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 Nachweise für
- getestete Personen,
- geimpfte Personen und
- genesene 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“ bzw. „SARS-CoV-2“,
- Art des Tests,
- Art der Probennahme,
- Bezeichnung des Tests und des Herstellers des Tests (optional bei NAAT-Tests),
- Datum und Uhrzeit der Probenahme,
- Datum und Uhrzeit der Erstellung des Testergebnisses (optional bei RAT-Tests),
- 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“ bzw. „SARS-CoV-2“,
Datum des ersten positiven Testergebnisses,
Datum des Serologie- oder Antikörpertests,
Bezeichnung des Staates, in dem der Test durchgeführt wurde,
Bezeichnung des Ausstellers des Genesungszertifikats,
Gültigkeitsbeginn des Genesungszertifikats,
Gültigkeitsende des Genesungszertifikats und
eindeutige Kennung des Genesungsnachweises.

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“ bzw. „SARS-CoV-2“,
Impfstoff/Prophylaxe (generische Beschreibung des Impfstoffs oder seiner Komponenten),
Impfarzneimittel (Bezeichnung des Impfstoffs gemäß Zulassung),
Zulassungsinhaber oder Hersteller des Impfstoffs,
Nummer der Impfung (Erstimpfung/Zweitimpfung/Auffrischungsimpfung),
Datum der Impfung (für jede erhaltene Impfdosis zur Grundimmunisierung sowie der Auffrischungsimpfung),
Bezeichnung des Staates, in dem die Impfung durchgeführt wurde,
Bezeichnung des Ausstellers des Impfzertifikats und
eindeutige Kennung des Impfzertifikats.

Die ELGA GmbH übermittelt die Chargennummer des verabreichten Impfstoffs sowie das bPK-GH aus dem zentralen Impfregister an den für das Gesundheitswesen zuständigen Bundesminister. Dies wird durch technische und 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 ein Abgleich der Daten mit dem EPI-Service sowie eine Offline-Identitätskontrolle durch Vorlage eines Ausweisdokuments (Amtlicher Lichtbildausweis oder e-Card mit Foto). Hierbei findet keine zusätzliche Speicherung statt und es erfolgt nur eine Überprüfung der Richtigkeit.

Eine Überprüfung findet mittels Elektronische Anwendungen zur Verifizierung von Zertifikaten gemäß §§ 4c bis 4e statt.

Hierbei dürfen nur zwei mögliche Ergebnisse angezeigt werden:

„gültig“ (grün hinterlegt), wenn ein zeitlich gültiges Test-, Genesungs- oder ein Impfzertifikat verfügbar ist, oder
„abgelaufen“ (rot hinterlegt), wenn kein oder kein zeitlich gültiges Zertifikat verfügbar ist.

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 1 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 2 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 eines Zertifikats zum Nachweis einer geringeren epidemiologischen Gefahr in Bezug auf SARS-CoV-2 gemäß § 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 Gesundheit zuständigen Minister 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 2 EpiG).

Empfänger sind ferner

- alle in § 4c Abs. 7 Z 1 EpiG genannten öffentlichen Stellen, welche das Zertifikat auf Anforderung des Betroffenen ausstellen,
- Teststellen, die das Testzertifikat auf Anforderung des Betroffenen ausdrucken (§ 4c Abs. 2 EpiG),
- Ärztinnen und Ärzte sowie Apotheken, die das Impfzertifikat auf Anforderung des Betroffenen ausdrucken (§4d Abs. 4 EpiG) und
- die ELGA GmbH, im Falle von Impfzertifikaten nach den Vorgaben von § 4d Abs. 4 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: 3 Tage (§ 4c Abs. 5 EpiG) ab Gültigkeitsende
- Genesungszertifikate: 1 Woche (§ 4d Abs. 5 EpiG) ab Gültigkeitsende
- Impfzertifikate: 1 Jahr (§ 4e Abs. 5 EpiG) ab Übermittlung Impfregister

Gemäß § 4 Abs. 9 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. 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. c 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. c 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):

Die betroffenen Personen erhalten die Möglichkeit ihre Zertifikate abzurufen bzw. ausdrucken zu lassen.

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.

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.

<u>RISIKEN</u>

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 „Eingeschränkt“ 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 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 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 Lichtbildausweises oder der e-Card mit Foto 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 ergeben sich teilweise bereits aus bestehenden Vorschriften, die explizit für anwendbar erklärt werden:

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).

Nachfolgend werden die 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.

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 jeweilig angebunden

Betreiber vor. Das EPI-Service ist nicht öffentlich. Jeglicher Zugriff auf das Service ist nur mit einem gültigen Clientzertifikat möglich.

Die eingesetzten Verfahren müssen dem Stand der Technik entsprechen.

Auch alle anderen Zugriffe) setzen eine, dem Stand der Technik entsprechende, Verschlüsselung ein.

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.

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

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 laufende 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 (zB für jüngere Personen, Schwangere, Kinder unter 16) 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.

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 „eingeschränkt“ zu betrachten. Gleiches gilt für Risiko 2, 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 wir bei Risiko 1 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
		Vernach-lässigbar	Einge-schränkt	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.