne und nicht auf einen Kalendermonat abgestellt wird..

Die Daten sind gemäß dem geltenden Abs. 11 zu löschen sobald sie zur Erfüllung der Aufgaben der Bezirksverwaltungsbehörden im Zusammenhang mit der Erhebung über das Auftreten und im Zusammenhang mit der Verhütung und Bekämpfung einer anzeigepflichtigen Krankheit nicht mehr erforderlich sind. Klargestellt wird, dass das Ausbruchs- und Krisenmanagement von „Verhütung und Bekämpfung einer anzeigepflichtigen Krankheit“ umfasst ist, sodass die Normierung einer darüber hinaus gehenden Löschverpflichtung unterbleiben kann.

Zu Z 4 (§ 4 Abs. 4 Z 3):

Es erfolgt die Behebung eines redaktionellen Versehens.

Zu Z 5 (§ 4 Abs. 6) und Z 6 (§ 4 Abs. 7):

Das bisher in Abs. 7 normierte Übermittlungs- und Weiterverarbeitungsverbot stellt eine angemessene und spezifische Maßnahme zur Wahrung der Rechte und Freiheiten der betroffenen Person im Sinne des Art. 9 Abs. 2 lit. i DSGVO dar (vgl. dazu auch die Rundschreiben des Bundeskanzleramts zur legistischen Gestaltung von Eingriffen in das Grundrecht auf Datenschutz vom 14. Mai 2008, GZ BKA-810.016/0001-V/3/2007 bzw. vom 2. August 2017, GZ BKA-810.026/0035-V/3/2017). Da dieses Übermittlungs- und Weiterverarbeitungsverbot in Abs. 7 jedoch zum einen unsystematisch und zum anderen aufgrund der durch die letzten Novellen neu hinzugekommenen Verarbeitungszwecke zu weit gefasst ist, soll es durch die gegenständliche Novelle von Abs. 7 in Abs. 6 verschoben werden.

Mit der Neuformulierung des Verarbeitungsverbots wird redundant, dass die Verarbeitung der im Register gespeicherten Daten zur Ausstellung eines Impfnachweises über eine Impfung gegen COVID-19 sowie zur

Ausstellung einer Bestätigung über eine erfolgte und aktuell abgelaufene Infektion an SARS-CoV-2 erfolgen darf, da beides gemäß den vorgeschlagenen §§ 4b ff ausdrücklich zulässige bestimmte Zwecke sind. Da die Ausstellung von Impfnachweisen nicht über das Register erfolgen soll, handelt es sich beim Entfall dieses Zwecks in Abs. 6 zudem um eine bereits zuvor beschriebene Anpassung.

Zu Z 9 (§ 4a Abs. 6):

Nach Inkrafttreten des Gesetzesbeschlusses des Nationalrats vom 25. März enthält § 4a einen neuen Abs. 6, wonach der Bundesanstalt „Statistik Österreich" (Bundesanstalt) auf deren Anfrage binnen vier Wochen zum Zweck der statistischen Aufbereitung und wissenschaftliche Erforschung der COVID-19-Krisensituation die mit dem verschlüsselten bereichsspezifischen Personenkennzeichen Amtliche Statistik (vbPK-AS) versehenen COVID-19-bezogenen Daten des Statistik-Registers zu übermitteln sind. Durch die vorgeschlagene Ergänzung des Abs. 6 soll die Bundesanstalt darüber hinaus konkrete statistische Auswertungen im Zusammenhang mit der epidemiologischen Überwachung sowie dem Monitoring der Wirksamkeit der Maßnahmen in Bezug auf die Bekämpfung von COVID-19 für den für das Gesundheitswesen zuständigen Bundesminister vornehmen. Dieses Vorgehen ist auch in anderen Bereichen der Statistik üblichen (siehe diesbezüglich den weiten Anwendungsbereich des Bundesstatistikgesetzes 2000, BGBl. I Nr. 163/1999).

Durch die Einschränkung auf COVID-19-bezogene Daten wird eine starke Begrenzung der vorzunehmenden statistischen Auswertungen vorgenommen. Welche konkreten statistischen Auswertungen die Bundesanstalt jedoch vorzunehmen hat, kann im Gesetz nicht näher beschrieben werden, weil das von den zu klärenden Fragen abhängt. Welche Fragen zu klären sind, ist einem dynamischen Prozess unterworfen. Gemäß § 4 Abs. 2 des Bundesstatistikgesetzes 2000 liegt eine bundesgesetzlich angeordnete statistische Erhebung und Erstellung einer Statistik vor, wenn im Bundesgesetz – also wie hier im vorgeschlagenen Abs. 6 - zumindest der Gegenstand der Erhebung oder Statistik festgelegt ist; dies ist durch die Einschränkung auf die Zwecke der epidemiologischen Überwachung sowie dem Monitoring der Wirksamkeit der Maßnahmen in Bezug auf die Bekämpfung von COVID-19 erfolgt.

Zu Z 10 (§ 4b):

Wie im Allgemeinen Teil festgehalten, waren die mit Z 10 und 11 zu ändernden Vorschriften im Lichte des noch unzureichenden Informationsstandes über die Ausgestaltung des Legislativvorschlags der Europäischen Kommission als innerstaatliche Übergangslösung konzipiert, um das vordringliche Problem im Zusammenhang mit der Ausstellung von Testnachweisen zu entschärfen. Mit der Neuregelung des § 4b werden gemeinsame Bestimmungen für alle Zertifikatsarten gemäß Legislativvorschlag der Europäischen Kommission (vgl. Art. 8b, der mit den Änderungen durch das Europäische Parlament vom 29. April 2021 dem Vorschlag der Kommission bzw. des Rates hinzugefügt werden soll) geschaffen, die Detailregelungen zu den Testzertifikaten finden sich neu gefasst im geänderten § 4c.

Die Einrichtung und der Betrieb des EPI-Service sowie die damit einhergehende Ausstellung und Bereitstellung der Zertifikate erfüllt ein erhebliches öffentliches Interesse gemäß Art. 9 Abs. 2 lit. g DSGVO sowie insbesondere auch ein öffentliches Interesse im Bereich der öffentlichen Gesundheit gemäß Art. 9 Abs. 2 lit. i DSGVO, jeweils in Verbindung mit Art. 6 Abs. 1 lit. e DSGVO: Durch die mit dem EPI-Service einhergehenden Datenverarbeitungen soll zum einen nämlich die COVID-19-Pandemie weiter bekämpft werden, wozu ein allfälliger Nachweis einer geringen epidemiologischen Gefahr einen erheblichen Beitrag leistet (Art. 9 Abs. 2 lit. i DSGVO). Gleichzeitig soll durch die damit einhergehenden Datenverarbeitungen ein Weg aus dem Stillstand des gesellschaftlichen und wirtschaftlichen Lebens – und zwar ohne Erhöhung des Infektionsgeschehens – gegangen werden (Art. 9 Abs. 2 lit. i DSGVO). Eine Einschränkung des öffentlichen Lebens ist nur für jene Personen gerechtfertigt, von denen eine (nicht geringe) epidemiologische Gefahr ausgeht.

Die Übermittlung der Daten durch die Einrichtungen, die SARS-CoV-2-Tests im Sinne des § 4b Abs. 2 auswerten (§ 4c Abs. 2), und der ELGA GmbH (§ 4e Abs. 2) erfolgt aufgrund einer rechtlichen Verpflichtung gemäß Art. 6 Abs. 1 lit. c in Verbindung mit Art. 9 Abs. 2 lit. g und i DSGVO. § 4b Abs. 1 konkretisiert die Nachweise dahingehend, dass sie auch, aber nicht ausschließlich, durch Vorlage von EU-konformen (dem Legislativvorschlag der Europäischen Kommission entsprechenden) Zertifikaten erbracht werden können. Weitere innerstaatlich anerkannte Nachweise können etwa der Papierimpfpass (gelbes WHO-Formular) oder ärztliche Impfbestätigungen sein. Die Zertifikatsarten sowie die Primäranforderungen ihrer Ausstellung werden in Abs. 1 abschließend genannt. Klargestellt wird auch der Zusammenhang mit COVID-19. Im Hinblick auf die im Verordnungsvorschlag der Europäischen Kommission genannten Voraussetzungen für die Ausstellung von Testzertifikaten werden diese in Abs. 2 konkretisiert. Die auf europäischer Ebene zwecks wechselseitiger Anerkennung akkordierte gemeinsame Liste betreffend COVID-19-Antigen-Schnelltests wird bei Bedarf aktualisiert und stellt somit auch eine der

Grundlagen für Testzertifikate dar, die auf Basis von Antigen-Schnelltests ausgestellt werden. Diese Liste soll zur leichteren Zugänglichkeit bzw. zur Vermeidung der Verwendung nicht enthaltener Produkte vom Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz auf geeignete Weise veröffentlicht werden. Antikörpertests werden ausschließlich zur Ausstellung von Genesungszertifikaten verwendet. Die wissenschaftliche Evidenz solcher Tests ist in Diskussion, weshalb Konkretisierungen einer Verordnung vorbehalten werden müssen – auch um Abweichungen oder Widersprüche zu künftigen europäischen Regelungen zu vermeiden.

In Abs. 3 wird festgelegt, dass der für das Gesundheitswesen zuständige Bundesminister als datenschutzrechtlich Verantwortlicher zur Ausstellung und Bereitstellung digitaler grüner Zertifikate eine elektronische Anwendung („EPI-Service") zu betreiben hat – er ist damit ausstellende Behörde im Sinne des Verordnungsvorschlags der Europäischen Kommission. Darin wird nicht zwingend eine einzige Behörde zur Ausstellung der Zertifikate vorgegeben, womit auf die unterschiedliche Organisation der Mitgliedstaaten Bedacht genommen wurde. Allerdings wird aus Gründen der leichteren technischen Umsetzbarkeit und Administrierbarkeit – auch in Bezug auf den gemeinsamen Vertrauensrahmen – für Österreich davon ausgegangen, dass eine zentrale Ausstellung operativ wesentlich einfacher, ökonomisch zweckmäßiger und im Hinblick auf die damit verbundenen bzw. einzuhaltenden Sicherheitsvorkehrungen besser umsetzbar ist.

EU-konforme Zertifikate sind grundsätzlich in Form eines QR-Codes (2D-Barcode) auszustellen und müssen jeweils alle Daten, die im Anhang zum Verordnungsvorschlag ausgewiesen sind, enthalten („minimum data set"). Damit wird eine offline-Überprüfung bzw. Verifizierung ermöglicht. Abs. 4 referenziert für die Ausstellung und innerstaatliche Verwendung solcher Zertifikate die Vorgaben des Verordnungsvorschlags der EK, wobei neben Inhalten für die unterschiedlichen Zertifikate auch die im Vertrauensrahmen festzulegenden Interoperabilitätsanforderungen zu beachten sind. Es wird erwartet, dass die bereits vorliegenden Spezifikationen des eHealth Netzwerks von der Europäischen Kommission mittels delegiertem Rechtsakt für verbindlich erklärt werden. Änderungen der in die Zertifikate aufzunehmenden Daten durch Änderungen der minimum data sets müssen in den betreffenden Bestimmungen (§ 4c Abs. 1, § 4d Abs. 1, § 4e Abs. 1) nachvollzogen werden.

Die Zertifikate müssen gemäß den EU-Vorgaben in digital verarbeitbarem Format (QR-Code) sowie in menschenlesbarem Format ausgestellt bzw. bereitgestellt werden (Abs. 5), um dem Anspruch der Niederschwelligkeit des Zugangs für die Betroffenen gerecht zu werden. Für die Ausprägung in menschenlesbarer Form wurde das pdf-Format gewählt, das alle Angaben des QR-Codes in Textform und den aufgedruckten QR-Code enthalten muss. Damit wird sichergestellt, dass die Zertifikate auch in gedruckter Form prüf- bzw. verifizierbar sind und die Inhaber bzw. Inhaberinnen nicht auf die Verwendung elektronischer Geräte (z. B. Smartphones) angewiesen sind. Die Feldbezeichnungen sind in der elektronischen Auflösung des QR-Codes bzw. in der textlichen Auflösung bei gedruckten Zertifikaten zumindest zweisprachig anzugeben, wovon die englische Sprachfassung zwingend ist. Durch die angestrebte gleichzeitige Verwendung der EU-seitig vorgesehenen Zertifikate auch für innerstaatliche Zwecke ist auch diesbezüglich EU-Konformität herzustellen.

Die Aus- und Bereitstellung EU-konformer Zertifikate muss gemäß Abs. 6 für die Betroffenen kostenlos erfolgen. Bei Vorliegen der sonst festgelegten Voraussetzungen werden die Zertifikate gleichsam en bloc generiert werden können. Dies ist deshalb notwendig, weil insbesondere die nur kurze Zeit validen Testergebnisse aktuell in hoher Anzahl (rd. zwei Millionen pro Woche) ermittelt und sehr rasch in Zertifikatsform bereitgestellt werden müssen. Eine Generierung von Testzertifikaten auf Anforderung der Betroffenen wäre unter den gegebenen Rahmenbedingungen operativ bzw. administrativ nicht machbar.

Zum Zeitpunkt des Inkrafttretens wird es bereits eine hohe Anzahl genesener Personen (Schätzungen bewegen sich um 500.000) geben, die ab Verfügbarkeit der Genesungszertifikate solche vermutlich in hoher Anzahl beantragen werden. Auch diesbezüglich wäre die Generierung der Zertifikate auf Anforderung nur mit hohem Aufwand machbar.

Erwartet wird, dass bis ca. Ende Juni 2021 rd. 4,5 Millionen Personen geimpft sind bzw. die Voraussetzungen für die Ausstellung eines Impfzertifikats erfüllen. Schon im Hinblick auf die längere Gültigkeitsdauer der Impfzertifikate (auch der Genesungszertifikate) und die beabsichtigte Rücknahme von Reiserestriktionen dürfte eine beträchtliche Anzahl dieser Personen die Ausstellung eines Impfzertifikats beantragen, wodurch die Generierung der Zertifikate in der Kürze der zur Verfügung stehenden Zeit (Beginn der Reisesaison) nicht machbar erscheint.

Zu diesen zu erwartenden Anforderungsspitzen kommt gleichsam der „Normalbetrieb" hinzu, zumal Testungen nach wie vor erforderlich sein werden und weitere Impfungen durchgeführt werden. Aus diesen Gründen sollen Genesungs- und Impfzertifikate – unabhängig von einer Anforderung durch die betroffene Person – gleichsam vorbereitend für jene Personen bereitgestellt werden dürfen, die die Anforderungen

bereits erfüllen. Freilich werden davon jene Genesungszertifikate auszunehmen sein, bei denen die Gültigkeitsdauer aufgrund des vermuteten Genesungszeitpunkts bereits abgelaufen ist.

Um die geforderte Niederschwelligkeit des Zugangs zu Zertifikaten sicherzustellen, sind gemäß Abs. 7 mehrere Maßnahmen vorgesehen, die um zertifikatsabhängige Maßnahmen (z. B. §§ 4c Abs. 2, 4e Abs. 4) ergänzt werden. Von mehreren Bundesländern wurden bislang zur Unterstützung des Testmanagements elektronische Systeme eingerichtet, die im Wesentlichen Funktionalitäten für die Terminverwaltung (Registrierung, Terminbuchung), administrative Unterstützung der Testabwicklung und Kommunikation der Testergebnisse an die getesteten Personen umfassen. Es besteht damit auf regionaler Ebene ein gesichertes behördliches Umfeld für die Verarbeitung personenbezogener Gesundheitsdaten, das zweckmäßigerweise auch für die Bereitstellung von Test- und Impfzertifikaten genutzt werden soll. Abs. 7 Z 1 ermöglicht den Ländern, die genannten Zertifikate oder Verweise (Links) darauf aus dem EPI-Service mit denselben bereits bewährten Methoden zu verarbeiten, wie dies schon bisher bezüglich der Testnachweise der Fall war. Die Zertifikate werden gleichsam aus dem EPI-Service abgeholt und den Betroffenen auf elektronischem Weg zur Verfügung gestellt, eine über die damit verbundenen technischen Notwendigkeiten hinausgehende Speicherung oder sonstige Weiterverarbeitung der Daten ist weder vorgesehen noch zulässig. Zur datenschutzrechtlichen Rollenverteilung siehe (sinngemäß) sogleich unten.

Als weitere Maßnahme zur Gewährleistung der Niederschwelligkeit des Zugangs zu Zertifikaten ist eine Portalverbundanwendung einzurichten, die es den in Abs. 7 Z 2 genannten Institutionen ermöglicht, Menschen, die ein Zertifikat in elektronischer Form nicht erhalten oder verwenden können oder wollen, wohnortnah in gedruckter Form bereitzustellen. Die genannten Einrichtungen werden als eigenständige datenschutzrechtlich Verantwortliche (Art. 4 Z 7 DSGVO) tätig: Der für das Gesundheitswesen zuständige Bundesminister hat nämlich zwar eine Portalverbundanwendung bereitzustellen, die es den genannten Stellen ermöglicht, die Zertifikate in gedruckter Form den betroffenen Personen zur Verfügung zu stellen, allerdings sind die genannten Stellen nicht verpflichtet, diese auch zu nutzen. Ob sie die Möglichkeit nutzen, obliegt der Entscheidung der genannten Stellen; sie entscheiden sohin eigenverantwortlich über den Zweck der Datenverarbeitung. Dieser Umstand bewirkt, dass sie im Zweifel als datenschutzrechtlich Verantwortliche zu qualifizieren sind (vgl. dazu *Art.-29-Datenschutzgruppe,* Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP 169, 00264/10/DE, 17).

Zertifikate in gedruckter Form sollen auch an gesetzliche Vertreterinnen bzw. Vertreter für nicht oder eingeschränkt geschäftsfähige Personen sowie an gewillkürte Vertreterinnen bzw. Vertreter ausgehändigt werden dürfen. Betroffene erhalten darüber hinaus auch die Möglichkeit (Abs. 7 Z 3) zur Einsichtnahme, zum Druck oder Download ihrer Zertifikate über das Zugangsportal. Voraussetzung dafür ist lediglich eine eGovernment-konforme Authentifizierung (Handysignatur, künftig ID Austria).

Zertifikate können fehlerhaft ausgestellt oder – durch welche Umstände auch immer – während ihrer Gültigkeitsdauer fehlerhaft werden. Darüber hinaus entstehen laufend neue wissenschaftliche Erkenntnisse, die sich auf die Gültigkeitsdauer oder etwa auf die dem Zertifikat zugrundeliegende Testmethode (z. B. in Bezug auf sogenannten Antikörpertests) auswirken können. In diesem Fall müssen die betroffenen Zertifikate (im Wesentlichen sind davon Genesungs- und Impfzertifikate betroffen) rasch und transparent widerrufen werden. Technisch umgesetzt wird dies nach derzeitigem Stand der Dinge durch die Einmeldung solcher Zertifikate in eine im gemeinsamen Vertrauensrahmen geführte Widerrufsliste. Eine Berichtigung von fehlerhaften Zertifikaten (QR-Codes) ist ausgeschlossen (Signaturbruch), sie können nur widerrufen und gegebenenfalls neu ausgestellt werden. Nachdem insbesondere aus Gründen der Datenaufbringung für die Ausstellung der Zertifikate nicht gewährleistet ist, dass der Verantwortliche für das EPI-Service die Ausstellung fehlerhafter Zertifikate verhindern kann, ist der Widerruf eines Zertifikats nur auf Grund einer diesbezüglichen Information der betroffenen Person möglich. Dafür ist eine Anlauf- oder Clearingstelle (benannte Stelle) vorgesehen. Es ist jedoch darauf hinzuweisen, dass nicht jeder Fehler einer Berichtigung zugänglich sein muss und auch nicht jede Berichtigung zwangsläufig zu einer Neuausstellung des Zertifikats führen muss. Diese Stelle hat daher, um eine mögliche Behebung des Fehlers durch die verursachende Stelle bzw. die Neuausstellung des Zertifikats veranlassen zu können, zunächst die Art des Fehlers zu erheben und im Falle der Neuausstellung das Zertifikat der betroffenen Person zur Verfügung zu stellen.

Davon unberührt bleibt die Pflicht des Verantwortlichen, den Grundsatz der Richtigkeit der Daten (Art. 5 Abs. 1 lit. d DSGVO) einzuhalten und dafür Sorge zu tragen, dass die personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; er hat alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Die betroffene Person ist über eine solche (amtswegige) Berichtigung durch den Verantwortlichen, der die Berichtung vorgenommen hat, zu informieren.

Testzertifikate haben im Vergleich zu den anderen Zertifikaten eine kurze Gültigkeitsdauer. Es ist davon auszugehen, dass diese bis zur Aufnahme in die Widerrufsliste in der überwiegenden Anzahl der Fälle bereits abgelaufen wäre, sodass ein diesbezüglicher Widerruf mit einem unnötigen bzw. vermeidbaren Aufwand verbunden wäre und das angestrebte Ziel nicht (mehr) erreicht würde. Deshalb wurde vom Widerruf von Testzertifikaten Abstand genommen. Im EPI-Service sind die widerrufenen Zertifikate unverzüglich zu löschen (Abs. 8).

Gemäß Art. 35 Abs. 1 DSGVO haben Verantwortliche eine Datenschutz-Folgenabschätzung durchzuführen, wenn die Datenverarbeitung neue Technologien verwendet oder Art, Umfang, Umstände und Zweck der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge haben. Eine Datenschutz-Folgenabschätzung ist aufgrund des § 2 Abs. 3 Z 1 und 5 der Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), BGBl. II Nr. 278/2018, durchzuführen.

Nach ErwG 92 und Art. 35 Abs. 10 DSGVO dürfen Datenschutz-Folgenabschätzungen auch auf abstrakter Ebene durchgeführt werden (vgl. dazu etwa auch § 111f AußerStrG, § 2k Abs. 4 FOG, § 18 Abs. 8 Z 5 lit. b EStG 1988, § 117 Z 10 BörseG 2018 sowie § 31 Abs. 5 TVG 2012); die bezugshabende Datenschutz-Folgenabschätzung findet sich als Anlage im Anschluss.

Der für das Gesundheitswesen zuständige Bundesminister wird über das Öffentliche Gesundheitsportal Österreichs (www.gesundheit.gv.at) darüber informieren, dass die Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 10 DSGVO bereits im Rahmen der Erlassung der Rechtsgrundlage vorweggenommen wurde und daher keine gesonderte Datenschutz-Folgeabschätzung durch die einzelnen Verantwortlichen erforderlich ist.

Zu Z 11 (§ 4c):

Die Pflichtfelder (sofern nicht explizit abweichend gekennzeichnet) für Testzertifikate sind im geänderten Abs. 1 ausgeführt, sie entsprechen dem minimum data set auf EU-Ebene. Der aus dem minimum data set übernommene Begriff „Nachname“ entspricht dem Begriff „Familienname“ in § 38 Personenstandsgesetz 2013, BGBl. I Nr. 16/2013.

Jene Stellen, die Tests auswerten, werden mit Abs. 2 zur Übermittlung der näher bezeichneten Testdaten verpflichtet. Die Mitübermittlung der Sozialversicherungsnummer ist erforderlich, um im Wege des Patientenindex das bereichsspezifische Personenkennzeichen (bPK-GH) ermitteln zu können, das beispielsweise für die Einsichtnahme in Zertifikate via Zugangsportal erforderlich ist. Die Testzertifikate in den festgelegten Formaten werden im EPI-Service gespeichert und dürfen den Teststellen zwecks sofortiger Bereitstellung eines gedruckten Zertifikats rückübermittelt werden. Ausschließlich zu diesem Zweck werden die Teststellen speziell berechtigt, die Testzertifikate in personenbezogener Form zu verarbeiten; eine Speicherung durch die Teststellen selbst ist unzulässig.

Im Anwendungsbereich dieser Bestimmung sind der für das Gesundheitswesen zuständige Bundesminister und die Einrichtungen, die SARS-CoV-2-Tests im Sinne des § 4b Abs. 2 auswerten, gemeinsam für die Verarbeitung Verantwortliche (Abs. 3). Gemäß § 26 Abs. 1 zweiter Satz DSGVO haben mehrere gemeinsam Verantwortliche in einer Vereinbarung festzulegen, wer von ihnen gegenüber der betroffenen Person welche Verpflichtungen nach der DSGVO – etwa Berichtigungs- und Löschungspflichten – wahrzunehmen hat, es sei denn, eine entsprechende Zuständigkeitsverteilung bzw. Pflichtenzuordnung ist bereits in einer gesetzlichen Vorschrift des Unions- oder des nationalen Rechts vorgesehen. In diesem Sinne sollen in den vorgeschlagenen Z 1 bis 3 die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber den betroffenen Personen widergespiegelt und die Aufteilung der Pflichten wie folgt vorgenommen werden:

Es erscheint zweckmäßig, dass die Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstige Pflichten nach der DSGVO von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, über die sie auch tatsächlich verfügen. Dies deshalb, weil der in diesem Sinne (ausschließlich) zuständige Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob einer betroffenen Person bezüglich der in Rede stehenden Daten tatsächlich ein Auskunfts-, Berichtigungs- oder sonstiger Anspruch nach der DSGVO zukommt. Wird ein Recht nach der DSGVO von einer betroffenen Person – unter Nachweis von deren Identität (vgl. ErwG 64 DSGVO) – bei einem nach dieser Bestimmung unzuständigen Verantwortlichen wahrgenommen, soll nach Z 3 lit. a direkt durch diesen die Weiterverweisung an den für die Bearbeitung des Gesuchs zuständigen Verantwortlichen erfolgen. Dies soll auch für Fälle gelten, in denen den in Anspruch genommenen Verantwortlichen nur einen Teil der Pflichten treffen. Sofern der unzuständige Verantwortliche den tatsächlichen Verantwortlichen aus dem Begehren der betroffenen Person eruieren kann, ist sie direkt an diesen zu verweisen; ist dies nicht möglich, sind der betroffenen Person Anhaltspunkte zu geben, an denen sie den zuständigen Verantwortlichen selbst eruieren kann (beispielsweise durch einen Hinweis auf die Teststelle, bei der der Test durchgeführt wurde).

Sofern sich aus den Informationen der betroffenen Person der zuständige Verantwortliche eruieren lässt und die betroffene Person darin ausdrücklich einwilligt, soll der unzuständige Verantwortliche das Begehren an den zuständigen Verantwortlichen direkt weiterleiten dürfen. Der unzuständige Verantwortliche hat im Sinne des Erleichterungsgrundsatzes gemäß Art. 12 Abs. 2 DSGVO die betroffene Person bei Wahrnehmung der ihm gegenüber geltend gemachten Betroffenenrechte anzuweisen (dies beinhaltet gegebenenfalls auch die Rückfrage, ob eine direkte Weiterleitung gewünscht sei). Der vorgeschlagenen Regelung steht Art. 26 Abs. 3 DSGVO nicht entgegen. Nach dieser Bestimmung kann die betroffene Person ein Recht aufgrund der DSGVO zwar gegenüber „jedem einzelnen der Verantwortlichen" geltend machen, und zwar unabhängig von einer zwischen den Verantwortlichen im Rahmen einer Vereinbarung getroffenen Zuständigkeitsverteilung; dies impliziert eine Pflicht des insoweit unzuständigen Verantwortlichen, ein Gesuch des Betroffenen nicht zurückzuweisen, sondern es jedenfalls entgegenzunehmen und an den zuständigen Verantwortlichen weiterzuleiten. Die freie Wahl des Verantwortlichen, gegenüber dem die betroffene Person ein Recht nach der DSGVO geltend macht, gilt jedoch nur dann, wenn die Zuständigkeitsverteilung auf einer Vereinbarung zwischen den Verantwortlichen, nicht aber, wenn sie auf einer gesetzlichen Regelung beruht. Verteilt daher – wie hier – eine gesetzliche Regelung die Zuständigkeiten unter den Verantwortlichen, so ist ein unzuständiger Verantwortlicher nicht gehalten, ein Gesuch der betroffenen Person entgegenzunehmen oder weiterzuleiten; vielmehr kann er die betroffene Person in einem solchen Fall an den zuständigen Verantwortlichen verweisen (siehe dazu bereits ErlRV 65 BlgNR XXIV. GP, 73). Bei der vorgeschlagenen Z 3 lit. a handelt es sich sohin lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff DSGVO bleiben davon unberührt. Macht die betroffene Person demnach beispielsweise das Recht auf Löschung geltend, ist durch den zuständigen Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt.

Testzertifikate haben, ausgehend von der Mitte Mai 2021 gegebenen Rechtslage Gültigkeitsdauern zwischen 24 und 168 Stunden (1-7 Tage). Die im Verordnungsvorschlag der Kommission ursprünglich enthaltene Gültigkeitsdauer von Testzertifikaten auf Basis von PCR-Tests findet sich im akkordierten Entwurf nicht mehr. Um eine – auch technisch – praktikable Löschung der Daten im EPI-Service sicherzustellen (andernfalls müssten schwierig umsetzbare und von der Gültigkeitsdauer des jeweiligen Testzertifikats abhängige Löschfristen festgelegt werden), wird die Löschung für Testzertifikate nunmehr einheitlich mit einer Woche ab Probenahme angeordnet. Nach ihrer Löschung sind diese Zertifikate auch nicht mehr über das Zugangsportal zugänglich (Abs. 5).

Zu Z 12 (§ 4d, § 4e, § 4f):

Die Pflichtfelder für Genesungszertifikate sind im neuen § 4d Abs. 1 ausgeführt, sie entsprechen dem „minimum data set" auf EU-Ebene. Zum Begriff „Nachname" wird auf die Ausführungen zu Z 11 (§ 4c) verwiesen. Die für die Ausstellung von Genesungszertifikaten erforderlichen Daten sind zum Teil aus dem Register anzeigepflichtiger Krankheiten zu ermitteln. Die Sozialversicherungsnummer ist erforderlich, um im Wege des Patientenindex das bereichsspezifische Personenkennzeichen (bPK-GH) ermitteln zu können, das beispielsweise für die Einsichtnahme in Zertifikate via Zugangsportal erforderlich ist. Mit diesen Daten und ergänzt um die Metadaten ist das Genesungszertifikat auf Grund einer Anforderung durch eine/einen Genesene/n auszustellen (§ 4d Abs. 2). Die Ergebnisse von Antikörpertests betreffend COVID-19 werden im zentralen Impfregister als Titer(werte) erfasst. Wie die Daten über Impfungen müssen diese Daten von der ELGA GmbH übermittelt werden, damit darauf beruhende Genesungszertifikate ausgestellt werden können.

Inhaltliche Voraussetzungen (Testmethode) sowie die Gültigkeitsdauer von Genesungszertifikaten sind in § 4d Abs. 3 entsprechend den diesbezüglichen Anhaltspunkten im Verordnungsvorschlag der Europäischen Kommission (in der Fassung der Position des Europäischen Parlaments) näher ausgeführt. Gerade betreffend Antikörperbestimmungen werden in absehbarer Zeit neue Erkenntnisse der Wissenschaft bzw. Empfehlungen internationaler oder nationaler Expertengremien erwartet, die eine Anpassung erfordern werden. Auf europäischer Ebene soll dies mit einem delegierten Rechtsakt erfolgen, innerstaatlich ist dafür eine Verordnung (§ 4d Abs. 4) vorgesehen. Damit soll es gegebenenfalls auch möglich sein, Titerwerte und ihre Interpretation oder die Qualifikation des Testpersonals festzulegen. Die übrigen Bestimmungen des § 4d (Abs. 5 und 6) sind den korrespondierenden Bestimmungen in § 4c nachgebildet, wobei die Löschfrist der Daten im EPI-Service auf Grund der längeren Gültigkeitsdauer und zwecks Aufklärung allfälliger Nachfragen mit einer Woche festgelegt wird.

Die Pflichtfelder für Impfzertifikate sind im neuen § 4e Abs. 1 ausgeführt, sie entsprechen dem „minimum data set" auf EU-Ebene. Zum Begriff „Nachname" wird auf die Ausführungen zu Z 11 (§ 4c) verwiesen. Die für die Ausstellung von Impfzertifikaten erforderlichen Daten sind aus dem zentralen Impfregister gemäß § 24c GTelG 2012 zu ermitteln. Dazu wird die ELGA GmbH als datenschutzrechtlich

Verantwortliche für das zentrale Impfregister (§ 27 Abs. 17 Satz 1 GTelG 2012) zur Übermittlung der näher bezeichneten Daten verpflichtet (§ 4e Abs. 2).

Über die Gültigkeitsdauer von Impfzertifikaten liegen derzeit weder Vorgaben auf EU-Ebene noch ausreichend gesicherte wissenschaftliche Erkenntnisse vor. Allfällige Änderungen im Wissensstand sollen daher mittels Verordnung rasch umgesetzt werden können (§ 4e Abs. 3).

Abweichend vom Test- und Genesungszertifikat sieht § 4e Abs. 4 neben der Speicherung der Impfzertifikate in den vorgegebenen Formaten im EPI-Service auch die Übermittlung des Impfzertifikats an die Impfstelle vor. Ziel ist es, geimpften Personen möglichst noch während ihrer Anwesenheit in der Impfstelle ein Impfzertifikat in gedruckter Form zur Verfügung stellen zu können.

§ 4e Abs. 5 sieht die Übermittlung des Impfzertifikats an das zentrale Impfregister zur dortigen Speicherung vor. Zweck dieser Übermittlung ist, es niedergelassenen Ärztinnen und Ärzten sowie Apotheken zu ermöglichen, ihren Patientinnen/Patienten bzw. Kundinnen/Kunden einen Ausdruck des Impfzertifikats zur Verfügung stellen zu können (siehe § 4e Abs. 6). Darüber hinaus ist auch evident, dass bis zum Inkrafttreten dieser Bestimmungen voraussichtlich 3 bis 3,5 Millionen Personen die Voraussetzungen für die Ausstellung eines Impfzertifikats erfüllen werden. Für diese Personen besteht klarerweise nicht mehr die Möglichkeit, ihnen gleichsam im Zuge der Impfung (vgl. § 4e Abs. 4) das Zertifikat zur Verfügung zu stellen. Daher wird die ELGA GmbH als datenschutzrechtlich Verantwortliche für das zentrale Impfregister beauftragt, Personen, die zu diesem Zeitpunkt bereits vollständig geimpft sind, gedruckte Impfzertifikate (pdf-Ausdrucke) im Versandwege zur Verfügung zu stellen. Vollständig geimpft bedeutet gemäß dem aktuellen Stand der Wissenschaft und abhängig vom Impfstoff, dass die Impfserie abgeschlossen und – wie vorgesehen – beide Impfdosen oder auch nur die eine vorgesehene Impfdosis verabreicht wurde oder dass eine genesene Person unabhängig vom verwendeten Impfstoff einmalig (eine Impfdosis) geimpft wurde. Zweck der Übermittlung ist daher auch, der ELGA GmbH die Erfüllung dieses Auftrages zu ermöglichen. Die ELGA GmbH erhält für diese Vorgänge eine dem GTelG 2012 nachgebildete spezielle Zugriffsberechtigung. Für Bürgerinnen und Bürger wird mit § 4e Abs. 6 eine zusätzliche Möglichkeit der Einsichtnahme über das ELGA-Portal geschaffen. Hingewiesen wird in diesem Zusammenhang darauf, dass die Speicherung von Impfdaten sowie die Darstellung im ELGA-Portal vom opt out-Regime für ELGA ausgenommen ist. Niedergelassenen Ärztinnen und Ärzten, die im Wege des e-card-Systems oder über eGovernment-Mechanismen (Wahlarztbereich) Zugang zum zentralen Impfregister haben, soll es durch die Speicherung des Impfzertifikats und unabhängig von allfälligen medizinischen Gründen ermöglicht werden, ihren Patientinnen und Patienten einen Ausdruck des Impfzertifikats zur Verfügung stellen zu können.

Als Frist für die Löschung der Daten im EPI-Service wurde vorläufig ein Jahr festgelegt. Es muss allerdings darauf hingewiesen werden, dass es dafür keine wissenschaftliche Evidenz gibt. Fraglich ist daher auch, ob die diesbezüglichen Änderungen durch das Europäische Parlament im Verordnungsvorschlag der EK angenommen werden (§ 4e Abs. 7).

Die bisherige Rechtsgrundlage für die Überprüfung (Verifizierung) von Zertifikaten, eingeschränkt auf Testzertifikate, findet sich in § 4c, die nunmehr in adaptierter (auf alle Zertifikatsarten erweitert) Form in § 4f ausgeführt wird.

Zum Zweck der Überprüfung dürfen bzw. müssen Überprüfende in die Zertifikate Einsicht nehmen können. Die Authentifizierung der/des Überprüfenden ist nicht erforderlich. Die/Der Überprüfende hat die Identifizierung der den QR-Code präsentierenden Person anhand eines amtlichen Lichtbildausweises durch Abgleich mit den Angaben im QR-Code durchzuführen (§ 4f Abs. 2). Alternativ zum amtlichen Lichtbildausweis kann eine gesicherte elektronische Vorzeigemethode verwendet werden, etwa wenn das Bild einer Person aus einem elektronischen Führerschein oder einem elektronischen Studierendenausweis vorgezeigt wird. Die kryptographische Absicherung kann in diesem Zusammenhang durch eine Signatur, einen Hashwert oder durch eine kryptographisch gleichwertige Sicherungsmethode erfolgen. Die Überprüfung hat anhand des QR-Codes (in elektronischer oder gedruckter Form vorliegend) zu erfolgen, sie ist unabhängig davon, ob ein Zertifikat im digitalen oder analogen Format vorliegt, stets digital. Mit der integrierten Signaturprüfung können allfällige Fälschungen rasch und sicher erkannt werden (§ 4f Abs. 3).

Gefordert wird auf EU-Ebene (Verordnungsentwurf der Europäischen Kommission) ein niederschwelliger Zugang zu den Zertifikaten. Dies umfasst wohl auch die Niederschwelligkeit des Prüfvorganges solcher Zertifikate für Überprüfende selbst, da ansonsten sowohl für Bürgerinnen und Bürger als auch für Überprüfende operative Hürden aufgebaut würden, die die gesamte Maßnahme infrage stellen könnten. Als Beispiel zu nennen wäre etwa, wenn Zertifikate als Eintrittsnachweis für Veranstaltungen mit größerer Teilnahmeanzahl vorgesehen werden. Eine in diesem Zusammenhang erforderliche rasche Abwicklung der Überprüfung ist unverzichtbar, will man lange Wartezeiten vermeiden und die Akzeptanz der Betroffenen sicherstellen. Aus datenschutzrechtlicher Sicht ist zu berücksichtigen, dass es für Überprüfende nicht von

Bedeutung ist, auf Grund welchen Zertifikatstyps vom Vorliegen einer geringen epidemiologischen Gefahr auszugehen ist. Es genügt daher die bloße Rückmeldung, dass ein – aber nicht welches – gültiges Zertifikat verfügbar ist (§ 4f Abs. 4). Damit kann aber auch ein weiterer Aspekt der Niederschwelligkeit adressiert werden. Um eine rasche und benutzerfreundliche Abwicklung der Prüfvorgänge zu gewährleisten, wird für die Verwendung einer Prüfanwendung ausschließlich für innerstaatliche Zwecke gefordert, die Zertifikate in gleichsam verkürzter Darstellung und unter Verwendung bekannter Signalfarben aufzulösen. Dazu ist es notwendig, in solche Anwendungen eine Berechnungslogik für die Gültigkeitsdauern der verschiedenen Zertifikate einzubauen, aus der eine farblich unterlegte Darstellung, ob das Zertifikat „gültig" oder „ungültig" ist, abgeleitet wird. Ein negatives bzw. ungültiges Prüfergebnis, das als „abgelaufen" ausgewiesen und mit rotem Hintergrund angezeigt wird, muss selbstverständlich nicht nur den Umstand, dass die Gültigkeitsdauer des Zertifikats tatsächlich überschritten ist, sondern auch jene Fälle, in denen kein Zertifikat verfügbar ist, abdecken (§ 4f Abs. 5).

In Bezug auf die elektronische Anwendung zur Überprüfung von Zertifikaten ist ergänzend festzuhalten, dass die Europäische Kommission eine open source-Lösung zur Verfügung stellt, die maßgeblich von Österreich initiiert und mitentwickelt wird. Ihre vollumfängliche Verwendung in Anwendungen zur Verifizierung von Zertifikaten wir daher unterstützt. Um mögliche unerwünschte Änderungen des Prüfmechanismus durch Anbieter von Prüfanwendungen erkennen zu können, sieht § 4f Abs. 6 eine Offenlegung des source code und die Möglichkeit zur Mängelbehebung vor. Ferner soll die Verwendung eines geänderten Prüfmechanismus durch ergänzende Publikation des Zugangs zum open source Code gefördert werden.

Jede Verarbeitung von Identifizierungsdaten, von Zertifikaten (des QR-Codes), von im QR-Code enthaltenen Daten oder sogenannter Verkehrsdaten (z. B. Logdaten) durch die/den Überprüfende/n ist unzulässig (§ 4f Abs. 7).

Zu Z 13 (§ 5 Abs. 4):

Damit erfolgt eine redaktionelle Berichtigung.

Zu Z 14 (§ 5a Abs. 1):

Gemäß Art. 4 Z 7 DSGVO ist Verantwortlicher derjenige, der alleine oder gemeinsam mit anderen über Zweck und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

Die Zwecke eines Screeningprogramms sind in Abs. 1 Z 1 bis 3 und Abs. 7 vorgegeben. Gemäß Abs. 1 können Landeshauptleute, soweit derartige Programme nur ein Bundesland betreffen, mit Zustimmung des Bundesministers innerhalb des jeweiligen Bundeslandes durchführen. Da die Zwecke durch Abs. 1 und Abs. 7 im Gesetz vorgegeben sind und die Landeshauptleute darüber entscheiden, ob und unter welchen Voraussetzungen ein Screeningprogramm durchgeführt wird, wird durch die vorgeschlagene Änderung klargestellt, dass die Landeshauptleute in solchen Fällen die datenschutzrechtlichen Verantwortlichen sind. Da sämtliche Kosten vom Bund getragen werden, bedarf die Durchführung eines Screeningprogramms durch die Landeshauptleute der Zustimmung des Bundesministers (vgl. 484/A XXVII. GP, 6); dies begründet jedoch keine (gemeinsame) Verantwortlichkeit des Bundesministers, da dieser nicht über Zweck und Mittel entscheidet, sondern lediglich als Kostenstelle fungiert.

Zu Z 15 (§ 5a Abs. 2 Z 1):

Mit der Aufnahme der Sozialversicherungsnummer in den Klammerausdruck wird eine Inkonsistenz mit § 5b Abs. 3 Z 1 behoben. Gemäß § 5b Abs. 3 Z 1 darf die Sozialversicherungsnummer im Screeningregister gespeichert werden, da sie in der Auflistung der nunmehr zu korrigierenden Bestimmung fehlt, dürfte sie allerdings nicht erhoben werden.

Zu Z 16 (§ 5a Abs. 7 und 8):

Der Änderungsvorschlag bezieht sich auf den Abänderungsantrag, der am 3.5.2021 im Parlament zur Beratung gelangt ist. Im Falle dessen Beschlussfassung bedarf es einer geringfügigen Anpassung aufgrund der Einführung des grünen Passes mit diesem Vorhaben.

Zu Z 17 (§ 25c Abs. 2 Z 3):

Insbesondere im Rahmen des nunmehr wieder vermehrt stattfindenden Tagestourismus ist davon auszugehen, dass Einreisende nicht über eine Wohn- oder Aufenthaltsadresse verfügen, so dass auf diesen Umstand auch bei den vorgesehenen Datenarten Rücksicht zu nehmen ist.

Zu Z 18 (§ 25a Abs. 2 Z 10):

Die in § 25a Abs. 2 genannten Daten, die im Zuge einer Verordnung nach Abs. 1 der für den Wohnsitz oder Aufenthalt örtlich zuständigen Bezirksverwaltungsbehörde im Zusammenhang mit der Einreise von Personen aus Staaten oder Gebieten mit Vorkommen von COVID-19 bekannt gegeben werden müssen, werden um die in § 4b genannten Zertifikate erweitert.

Zu Z 19 (§ 28a Abs. 1):

Grundsätzlich sind die Organe des öffentlichen Sicherheitsdienstes nach § 28a EpiG, da die COVID-19-EinreiseV insbesondere auf 25 beruht, zur Assistenzleistung und Kontrolltätigkeit im Auftrag der Gesundheitsbehörden berufen. Da aufgrund der Öffnungen mit vermehrter Reisetätigkeit zu rechnen ist, werden auch die Organe der Landespolizeidirektionen nach § 12b GrekoG in den § 28a EpiG im Zusammenhang mit der Ausübung von Aufgaben nach § 25 EpiG aufgenommen.

Zu Z 20 (§ 28d Abs. 1 Z 5):

Hiermit werden Tierärzte den in dieser Bestimmung genannten Gesundheitsberufen gleichgestellt.

Zu Z 21 (§ 28d Abs. 1):

Mangels entsprechender Verschwiegenheitspflicht im Zusammenhang mit Abstrichen aus Nase und Rachen einschließlich Point-of-Care-Covid-19Antigen-Test zu diagnostischen Zwecken für Angehörige des tierärztlichen Berufes wird eine dementsprechende subsidiäre Verschwiegenheitspflicht angeordnet.

Zu Z 22 (§ 50 Abs. 23):

Diese Bestimmung legt das Inkrafttreten – mit Ausnahme der §§ 4b bis 4f samt Überschriften –mit dem auf die Kundmachung folgenden Tag fest. Im Hinblick auf diejenigen Bestimmungen, die Zertifikate im Zusammenhang mit SARS-CoV-2 festlegen, wird das Außerkrafttreten der einschlägigen Bestimmungen mit dem 30. Juni 2022 festgelegt.

Zu Artikel 2 (COVID-19-Maßnahmengesetz)

Zu Z 1 (§ 1 Abs. 5b):

Diese Bestimmung kann entfallen, da deren Inhalt schon durch § 4c Abs. 4 EpiG abgedeckt wird. Im Hinblick auf die Form des Nachweises wird in § 1 Abs. 5g eine umfassende Verordnungsermächtigung für den für das Gesundheitswesen zuständigen Bundesminister geschaffen, die sich auch auf Schutzimpfungen gegen COVID-19 und überstandene Infektionen mit SARS-CoV-2 bezieht. Darüber hinaus werden die entsprechenden Absätze neu nummeriert.

Zu Z 2 (§ 1 Abs. 5b [neu]):

Auf Grund der Streichung von Abs. 5b wird hier auf ein Testzertifikat nach § 4c des Epidemiegesetzes verwiesen.

Zu Z 3 (§ 1 Abs. 5b [neu]):

Der neu angefügte Satz dient der Klarstellung, dass die darin vorgesehenen Vorhalte- und Nachweispflichten auch für die in § 4b des Epidemiegesetzes 1950 genannten Zertifikate gelten. § 4f enthält zwar ebenso Bestimmungen zur Identifizierung einer Person durch Überprüfende, jedoch lediglich im Zusammenhang mit der Authentifizierung der in § 4b des Epidemiegesetzes 1950 genannten Zertifikate. Eine darüber hinaus gehende Nachweispflicht gegenüber Behörden, Organen des öffentlichen Sicherheitsdienstes und Personen, die bei sonstiger verwaltungsbehördlicher Strafbarkeit gemäß § 8 Abs. 3, 3 und 5a dafür Sorge zu tragen haben, dass in ihrem Einflussbereich die jeweils geltenden Beschränkungen eingehalten werden, ist lediglich in dieser Bestimmung verankert. Hierdurch wird angeordnet, dass diese Pflichten auf im Zusammenhang mit diesen Zertifikaten – und nicht nur im Zusammenhang mit anderslautenden Nachweisen – zur Anwendung gelangen.

Zu Z 4 (§ 1 Abs. 5c [neu]):

Diese Bestimmung wird dahingehend vereinfacht, als neben der Schutzimpfung gegen COVID-19 lediglich eine überstandene Infektion mit SARS-CoV-2 angeführt wird. Die bisher enthaltenen Umstände einer ärztlichen Bestätigung, eines Absonderungsbescheides, der wegen einer Infektion des Bescheidadressaten mit SARS-CoV-2 erlassen wurde und eines durchgeführten Tests, der das Vorhandensein von Antikörpern gegen eine Infektion mit SARS-CoV-2 bestätigt, werden ausdrücklich in Abs. 5d (neu) erwähnt.

Zu Z 5 (§ 1 Abs. 5d [neu]):

Hierbei handelt es sich um die Berichtigung eines Redaktionsversehens.

Zu Z 6 (§ 1 Abs. 5d [neu]):

Diese Bestimmung ordnet an, dass – auf Grund der Vereinfachung in Abs. 5c (neu) – von einer grundsätzlichen Gleichstellung mit einem negativen Test auf SARS-CoV-2 bei Vorliegen einer ärztlichen Bestätigung über eine überstandene Infektion mit SARS-CoV-2, eines Absonderungsbescheides, der wegen einer Infektion des Bescheidadressaten mit SARS-CoV-2 erlassen wurde, oder eines durchgeführten Tests, der das Vorhandensein von Antikörpern gegen eine Infektion mit SARS-CoV-2 bestätigt, auszugehen ist.

Zu Z 7 und Z 8 (§ 1 Abs. 5d [neu] und 5e [neu]):

Hier werden lediglich die Zitate angepasst.

Zu Z 9 (§ 1 Abs. 5f und 5g):

Mit dieser Bestimmung wird klargestellt, dass die in § 4b Abs. 1 Z 1 bis 3 EpiG genannten Zertifikate zum Nachweis eines negativen Tests auf SARS-CoV-2, einer Schutzimpfung gegen COVID-19 oder einer überstandenen Infektion mit SARS-CoV-2 herangezogen werden können. Neben diesen Zertifikaten soll es aber weiterhin möglich sein, auch sonstige Dokumente zum Nachweis eines negativen Tests auf SARS-CoV-2, einer Schutzimpfung gegen COVID-19 oder einer überstandenen Infektion mit SARS-CoV-2 heranzuziehen. So kann z. B. auch weiterhin der Internationale („gelbe“) Impfpass als Nachweis einer Schutzimpfung gegen COVID-19 herangezogen werden. Für derartige sonstige Dokumente soll die Möglichkeit bestehen, durch Verordnung des für das Gesundheitswesen zuständigen Bundesministers deren Form festzulegen. Diese dürfen jedoch lediglich die in § 4c Abs. 1, § 4d Abs. 1 und § 4e Abs. 1 des Epidemiegesetzes 1950 genannten Daten enthalten. Auf Grund des Umstandes, dass die Art und Weise der Ausstellung dieser Dokumente – insbesondere im Zusammenhang mit jenen, die eine überstandene Infektion mit SARS-CoV-2 bestätigen, da diese überwiegend von niedergelassenen Ärzten ausgestellt werden – sehr heterogen und dezentral erfolgt, ist es nicht möglich, hierfür einen einheitlichen dahinterliegenden Datenverarbeitungsprozess abzubilden, zumal es sich ja auch um ein handschriftlich ausgefülltes Formular handeln könnte.

Zu Z 10 (§ 9 Abs. 3):

Um eine höhere Kontrolldichte im Zusammenhang mit COVID-19-Präventionkonzepten zu ermöglichen, werden Aufsichtsorgane gemäß §§ 24ff des Lebensmittelsicherheits- und Verbraucherschutzgesetzes – LMSVG, BGBl. I Nr. 151/2005, Organe der zur Vollziehung der gewerberechtlichen Vorschiften zuständigen Behörden und Organe der Arbeitsinspektion berechtigt, im Rahmen ihrer dienstlichen Aufgaben vor Ort auch COVID-19-Präventionskonzepte zu überprüfen.

Zu Z 12 (§ 13 Abs. 12):

Hier wird das Inkrafttreten der Bestimmungen dieses Bundesgesetzes geregelt.

Anlage

DATENSCHUTZ-FOLGENABSCHÄTZUNG

SYSTEMATISCHE BESCHREIBUNG

der geplanten Verarbeitungsvorgänge, Zwecke sowie berechtigten Interessen

Das EPI-Service ist ein elektronisches Service, welches Zertifikate erstellt, die zum Nachweis eines Tests auf COVID-19, einer Genesung von COVID-19 oder einer Impfung gegen COVID-19 dienen. Die Bereitstellung des Zertifikats wird als QR-Code in elektronischer Form und im Format PDF erfolgen. Die Verwendung des Zertifikats soll überall dort erfolgen, wo ein Nachweis einer geringen epidemiologischen Gefahr in Bezug auf SARS-CoV-2 aus gesetzlichen Gründen erforderlich ist (zum Beispiel Eintrittstest in Gastronomie, Handel, Tourismus). Gemäß der gemeinsamen Zielsetzung der Mitgliedsstaaten der Europäischen Union, die Freizügigkeit innerhalb der Union wiederherzustellen und Tourismus und Geschäftsreisen zu ermöglichen, sollen die Zertifikate auf europäischer Ebene interoperabel sein, und „die Freizügigkeit von Personen, die keine Gefahr für die öffentliche Gesundheit darstellen, etwa weil sie gegen SARS-CoV-2 immun sind und das Virus nicht übertragen können, sollte nicht eingeschränkt werden, da dies zur Erreichung des angestrebten Ziels nicht erforderlich wäre“ (vgl. ErwG 7 des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von Impfungen, Tests und der Genesung mit der Zielsetzung der Erleichterung der Freizügigkeit während der COVID-19-Pandemie [digitales grünes Zertifikat, im Folgenden kurz: „*VO-Entwurf*“]). Die nachfolgende Datenschutz-Folgenabschätzung beschreibt den Grünen Pass und das EPI-Service.

Art der Verarbeitung (ErwG 90 DSGVO):

Das EPI-Service erstellt aufgrund der übermittelten Daten Zertifikate für

- getestete Personen,
- genesene Personen und
- geimpfte Personen.

Die Daten können in Papierform oder in digitaler Form als Nachweis der oben genannten Personen verwendet werden, dass diese entweder nicht an COVID-19 erkrankt sind oder gegen COVID-19 immun sind.

Im Rahmen des EPI-Service werden folgende Daten von getesteten Personen verarbeitet (vgl. § 4c Abs. 1 EpiG):

- Nachname(n) und Vorname(n) der getesteten Person, in dieser Reihenfolge,
- Geburtsdatum der getesteten Person,
- Zielkrankheit oder -erreger, auf die oder den die Person getestet wurde, ausschließlich lautend auf „COVID-19“ (umfasst auch „SARS-CoV-2“ oder dessen Varianten),
- Art des Tests,
- Bezeichnung des Tests und des Herstellers des Tests (optional bei NAAT-Tests),
- Datum und Uhrzeit der Probenahme,
- Testergebnis,
- Bezeichnung des Testzentrums oder der testenden Einrichtung,
- Bezeichnung des Staates, in dem der Test durchgeführt wurde,
- Bezeichnung des Ausstellers des Testzertifikats und
- eindeutige Kennung des Testzertifikats
- sowie nach § 4c Abs. 2 - sofern vorhanden – Sozialversicherungsnummer.

Aus den oben angegebenen übermittelten Daten wird im Wege der Abfrage des Patientenindex (§ 4 iVm § 18 GTelG 2012) oder – im Falle des Fehlens der Sozialversicherungsnummer – im Wege der Stammzahlenregisterbehörde das bereichsspezifische Personenkennzeichen Gesundheit (bPK-GH) ermittelt und das Testzertifikat erstellt. Das Testzertifikat wird als PDF und QR-Code mit dem bPK-GH im EPI-Service gespeichert.

Im Rahmen des EPI-Service werden folgende Daten von genesenen Personen verarbeitet (vgl. § 4d Abs. 1 EpiG):

- Nachname(n) und Vorname(n) der getesteten Person, in dieser Reihenfolge,
- Geburtsdatum der getesteten Person,
- Krankheit oder Erreger, von der oder dem die Person genesen ist, ausschließlich lautend auf „COVID-19“ (umfasst auch „SARS-CoV-2“ oder dessen Varianten),
- Datum des ersten positiven Testergebnisses,
- Bezeichnung des Staates, in dem der Test durchgeführt wurde,
- Bezeichnung des Ausstellers des Genesungszertifikats,
- Gültigkeitsbeginn und Gültigkeitsende des Genesungszertifikats,
- eindeutige Kennung des Genesungszertifikats.

Die Vorgehensweise zur Erstellung des Zertifikats erfolgt analog zu den Zertifikaten für Getestete.

Im Rahmen des EPI-Service werden folgende Daten von geimpften Personen verarbeitet (vgl. § 4e Abs. 1 EpiG):

- Nachname(n) und Vorname(n) der geimpften Person in dieser Reihenfolge,
- Geburtsdatum der geimpften Person,
- Krankheit oder Erreger, gegen die oder den die Person geimpft ist, ausschließlich lautend auf „COVID-19“ (umfasst auch „SARS-CoV-2“ oder dessen Varianten),
- Impfstoff/Prophylaxe (generische Beschreibung des Impfstoffs oder seiner Komponenten),
- Impfarzneimittel (Bezeichnung des Impfstoffs gemäß Zulassung),
- Zulassungsinhaber oder Hersteller des Impfstoffs,
- Nummer der Impfdosis und die Gesamtanzahl der Impfdosen einer Impfserie,
- Datum der letzten Impfung der Impfserie,
- Bezeichnung des Staates, in dem die Impfung durchgeführt wurde,
- Bezeichnung des Ausstellers des Impfzertifikats und
- eindeutige Kennung des Impfzertifikats.

Die ELGA GmbH übermittelt die Impfdaten und die Chargennummer des verabreichten Impfstoffs sowie das bPK-GH aus dem zentralen Impfregister an den für das Gesundheitswesen zuständigen Bundesminister. Dies wird durch technisch-organisatorische Maßnahmen abgesichert. Das Zertifikat wird im EPI-Service gespeichert und an die ELGA GmbH übermittelt, um eine Speicherung im zentralen Impfregister zu ermöglichen.

Der erstellte QR-Code enthält die oben angegebenen Daten und wird – nach Feststehen der EU-Vorgaben – auch interoperabel innerhalb der Union verwendet werden können und damit auch die Freizügigkeit innerhalb der Union nach den Vorgaben der VO ermöglichen. Weiters muss eine Überprüfung der Authentizität, Gültigkeit und Integrität des Zertifikats möglich sein (§ 4b Abs. 4 EpiG).

Beim Prüfen des Zertifikats durch Überprüfende nach § 1 Abs. 5 Z 5 und 6 COVID-19-MG erfolgt eine Offline-Identitätskontrolle durch Vorlage eines Ausweisdokuments (Amtlicher Lichtbildausweis). Hierbei findet keine zusätzliche Speicherung statt und es erfolgt nur eine Überprüfung der Richtigkeit.

Eine Überprüfung findet mittels Elektronischer Anwendungen zur Verifizierung von Zertifikaten gemäß §§ 4c bis 4e statt, die Ergebnisse sind „gültig“ oder „ungültig“.

Im Falle des Rückgabewerts „ungültig“ dürfen über dessen Ursache nur folgende drei mögliche Ergebnisse angezeigt werden:

- „Gültigkeitsdauer abgelaufen“,
- „QR-Code fehlerhaft“,
- „Signaturprüfung fehlgeschlagen“

Umfang der Verarbeitung (ErwG 90 DSGVO):

Grundsätzlich kann die Verarbeitung jede in Österreich ansässige Person betreffen. Jede in Österreich ansässige Person ist berechtigt, an Screeningprogrammen (§ 5a EpiG) teilzunehmen und somit Testergebnisse zu erhalten und sich privaten Tests in Laboren zu unterziehen. Ebenso ist es denkbar, dass jede in Österreich ansässige Person an COVID-19 erkrankt und ein Genesungszertifikat erhält. Für Impfungen ist der Umfang der Verarbeitung zum jetzigen Zeitpunkt auf Personen beschränkt, die

mindestens 16 Jahre alt sind. Es können im Einzelfall auch Personen aus medizinischen Gründen von der Impfung ausgeschlossen sein (z. B. aufgrund von Erkrankungen).

Bei den getesteten Personen kann es sich auch um Minderjährige handeln, die von Ihren Obsorgeberechtigten begleitet werden. Impfungen sind im Zeitpunkt der Erstellung dieser Datenschutz-Folgenabschätzung erst ab dem 16. Lebensjahr möglich, sodass aktuell nur Minderjährige zwischen dem 16. und 18. Lebensjahr für die Erstellung von Impfzertifikaten infrage kommen. Alle Minderjährigen unter 16 können bis zu einer allfälligen Freigabe von Impfungen für diese Altersgruppe durch Testungen Testzertifikate erhalten. Genesene können grundsätzlich Personen sämtlicher Altersstufen einschließlich minderjähriger Personen sein.

Testergebnisse werden durch die Einrichtungen, die SARS-CoV-2-Tests im Sinne des § 4b Abs. 2 auswerten, an den für das Gesundheitswesen zuständigen Bundesminister übermittelt. Die Impfdaten werden von der ELGA GmbH an den für das Gesundheitswesen zuständigen Bundesminister übermittelt. Die Zertifikatsdaten werden nur in sehr eingeschränktem Maß verarbeitet: Zum einen durch den für das Gesundheitswesen zuständigen Bundesminister, sowie im Fall von Impfungen auch durch die ELGA GmbH im Rahmen ihrer gesetzlichen Aufgaben. Teststellen (im Fall von Testungen) bzw. niedergelassene Ärztinnen und Ärzte (im Fall von Impfungen) und Apotheken dürfen Zertifikate ausdrucken und zu diesem Zweck Daten verarbeiten. Ferner besteht für die in § 4b Abs. 7 Z 2 EpiG genannten Stellen die Möglichkeit, die Zertifikate auszudrucken. Die Betroffenen können die Zertifikate auch selbst abrufen oder ausdrucken, ohne dass eine weitere Stelle eingeschaltet wird (§ 4b Abs. 7 Z 3 EpiG).

Kontext der Verarbeitung (Art-29-Datenschutzgruppe, WP 248, 21):

Die Verarbeitung erfolgt im Kontext der Pandemiebekämpfung und den damit verbundenen Regelungen im EpiG bzw. COVID-19-MG. Hierbei ist es erforderlich bei bestimmten Tätigkeiten sicherzustellen, dass von Personen eine geringere epidemiologische Gefahr ausgeht.

Zwecke der Verarbeitung (Art. 35 Abs. 7 lit. a DSGVO):

Zweck der Verarbeitung ist die Zurverfügungstellung von Zertifikaten zum Nachweis eines Tests auf eine Infektion mit SARS-CoV-2, einer überstandenen Infektion mit SARS-CoV-2 und einer empfangenen Schutzimpfung gegen COVID-19gemäß § 4b Abs. 1 EpiG.

Empfängerinnen und Empfänger (Art-29-Datenschutzgruppe, WP 248, 21):

Empfängerin ist die Auftragsverarbeiterin für das EPI-Service, welche durch den für das Gesundheitswesen zuständigen Bundesminister festzulegen ist. Dieses Vertragsverhältnis ist in datenschutzrechtlicher Hinsicht durch eine Vereinbarung nach Art. 28 DSGVO abgesichert.

Die Betroffenen erhalten den QR-Code, welcher die oben angegebenen Daten enthält. Betroffene erhalten Einsichtnahme zum Druck und zum Download von Zertifikaten im Wege des Zugangsportals nach § 23 GTelG 2012 (§ 4c Abs. 7 Z 3 EpiG).

Empfänger sind ferner

- Landeshauptleute, die Zertifikate in elektronischer Form an Betroffene weitergeben (§ 4b Abs. 7 Z 1),
- alle in § 4b Abs. 7 Z 2 EpiG genannten öffentlichen Stellen, welche das Zertifikat auf Anforderung des Betroffenen ausdrucken,
- Teststellen, die das Testzertifikat auf Anforderung des Betroffenen ausdrucken (§ 4c Abs. 2 EpiG),
- Impfstellen, die das Impfzertifikat auf Anforderung des Betroffenen ausdrucken (§ 4e Abs. 4 EpiG)
- Ärztinnen und Ärzte sowie Apotheken, die das Impfzertifikat auf Anforderung des Betroffenen ausdrucken (§4e Abs. 6 EpiG) und
- die ELGA GmbH, im Falle von Impfzertifikaten nach den Vorgaben von § 4e Abs. 5 EpiG.

Speicherdauer (Art-29-Datenschutzgruppe, WP 248, 21):

Da es unter Umständen notwendig ist das Vorhandensein eines Zertifikats über einen gewissen Zeitraum auch nach dem Ablauf der Gültigkeit nachvollziehen zu können, ist eine Speicherung der Daten im EPI-Service auch über den Zeitpunkt des Ablaufs hinaus für einen gewissen Zeitraum erforderlich.

Im Einzelnen erfolgt eine Löschung der Daten im EPI-Service:

- Testzertifikate: 1 Woche ab dem Datum der Probenahme (§ 4c Abs. 5 EpiG)
- Genesungszertifikate: 1 Woche ab Gültigkeitsende (§ 4d Abs. 6 EpiG)
- Impfzertifikate: 1 Jahr ab Übermittlung an das zentrale Impfregister (§ 4e Abs. 7 EpiG)

Gemäß § 4 Abs. 8 EpiG sind fehlerhafte Genesungs- und Impfzertifikate vor Ablauf der Gültigkeitsdauer zu widerrufen. Widerrufene Zertifikate sind unverzüglich im EPI-Service zu löschen.

Funktionelle Beschreibung der Verarbeitung (Art. 35 Abs. 7 lit. a DSGVO):

1. Die betroffenen Personen nehmen das Testangebot in Österreich wahr, sind von COVID-19 genesen oder haben sich gegen COVID-19 impfen lassen.

2. Diese Informationen werden ins EPI-Service eingemeldet. Die Informationen kommen entweder von Labors oder Teststraßen (Testung), Labors und Ärzten (Antikörpernachweis bei Genesenen) bzw. Impfstraßen und Ärzten (Impfung) über den Elektronischen Impfpass (ELGA GmbH).

3. Das EPI-Service erstellt den QR-Code mit den notwendigen Daten.

4. Die betroffenen Personen erhalten den QR-Code auf einem Papierzertifikat oder als digitale Version.

5. Die Informationen werden bei der Inanspruchnahme bestimmter Dienstleistungen verifiziert. Die überprüfende Person bekommt als Ergebnis, dass das Zertifikat gültig oder ungültig ist. Um die Identität zu prüfen, muss sich die betroffene Person ausweisen. Die überprüfende Person erhält keine Kopie der Daten.

6. Nach Ablauf der Gültigkeit werden die Zertifikate gelöscht (Details siehe oben).

Beschreibung der Anlagen (Hard- und Software bzw. sonstige Infrastruktur, Art-29-Datenschutzgruppe, WP 248, 21):

Als Software werden RedHat Enterprise Linux 7, RedHat openShift, Postgres (Datenbank), Apache, (Java in Container) eigesetzt. Die Software wird regelmäßig gemäß Prozess aktualisiert.

Als Hardware werden überwiegend HP-Server mit Intel-Prozessoren eingesetzte. Die Hardware ändert sich mit dem jeweiligen Life-Cycle.

BEWERTUNG

der Notwendigkeit und Verhältnismäßigkeit

Festgelegter, eindeutiger und legitimer Zweck (Art. 5 Abs. 1 lit. b DSGVO):

Die Daten werden nur zum gesetzlich vorgesehenen Zwecken verwendet:

- Erstellung eines Zertifikats für Eintrittstest nach COVID-19-MG auf nationaler Ebene für die Inanspruchnahme von bestimmten Dienstleistungen (zB körpernahe Dienstleistungen, Gastronomie, Tourismus) und dessen Verifizierung sowie zur allfällige Fehlersuche und -behebung und Erstellung von statistischen Auswertungen (vgl. § 4b Abs. 8 und 9 EpiG).
- Nach deren Inkrafttreten die Erfüllung der Zielsetzung der entsprechenden europäischen Verordnung und der damit verbundenen Wiederherstellung der Personenfreizügigkeit in der Union.
- Erfüllung der Vorgaben des EpiG und des COVID-19-MG

Die Daten werden ausschließlich in einer mit diesen Zwecken zu vereinbarenden Weise verarbeitet.

Die durch die nationalen und europäischen Gesetze bzw. Verordnungen vorgesehenen Zwecke sind eindeutig formuliert. Die Anwendung dient den oben angegebenen Zwecken. Eine Verwendung darüber hinaus findet nicht statt.

Die Verarbeitung verstößt nicht gegen höherrangige geltende Rechtsnormen; insbesondere wird mit § 4b Abs. 3 EpiG eine Rechtsgrundlage nach Art. 6 Abs. 1 lit. e (Einrichtung und der Betrieb des EPI-Service) bzw. Art. 6 Abs. 1 lit. c (Zulieferung der Daten an das EPI-Service) in Verbindung mit Art. 9 Abs. 2 lit. i DSGVO geschaffen.

Rechtmäßigkeit der Verarbeitung (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 6 DSGVO):

Die Verarbeitung kann auf nach Art. 6 Abs. 1 lit. e (Einrichtung und der Betrieb des EPI-Service) bzw. Art. 6 Abs. 1 lit. c (Zulieferung der Daten an das EPI-Service) und bezogen auf besondere Kategorien personenbezogener Daten auf Art. 9 Abs. 2 lit. i DSGVO und § 4b Abs. 3 EpiG gestützt werden. ErwG 37 des VO-Entwurfs erwähnt ausdrücklich, dass nur die Verarbeitung personenbezogener Daten im Zusammenhang mit den interoperablen Zertifikaten für die Zwecke der Reisefreiheit durch die Verordnung abschließend geregelt wird. Art. 8a des VO-Entwurfs ermöglicht die Verwendung der Zertifikate zu innerstaatlichen Zwecken mit Ausnahme der Reisefreiheit unter einigen Bedingungen für die nationale Umsetzung.

Die strengen Voraussetzungen von Art. 9 Abs. 2 lit. i DSGVO sind erfüllt. Für den Begriff der öffentlichen Gesundheit ist gemäß ErwG 54 der DSGVO die VO (EG) 1338/2008 heranzuziehen. Es handelt sich demnach bei Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit im Sinne der VO

(EG) 1338/2008 um „alle Elemente im Zusammenhang mit der Gesundheit, nämlich den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von Gesundheitsversorgungsleistungen und den allgemeinen Zugang zu diesen Leistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität". Die DSGVO nennt beispielhaft etwa der Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren. Bei SARS-CoV-2 handelt es sich um eine schwerwiegende grenzüberschreitende Gesundheitsgefahr mit hoher Mortalität in bestimmten Alter- und Risikogruppen und mit Langzeitfolgen (sog. „Long Covid") für einen Teil der Erkrankten. Aber auch die Bereitstellung von Gesundheitsversorgungsleistungen und der allgemeine Zugang zu diesen Leistungen ist durch SARS-CoV-2 berührt, weil die Zahl der schwer Erkrankten die Ressourcen des Gesundheitswesens über seine Grenzen hinaus belasten könnte.

Zudem erfüllen die Rechtsgrundlagen auch die qualitativen Voraussetzungen von Art. 9 Abs. 2 lit. i DSGVO. Nationale Rechtsgrundlagen müssen hierbei spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsehen. Insbesondere darf die Verarbeitung nicht dazu führen, dass „Dritte, unter anderem Arbeitgeber oder Versicherungs- und Finanzunternehmen, solche personenbezogenen Daten zu anderen Zwecken verarbeiten" (vgl. ErwG 54 S. 4 zur DSGVO). Die strikte Zweckbindung ist dadurch sichergestellt, dass die Ausstellung der Zertifikate im EPI-Service dafür sorgt, dass die Gesundheitsdaten der Betroffenen an einem zentralen Ort gespeichert sind, der durch technische und organisatorische Maßnahmen entsprechend abgesichert ist (s.u.). Es kommt im Rahmen einer Überprüfung zu keiner Kopie, sondern der Prüfende verifiziert lediglich die Gültigkeit des Zertifikats, wobei die Überprüfung „offline" am Endgerät erfolgt. Die Identifikation der Personen durch ein geeignetes Ausweisdokument erfolgt ebenfalls offline. Ein Missbrauch der Daten durch Dritte ist somit ausgeschlossen. Zudem unterliegen die Personen, welche die Daten erheben, die letztlich im EPI-Service verarbeitet werden, beruflichen Verschwiegenheitspflichten (z. B. § 54 ÄrzteG, § 6 SanG). Durch die Maßnahmen ist auch sichergestellt, dass die einschlägigen Grundrechte der Betroffenen (z. B. § 1 DSG, Art. 8 EMRK) in Ihrem Wesensgehalt nicht angetastet werden.

Angemessenheit der Verarbeitung (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 5 Abs. 1 lit. c DSGVO):

Zur Reduktion des Infektionsgeschehens und damit einhergehend auch der Todesfälle stehen mehrere Möglichkeiten zur Verfügung. Das langfristige Ziel stellt die Möglichkeit der Durchimpfung der Gesellschaft dar. Solange jedoch nicht ausreichend Impfstoff zur Verfügung steht um alle impfwilligen Personen mittels einer COVID-19-Impfung zu immunisieren, müssen Testungen auf SARS-CoV-2 als ergänzende Maßnahme hinzutreten. Diese Testungen, deren Teilnahme ausschließlich freiwillig erfolgt, ermöglichen die Feststellung von symptomlosen Erkrankungen und das damit einhergehende, temporäre Ausscheiden der positiv getesteten Personen aus dem gesellschaftlichen Leben um bisher unerkannte Infektionsketten zu durchbrechen. Den negativ getesteten Personen wird aufgrund der, wenn auch nur temporär festgestellten, geringen epidemiologischen Gefahr die Teilnahme am gesellschaftlichen Leben analog zu Geimpften ermöglicht. Die zeitliche Befristung des Testergebnisses ist aufgrund seiner nur zum Zeitpunkt der Testung gültigen Aussage unbedingt erforderlich, doch wird der dadurch entstehende Nachteil gegenüber Geimpften, welche lediglich einen gewissen Zeitraum nach erfolgter Impfung abwarten müssen, durch die Niederschwelligkeit der Testangebote zumindest zum Teil kompensiert.

Alternativ zu der Gleichstellung von Geimpften und Genesenen mit Getesteten könnte der Gesetzgeber das Wirtschaftsleben bis zum Erreichen bestimmter Inzidenzen noch weiter herunterfahren. Dies würde die wirtschaftlichen und mittelbaren gesundheitlichen (insbesondere psychischen) Folgen der Pandemie noch weiter verschlimmern und ist somit kein gelinderes Mittel.

Auch ist es nach jetzigen wissenschaftlichen Erkenntnissen nicht sinnvoll, Personen, welche eine COVID-19-Erkrankung überstanden oder alternativ oder ergänzend eine COVID-19-Schutzimpfung erhalten haben, die Teilnahme am wirtschaftlichen und gesellschaftlichen Leben zur erschweren, da diese für einen gewissen Zeitraum keine epidemiologische Gefahr darstellen.

Die Verarbeitung dient dazu, den betroffenen Personen – ohne Erhöhung des Infektionsgeschehens – die Rückkehr zur Normalität zu ermöglichen. Eine solche Lösung dürfte staatlicherseits auch geboten sein, weil jegliche Einschränkungen des öffentlichen Lebens nur für solche Personen gerechtfertigt sein können, von denen eine epidemiologische Gefahr ausgeht.

Die gesammelten Daten sind darüber hinaus adäquat; es werden keine Daten gesammelt, die dem Zweck nicht entsprechen. Die Verarbeitung ist somit angemessen.

Erheblichkeit der Verarbeitung (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 5 Abs. 1 lit. c DSGVO):

Ohne die Verfügbarkeit der oben genannten Möglichkeiten zur Pandemiebekämpfung sowie und die Verarbeitung der zur Ausstellung der Zertifikate notwendigen, oben referenzierten Datenkategorien kann der oben beschriebene Zweck nicht erreicht werden.

Alle gesammelten Daten sind daher erheblich.

Beschränktheit der Verarbeitung auf das notwendige Maß (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 5 Abs. 1 lit. c DSGVO):

Die Verarbeitung ist auf das notwendige Maß beschränkt (vgl. auch § 4b Abs. 9 EpiG), insbesondere ist die Art der Empfänger eingeschränkt. Eine lokale Kopie bei der Inanspruchnahme von Dienstleistungen erfolgt auch nicht.

Speicherbegrenzung (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 5 Abs. 1 lit. e DSGVO):

Die Daten werden nach Ablauf der Gültigkeit des Zertifikates in beschränktem Umfang aufbewahrt und anschließend gelöscht (siehe dazu bereits oben).

Information der betroffenen Personen bei Erhebung (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 13 DSGVO):

Gemäß § 4c Abs. 3 Z 2 lit. a EpiG haben die Einrichtungen, die SARS-CoV-2-Tests im Sinne des § 4b Abs. 2 auswerten, die betroffenen Personen gemäß Art. 13 DSGVO in geeigneter Weise zu informieren. Gemäß § 4b Abs. 2 Z 2 der eHealth-Verordnung (eHealthV) obliegt der ELGA GmbH die Information der betroffenen Personen gemäß den Art. 13 durch Veröffentlichung einer Datenschutzinformation auf der Website der ELGA GmbH.

Zu den genesenen Personen siehe sogleich unten.

Information der betroffenen Personen, wenn die Daten nicht bei ihnen erhoben werden (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 14 DSGVO):

Eine Information gemäß Art. 14 DSGVO ist aufgrund dessen Abs. 5 lit. c nicht notwendig: Dies betrifft zum einen die Erstellung der Zertifikate, zum anderen aber auch die Ermittlung der genesenen Personen, da die Offenlegung der Daten in § 4d in Verbindung mit § 4f EpiG ausdrücklich geregelt ist. Auf das Register der anzeigepflichtigen Krankheiten gem. § 4 EpiG als Datenquelle der Genesungszertifikate wird in § 4d Abs. 2 EpiG explizit verwiesen, weshalb der Prozess der Datenerhebung- und Übermittlung für die betroffene Person nachvollziehbar ist.

Auskunftsrecht der betroffenen Person und Recht auf Datenübertragbarkeit (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 15 und 20 DSGVO):

Gemäß ErwG 63 zur DSGVO sollte der Verantwortliche nach Möglichkeit einen Fernzugang zu einem sicheren System bereitstellen, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglicht. Ein solcher Fernzugang ist vorliegend gegeben, sodass die Betroffenen Ihre Daten jederzeit selbst abfragen können. Voraussetzung für die Abfrage ist das Vorliegen einer Bürgerkarte bzw. Handysignatur.

Als Offline-Pendant steht den Bürgern folgende Möglichkeiten zur Verfügung:

- Druck durch Gemeinden, Bezirksverwaltungsbehörden und die ELGA-Ombudsstelle für alle Zertifikate;
- Druck bei Test- und Impfstellen für Test- und Impfzertifikate;
- Druck durch Ärzte/Ärztinnen und Apotheken (aus dem Impfregister) für Impfzertifikate;
- Versand durch ELGA GmbH für Impfzertifikate.

Die Personen können darüber hinaus von Ihrem Auskunftsrecht durch Kontaktaufnahme mit dem jeweiligen Verantwortlichen Gebrauch machen (siehe zum Beispiel die Pflichtenaufteilung in § 4c Abs. 3 EpiG).

Recht auf Datenübertragbarkeit (Art. 20 DSGVO):

Das Recht auf Datenübertragbarkeit ist aufgrund von Art. 20 Abs. 3 Satz 2 DSGVO ausgeschlossen.

Recht auf Berichtigung und Löschung (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 16, 17 und 19 DSGVO):

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. Das Prozedere wird durch § 4b Abs. 8 EpiG vorgegeben. Demnach sind fehlerhafte Zertifikate zu löschen und ggf. binnen fünf Arbeitstagen neu auszustellen.

Zertifikate, welche keine Fehler enthalten, unterliegen den im EpiG angegebenen Aufbewahrungsfristen. Eine vorzeitige Löschung kommt aufgrund von Art. 17 Abs. 3 lit. b DSGVO nicht in Betracht.

Widerspruchsrecht und Recht auf Einschränkung der Verarbeitung (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 18, 19 und 21 DSGVO):

Das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO findet keine Anwendung. Die Daten sind entweder als richtige Daten gemäß den gesetzlichen Vorschriften im EpiG aufzubewahren und nach Ende der Frist zu löschen oder direkt zu löschen, falls die Daten unrichtig sind.

Das Widerrufsrecht gemäß Art. 21 DSGVO steht nur in den Fällen zu, in denen sich die Datenverarbeitung auf Art. 6 Abs. 1 lit. e oder lit. f DSGVO stützt.

Die Einrichtung und der Betrieb des EPI-Service stützt sich auf Art. 9 Abs. 2 iVm Art. 6 Abs. 1 lit. e DSGVO, weshalb das Widerrufsrecht gegenüber den für das Gesundheitswesen zuständigen Bundesminister geltend zu machen ist.

Die „Zulieferung" der Daten an das EPI-Service erfolgt vorrangig aufgrund des Art. 9 Abs. 2 iVm Art. 6 Abs. 1 lit. c DSGVO, weshalb dort das Widerspruchsrecht nicht zur Anwendung gelangt.

Verhältnis zu Auftragsverarbeitern (Art. 28 DSGVO):

Auftragsverarbeiter: Durch den für Gesundheit zuständigen Bundesminister festzulegen.

Schutzmaßnahmen bei der Übermittlung in Drittländer (Kapitel V DSGVO):

Auf Grundlage der österreichischen (nationalen) Lösung findet keine Übermittlung in Drittstaaten statt. Eine solche Übermittlung kann jedoch in einzelne Drittstatten für die interoperablen Zertifikate auf Grundlage eines Durchführungsrechtsakts der europäischen Kommission erfolgen.

Vorherige Konsultation (Art. 36 und ErwG 96 DSGVO):

Eine vorherige Konsultation gemäß Art. 36 Abs. 1 DSGVO hat nicht stattgefunden, war aber auch nicht erforderlich.

RISIKEN

Physische, materielle oder immaterielle Schäden (ErwG 90 iVm 85 DSGVO):

Im Falle eines Data Breaches würden Daten zu aktuellen und überstandenen COVID-19-Infektionen und Daten zu Impfungen gegen COVID-19 einem größeren Personenkreis bekannt werden.

Da mit einer Infektion eine gewisse Stigmatisierung verbunden ist, besteht die Gefahr, dass Infizierte – auch nach überstandener Infektion – gemieden werden und dies zu psychischen Beeinträchtigungen führt. Besonders für jene Betroffene von „Long-COVID" kann aufgrund der zu erwartenden Symptome wie Konzentrationsschwächen und reduzierte körperliche Belastbarkeit und der damit einhergehenden Stigmatisierung das Fortkommen auf dem Arbeitsmarkt erschwert sein (siehe im Detail unter dem Punkt „Diskriminierung").

Nach dem Schema der CNIL wäre die Schwere damit maximal als „Eingeschränkt" zu betrachten.

Aufgrund der getroffenen Abhilfemaßnahmen lassen sich die Risiken mitigieren.

Verlust der Kontrolle über personenbezogene Daten (ErwG 90 iVm 85 DSGVO):

Es besteht die Gefahr, dass Gesundheitsdaten in die Hände Unberechtigter geraten.

Würde der Data Breach auf der Datenbankebene des EPI-Service geschehen, wo die eingemeldeten Daten einlangen, bevor der QR-Code erstellt wird, könnte eine Rückführung auf die Betroffenen erfolgen.

Nach dem Schema der CNIL wäre diese Schwere als „Eingeschränkt" zu betrachten.

Aufgrund der getroffenen Abhilfemaßnahmen lassen sich die Risiken mitigieren.

Diskriminierung (ErwG 90 iVm 85 DSGVO):

Es besteht die Gefahr, dass Gesundheitsdaten in die Hände Unberechtigter geraten.

Es ist möglich, dass Personen, über die eine frühere Infektion bekannt wird, gemieden werden.

Es ist darüber hinaus denkbar, dass Personen diskriminiert werden, über die bekannt wird, dass sie sich aufgrund ihres Berufs hätten impfen lassen können, aber darauf verzichtet haben.

Gemeinhin sollte eine Information über eine vollständige Genesung oder eine Impfung keinerlei Diskriminierung zur Folge haben, aber es muss mitbedacht werden, dass es in breiten Teilen der Bevölkerung verschiedene Theorien zu einem gewissen Impfskeptizismus geführt haben. Es ist denkbar, dass auch geimpfte Personen von Impfskeptikern wegen ihrer Impfung diskriminiert werden.

Es ist denkbar, dass Genesenen eine nicht vollständige Genesung unterstellt wird. Dieser Zustand – allgemein als „Long Covid" bezeichnet – beschreibt verschiedene, heterogen ausgeprägte Langzeitfolgen. Ob die damit einhergehenden Beeinträchtigungen tatsächlich bei allen oder einigen irreversibel sind oder nur für einen längeren Zeitraum andauern, kann noch nicht mit Sicherheit gesagt werden. Der Verdacht eines schwerwiegenden Falls von „Long Covid" kann dazu führen, dass einem Genesenen Erschöpfung und Konzentrationsschwächen unterstellt werden, und dass ihm keine oder nur eine eingeschränkte Erwerbstätigkeit möglich sei, was zu einer krankheitsbedingten Diskriminierung führen könnte.

Weiters sind auch Auswirkungen auf das Privat- und Familienleben denkbar. Dadurch, dass Geimpfte oder auch Genesene privaten und familiären Aktivitäten relativ uneingeschränkt nachgehen können, ergibt sich im Alltag eine vorübergehende Ungleichbehandlung gegenüber Nicht-Geimpften. Solange keine ausreichenden Impfmöglichkeiten aufgrund von Impfstoffknappheit zur Verfügung stehen bzw bestimmte Altersgruppen ohne Vorerkrankung keinen Zugang zu Impfstoffen haben, kann die Ausübung von privaten und familiären Aktivitäten für diese Bevölkerungsgruppen erschwert sein.

Darüber hinaus ist es denkbar, dass Personen diskriminiert werden, die sich im Ausland wie (zB in den Vereinigten Arabischen Emiraten oder Serbien) impfen ließen.

Nach dem Schema der CNIL wäre diese Schwere als „Wesentlich" zu betrachten.

Aufgrund der getroffenen Abhilfemaßnahmen lassen sich die Risiken mitigieren.

Identitätsdiebstahl oder -betrug (ErwG 90 iVm 85 DSGVO):

Theoretisch wäre es auch denkbar, dass sich unbefugte Zugriff auf die Datenbank verschaffen. Dies wäre schwerwiegend, weil dann Zugriff auf einen großen Datensatz personenbezogener Daten von einem kaum eingrenzbaren Personenkreis besteht. Die Daten könnten missbraucht werden und Identitätsdiebstahl und/oder -betrug wäre dann wahrscheinlich anzunehmen. Insbesondere könnten nicht gegen COVID-19 geimpfte Personen ggf auch die Identität einer geimpften oder genesenen Person annehmen.

Nach dem Schema der CNIL wäre die Schwere als „Eingeschränkt" zu betrachten. Aufgrund der großen Datenmenge ist diesem Punkt aber erhöhte Priorität im Rahmen der Abhilfemaßnahmen einzuräumen. Aufgrund der getroffenen Abhilfemaßnahmen lassen sich die Risiken mitigieren.

Finanzielle Verluste (ErwG 90 iVm 85 DSGVO):

Finanzielle Verluste können sich als Folge des oben geschilderten Szenarios zum Identitätsdiebstahl ergeben (siehe dort). Auch im Rahmen von Diskriminierung kann es zu finanziellen Verlusten kommen, etwa, wenn Ängste anderer selbst nach überstandener Infektion die Erwerbstätigkeit (insbesondere bei Selbstständigen und Arbeitssuchenden) einschränkt, oder ein (potentieller) Arbeitgeber Impfungen so stark ablehnt, dass dies finanzielle Folgen hat.

Nicht gegen COVID-19 geimpfte Personen, die sich hätten impfen lassen können, könnten ebenfalls beruflichen Nachteilen ausgesetzt sein, indem sie etwa eine Arbeit nicht bekommen, ihnen die Arbeit im Team verweigert wird oder Geschäftspartner die Zusammenarbeit ablehnen.

Schließlich kann es zu beruflichen Nachteilen und damit verbunden finanziellen Verlusten im Zusammenhang mit einer Genesung kommen, wenn dem Genesenen „Long Covid"-Symptome, also vor allem Erschöpfung und Konzentrationsschwäche und damit einhergehend eine geringere berufliche Leistungsfähigkeit unterstellt werden.

Unbefugte Aufhebung der Pseudonymisierung (ErwG 90 iVm 85 DSGVO):

Eine unbefugte Person müsste mit Zusatzwissen die Daten aus dem EPI-Service-QR-Code auf die Person zurückführen. Würde ihr dies gelingen, hätte die unbefugte Person Zugriff auf Testergebnisse bzw. Nachweise zur Immunität mit den gleichen Folgen wie oben geschildert. Die Gefahr ist als gering einzustufen.

Rufschädigung (ErwG 90 iVm 85 DSGVO):

Der Ruf scheint durch eine COVID-19-Infektion grundsätzlich nicht berührt. Eine COVID-19-Infektion ist an sich keine negativ konnotierte Erkrankung wie beispielsweise eine sexuell übertragbare Krankheit, Adipositas oder Alkoholismus.

Eine Rufschädigung im Falle einer Genesung, weil dem Betroffenen „Long Covid" unterstellt wird, ist allerdings nicht ausgeschlossen, da in manchen Teilen der Bevölkerung das Ansehen, die Wertschätzung und die Achtung einer Person eng mit der beruflichen Leistungsfähigkeit verbunden ist, und daher die Behauptung, jemand habe „Long Covid", eine diffamierende Wirkung haben kann.

Auch eine Impfung gegen COVID-19 oder umgekehrt das Nichtimpfen trotz der Möglichkeit dazu hat kein Potential zur Rufschädigung.

Verlust der Vertraulichkeit bei Berufsgeheimnissen (ErwG 90 iVm 85 DSGVO):

Die im Rahmen der Testung oder Impfung beteiligten Personen unterliegen Berufsgeheimnissen (beispielsweise § 54 Abs. 1 ÄrzteG 1998) und/oder gesetzlichen Verschwiegenheitsverpflichtungen. Würden Daten aus der Testung oder Impfung Unbefugten bekannt, wäre dies nicht nur ein datenschutzrechtlicher Verstoß, sondern auch eine Verletzung von Berufsgeheimnissen oder ein Bruch von Amtsgeheimnissen.

Nach dem Schema der CNIL wäre die Schwere als „Eingeschränkt" zu betrachten. Aufgrund der getroffenen Abhilfemaßnahmen lassen sich die Risiken mitigieren.

Erhebliche wirtschaftliche oder gesellschaftliche Nachteile (ErwG 90 iVm 85 DSGVO):

Hier kann nach oben zum Punkt „Diskriminierung" und „Finanzielle Verluste" verwiesen werden. Aufgrund der getroffenen Abhilfemaßnahmen lassen sich die Risiken mitigieren.

ABHILFEMASSNAHMEN

Minimierung der Verarbeitung personenbezogener Daten (ErwG 78 DSGVO):

Bei der Überprüfung der Zertifikate kommt es zu keiner Speicherung beim Überprüfenden. Die personenbezogenen Daten werden somit bei keiner weiteren Stelle dauerhaft gespeichert.

Zudem findet die Kontrolle der Zuordnung des Zertifikats zu einer natürlichen Person „offline" durch eine Kontrolle des amtlichen Lichtbild(ausweise)s statt.

Die Verarbeitung personenbezogener Daten findet zudem nur in den gesetzlich vorgesehenen Fällen statt.

Einsatz bereichsspezifischer Personenkennzeichen (§ 9 E-GovG), die nur in Teilbereichen des täglichen Lebens gelten und somit einen wesentlich höheren Schutz, insbesondere gegen erhebliche wirtschaftliche oder gesellschaftliche Nachteile, bieten.

Datensicherheitsmaßnahmen (ErwG 78 und 83 DSGVO):

Die Datensicherheitsmaßnahmen werden zum Teil bereits durch die anwendbaren gesetzlichen Vorschriften vorgegeben:

Gemäß § 4c Abs. 3 EpiG jedenfalls einzuhalten ist von den übermittelnden Einrichtungen § 6 GTelG 2012, der die Vertraulichkeit bei der Übermittlung von Gesundheitsdaten regelt. Außerdem sind von den übermittelnden Einrichtungen gemäß § 4c Abs. 3 EpiG die in § 4 Abs. 12 bis 14 EpiG vorgesehenen Datensicherheitsmaßnahmen zu ergreifen. Auch die ELGA GmbH hat bei der Übermittlung der Daten aus dem zentralen Impfregister § 6 GTelG 2012 einzuhalten. Auch § 4 EpiG, der das Register anzeigepflichtiger Krankheiten regelt, aus dem die Daten für die Genesungszertifikate zu ermitteln sind, sieht diverse Datensicherheitsmaßnahmen vor (vgl. § 4 Abs. 9 bis 11 EpiG).

In Anbetracht der vorgehend umrissenen gesetzlichen Anforderungen werden nachfolgend die grundsätzlichen technischen und organisatorischen Maßnahmen für das EPI-Service beschrieben. Die technischen Details werden in einem verbindlichen Sicherheitskonzept (SIKO) dokumentiert.

I. Pseudonymisierung und Verschlüsselung:

Pseudonymisierung ist im EPI-Service nicht möglich, da auch die Klartexte (Vorname, Nachname, Geburtsdatum) jedenfalls in den Daten enthalten sein müssen.

Einmeldung von Daten in das EPI-Service: Die Anbindung an das EPI-Service erfolgt nur nach schriftlicher Freigabe durch das BMSGPK. Im Zuge der Anbindung wird durch den angebundenen Partner mittels CSR ein Client-Zertifikat beantragt, welches aus einer internen CA ausgestellt wird. Der Schlüssel zum Zugriff liegt also nur dem jeweils angebunden Betreiber vor. Das EPI-Service ist nicht öffentlich. Jeglicher Zugriff durch eintragende Stellen auf das Service ist nur mit einem gültigen Clientzertifikat möglich.

Abfrage von Daten aus dem EPI-Service: Auch die Zugriffe abfragender Stellen setzen eine, dem Stand der Technik entsprechende Verschlüsselung ein. Die Abfrage kann entweder durch den Betroffenen selbst mittels Handysignatur erfolgen oder durch Behörden (Gemeinden, Bezirksverwaltungsbehörden und der ELGA-Ombudsstelle) mittels Portalverbund (hier erfolgt auch eine Protokollierung der Zugriffe). Arztinnen/Ärzte und Apotheken haben Zugang über das zentrale Impfregister, wobei die Authentifizierung gemäß GTELG 2021 erfolgt und alle Aktivitäten protokolliert werden.

Die eingesetzten Verfahren müssen dem Stand der Technik entsprechen. Datenübertragung und Kommunikationsschnittstellen kommunizieren in verschlüsselter Form.

II. Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

a) Zugangskontrolle

- Alle Gebäude sind durch physische Sicherheitsmaßnahmen geschützt, um den unberechtigten Zutritt zu verhindern.
- Für sämtliche Gebäude kommt ein Zonenkonzept mit einer adäquaten Sicherung der Zonen und der Übergänge zum Einsatz.
- Türzutrittsprotokolle werden nachvollziehbar dokumentiert gespeichert.
- Der Zutritt zu Serverstandorten wird mittels elektronischen Zugangskontrollen verwaltet.
- Alle Besucher müssen sich ausweisen und registrieren und werden stets von berechtigten Mitarbeitern begleitet.
- Der Zutritt zu sensiblen Bereichen wird zusätzlich durch Videoüberwachung überwacht.
- Alle Mitarbeiter werden in regelmäßigen Abständen nachweislich in Bezug auf Sicherheit geschult.
- Es erfolgt eine Sicherung strategisch wichtiger Objekte mittels Überwachungseinrichtungen (Alarmanlage, Videoüberwachung) oder Wachschutz

b) Datenträgerkontrolle

- Die Bereiche und Räumlichkeiten, in denen Datensicherungen durchgeführt und Datenträger aufbewahrt werden, sind entsprechend gesichert.
- Der Zugriff auf Datensicherungen erfolgt ausschließlich durch autorisiertes Personal.
- Die Speicherung von Daten auf mobilen Datenträgern erfolgt zwingend verschlüsselt.
- Nicht mehr benötigte Datenträger werden nachweislich entsorgt; datenschutzgerechte Entsorgung bzw. Vernichtung.

c) Benutzerkontrolle

- Die Aktivierung von Benutzerkonten erfolgt von zentraler Stelle.
- Es gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine übertragenen Aufgaben durchführen zu können.
- Die Beantragung von Rechten und die weiterführende Beauftragung zur Vergabe von Benutzerrechten erfolgt Workflow gesteuert.
- Benutzerkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet.
- Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus muss eine nachvollziehbare Genehmigung und Freigabe erfolgen.
- Benutzer- und Administratorzugriffe beruhen auf einem rollenbasierten Zugriffsberechtigungsmodell. Jeder Nutzer erhält eine eindeutige ID um sicherstellen zu können, dass alle Systemkomponenten nur von berechtigten Benutzern und Administratoren genutzt werden können.
- Bestehende Zugriffsrechte auf IT-Systeme werden unmittelbar nach Deaktivierung des jeweiligen Mitarbeiterdatensatzes zentral gesteuert entzogen.
- Für zeitlich begrenzte Zugriffe werden nach Ablauf entsprechende Berechtigungslöschverfahren eingeleitet.
- Das Erstellen, Löschen und Ändern von Benutzer-IDs, Anmeldeinformationen und anderen Identifizierungsmerkmalen wird mit einem Zeitstempel protokolliert.

d) Zugriffskontrolle

- Passwörter für die Erstanmeldung bestehen aus einem zufällig generierten Wert und sind nach der ersten Verwendung zwingend zu ändern.
- Benutzerpasswörter werden periodisch geändert. Es sind nur komplexe Passwörter zulässig.
- Auf mobilen Arbeitsplätzen (z. B. Notebooks) ist eine Firewall und Antivirus-Software installiert.
- Für externe Zugriffe auf interne Systeme ist eine Multifaktorauthentifizierung implementiert.
- Sensible Netzwerkbereiche sind voneinander getrennt.
- Wesentliche Aktivitäten der Benutzer werden protokolliert, Möglichkeiten zur Auswertung wurden zwischen Arbeitgeber- und Arbeitnehmervertretung vereinbart.
- Die erteilten Zugriffsrechte werden mindestens jährlich von zuständigen Mitarbeitern auf Angemessenheit und Aktualität überprüft. Zugriffsberechtigungen werden sofort aufgehoben, wenn die entsprechenden Zugriffsrechte für die Tätigkeiten des Benutzers nicht mehr erforderlich sind.

- Test- und Produktionssystem sind voneinander getrennt. Für Testsysteme gelten die gleichen Datensicherungsmaßnahmen wie für Produktivsysteme, sofern personenbezogene Daten verwendet werden.
- Bildschirmarbeitsplätze werden automatisch nach wenigen Minuten Inaktivität gesperrt.

e) Übertragungskontrolle

- Alle Mitarbeiter werden zum Datenschutz verpflichtet und periodisch geschult. Hierbei ist ein zweijähriges Schulungsintervall mit Prüfung vorgesehen.
- Die der Datenklassifizierung angepassten Übermittlungswege und die generellen Handhabungsvorschriften wurde allen Mitarbeitern zur Kenntnis gebracht.
- Die Einhaltung kryptografischer Vorgaben sichert die Einhaltung der Vertraulichkeit verschlüsselter Informationen.

f) Eingabekontrolle

- Wesentliche Aktivitäten der Benutzer werden protokolliert.
- Alle Mitarbeiter beim Auftragsverarbeiter werden zum Datenschutz verpflichtet und periodisch geschult.

g) Datenintegrität

- Die Rechenzentren des Auftragsverarbeiters haben Einrichtungen zur automatischen Branderkennung und -bekämpfung installiert.
- Die für den Betrieb wesentliche IT-Infrastruktur der Rechenzentren des Auftragsverarbeiters wurde so entwickelt, dass sie vollständig redundant sind und ohne Beeinträchtigung des Betriebs gewartet werden können.
- Unterbrechungsfreie Stromversorgungen gewährleisten im Fall eines Stromausfalls, dass entsprechend der Verfügbarkeitsanforderung Bereiche der Rechenzentren weiterhin mit Strom versorgt und somit Datenverluste oder Datenbeschädigungen verhindert werden.
- Die Rechenzentren verfügen darüber hinaus über Generatoren, welche für den Notbetrieb erforderlichen Teile der Anlage mit Notstrom versorgen können.
- Mitarbeiter und entsprechende Systeme steuern die atmosphärischen Bedingungen innerhalb der Rechenzentren.
- Es werden vorbeugende Wartungsmaßnahmen durchgeführt, um den fortlaufenden Betrieb der Anlagen zu gewährleisten.
- Updates und Patches für Betriebssysteme und sonstige Programme werden nach eingehender Analyse eingespielt.
- Für Security-Patches und gemeldete Schwachstellen gibt es geordnete Verfahren.
- Der eingehende Datenverkehr wird auf Schadcode geprüft.
- Alle Arbeitsplätze sind mit einem zentral gewarteten Virenschutz geschützt.
- Wesentliche IT-Ressourcen sind ausfallsicher über mehrere Rechenzentren und Standorte verteilt.

<u>III. Wiederherstellung, der Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall</u>

- Ein Security Incident Management Prozess ist etabliert und getestet, die Verantwortlichkeiten und Rollen sind definiert.
- Wiederherstellungsprozeduren werden laufend angepasst und periodisch getestet.
- Einheitliche Wiederherstellungskonzepte gewährleisten die zeitnahe Wiederherstellung von Daten.
- Redundant ausgelegte Systeme verringern die Auswirkungen von Betriebsstörungen.
- Es gibt einen Notfall- und Wiederherstellungsplan für das EPI-Service.
- Für Notfälle und Krisen wurde eine Krisenorganisation etabliert. Die dafür notwendigen Rollen wurden besetzt, periodische Krisenübungen werden durchgeführt.
- Für Notfälle- und Krisen beim Auftragsverarbeiter wurde eine Krisenorganisation etabliert. Die dafür notwendigen Rollen wurden besetzt, periodische Krisenübungen werden durchgeführt.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Organisationskontrolle)

- Ein Datenschutzbeauftragter wurde bestellt.
- Formalisierte Freigabeverfahren für neue Datenverarbeitungsverfahren und bei wesentlichen Änderungen wurden etabliert.
- Es liegen Richtlinien für Softwareentwicklungen vor.
- Die Überprüfung der Einhaltung von Entwicklungs- und Sicherheitsvorgaben durch wiederkehrende Penetrationstests wurde vereinbart.
- Alle Mitarbeiter des Auftragsverarbeiters werden jährlich in Bezug auf Informationssicherheit und Datensicherheit geschult.
- Es sind Key Risk und Key-Performance Indikatoren zur periodischen Überprüfung der Wirksamkeit von Einrichtungen und Maßnahmen implementiert.
- Ein internes Kontrollsystem wurde beim Auftragsverarbeiter etabliert. Dies kann auch durch das Vorliegen von Zertifizierungen nachgewiesen werden.

Weitere Abhilfemaßnahmen:

Die Ungleichbehandlung von Geimpften und Genesenen auf der einen Seite und Ungeimpften auf der anderen Seite wird durch ein flächendeckendes, kostenloses Testangebot in Teststraßen in den Bundesländern, Apotheken und Betrieben mitigiert. Dadurch, dass ein Testnachweis den Getesteten vorübergehend die gleichen Möglichkeiten wie Geimpften und Genesenen einräumt, lässt sich für diese der Zeitraum, in dem Impfungen noch nicht flächendeckend zur Verfügung stehen, überbrücken. Die Testzertifikate sind also auch eine Möglichkeit um Ungleichheit (z. B. für jüngere Personen, Schwangere, Kinder und Jugendliche unter 16 Jahren) auf ein Minimum zu reduzieren.

BERÜCKSICHTIGUNG VON DATENSCHUTZINTERESSEN

Die Einholung des Rates der Datenschutzbeauftragten (Art. 35 Abs. 2 DSGVO) des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz zu dieser Datenschutz-Folgenabschätzung erfolgte bei deren Durchführung. Die Datenschutzbehörde wurde gemäß Art. 36 Abs. 4 DSGVO konsultiert. Darüber hinaus wurde ein Begutachtungsverfahren durchgeführt, und es fand ein intensiver Austausch mit der Datenschutz-Community statt.

ERGEBNIS

Methodik:

Die nachfolgende Risikomatrix hilft, Risiken im Verhältnis von Auswirkungen und Eintrittswahrscheinlichkeit einzuordnen und als geringe Risiken, mittlere Risiken oder hohe Risiken einzustufen.

Ergebnis der Einstufung ist, dass das Risiko der Verarbeitung als niedrig, mittel oder hoch eingeschätzt wird, wobei sich die Einstufung der gesamten Verarbeitung am höchsten ermittelten Risiko orientiert.

Risikoanalyse im vorliegenden Fall:

Nach Analyse der oben dargelegten Risiken, ergeben sich die folgenden Risiko-Themenkomplexe:

- Immaterielle Schäden, Verletzung von Berufsgeheimnissen, Diskriminierung durch Kenntnisnahme oder sonstige unbefugte Verarbeitung von personenbezogenen Daten durch Dritte (Risiko 1).
- Identitätsdiebstahl (Risiko 2)
- Unbefugte Aufhebung der Pseudonymisierung (Risiko 3).

Bezüglich des Risiko 1 sind die Auswirkungen auf Sicht der Betroffenen nach dem Schema der CNIL als „wesentlich" zu betrachten. Die Auswirkungen bei Risiko 2 wären zwar lediglich als „eingeschränkt" zu sehen, wobei hier aufgrund der großen Datenmenge eine Abweichung vom Schema denkbar ist und das Risiko als „wesentlich bis eingeschränkt" bezeichnet werden kann. Bei Risiko 3 wären die Auswirkungen als „eingeschränkt" einzustufen.

Unter Berücksichtigung der Abhilfemaßnahmen kann in Bezug auf die Risiken 1 und 2 von einer „eingeschränkten Eintrittswahrscheinlichkeit" ausgegangen werden, für die ausgewählte Risikoquelle scheint es schwierig zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen. Schwachstellen ergeben sich noch am ehesten durch menschliche Fehler, die zu Abweichungen im beschriebenen Prozedere führen (Beispiel: Ein Sanitäter folgt das Testergebnis

aus Unachtsamkeit der falschen Person aus.). Es ist aber nicht damit zu rechnen, dass solche Fehler zu massenhaften Data Breaches führen. Bezogen auf Risiko 3 ist sogar davon auszugehen, dass die Eintrittswahrscheinlichkeit in diesem Fall vernachlässigbar ist.

- Immaterielle Schäden, Verletzung von Berufsgeheimnissen, Diskriminierung durch Kenntnisnahme oder sonstige unbefugte Verarbeitung von personenbezogenen Daten durch Dritte (Risiko 1).
- Identitätsdiebstahl (Risiko 2)
- Unbefugte Aufhebung der Pseudonymisierung (Risiko 3).

Auswirkungen aus Sicht der Betroffenen	**Maximal**	**mittel**	**mittel**	**hoch**	**hoch**
	Wesentlich	**mittel**	**mittel**	**mittel**	**hoch**
	Eingeschränkt	**gering**	**mittel**	**mittel**	**mittel**
	Vernachlässigbar	**gering**	**gering**	**mittel**	**mittel**
		Vernachlässigbar	**Eingeschränkt**	**Wesentlich**	**Maximal**
		Eintrittswahrscheinlichkeit			

In der Gesamtbetrachtung ergibt sich damit eine

mittlere Einstufung

des Risikos. Die Maßnahmen sind laufend zu evaluieren und bei Bekanntwerden von Schwachstellen unverzüglich anzupassen.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2021-05-26T17:57:05+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.	