DURCHFÜHRUNGSBESCHLUSS (EU) 2022/483 DER KOMMISSION

vom 21. März 2022

zur Änderung des Durchführungsbeschlusses (EU) 2021/1073 zur Festlegung technischer Spezifikationen und Vorschriften für die Umsetzung des mit der Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates geschaffenen Vertrauensrahmens für das digitale COVID-Zertifikat der EU

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates vom 14. Juni 2021 über einen Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von COVID-19-Impfungen und -Tests sowie der Genesung von einer COVID-19-Infektion (digitales COVID-Zertifikat der EU) mit der Zielsetzung der Erleichterung der Freizügigkeit während der COVID-19-Pandemie ([1]), insbesondere auf Artikel 9 Absatz 1,

in Erwägung nachstehender Gründe:

(1) Gegenstand der Verordnung (EU) 2021/953 ist das digitale COVID-Zertifikat der EU, mit dem nachgewiesen wird, dass eine Person eine COVID-19-Impfung oder ein negatives Testergebnis erhalten hat oder von einer Infektion genesen ist; hierdurch soll für den Inhaber des Zertifikats die Ausübung des Rechts auf Freizügigkeit während der COVID-19-Pandemie erleichtert werden.

(2) Gemäß der Verordnung (EU) 2021/954 des Europäischen Parlaments und des Rates ([2]) müssen die Mitgliedstaaten die Vorschriften der Verordnung (EU) 2021/953 auf diejenigen Drittstaatsangehörigen anwenden, die nicht in den Anwendungsbereich dieser Verordnung fallen, sich jedoch in ihrem Hoheitsgebiet rechtmäßig aufhalten oder ihren Wohnsitz haben und gemäß Unionsrecht zu Reisen in andere Mitgliedstaaten berechtigt sind.

(3) Gemäß der Empfehlung (EU) 2022/290 des Rates zur Änderung der Empfehlung (EU) 2020/912 zur vorübergehenden Beschränkung nicht unbedingt notwendiger Reisen in die EU und möglichen Aufhebung dieser Beschränkung ([3]) sollten Drittstaatsangehörige, die nicht unbedingt notwendige Reisen aus einem Drittland in die Union unternehmen wollen, im Besitz eines gültigen Impf- oder Genesungsnachweises sein, beispielsweise eines digitalen COVID-Zertifikats der EU oder eines von einem Drittland ausgestellten COVID-19-Zertifikats, für das ein Durchführungsrechtsakt gemäß Artikel 8 Absatz 2 der Verordnung (EU) 2021/953 gilt.

(4) Damit das digitale COVID-Zertifikat der EU in der gesamten Union verwendet werden kann, hat die Kommission den Durchführungsbeschluss (EU) 2021/1073 ([4]) erlassen, in dem technische Spezifikationen und Vorschriften festgelegt sind, um die digitalen COVID-Zertifikate der EU zu füllen, auf sichere Weise auszustellen und zu überprüfen, den Schutz personenbezogener Daten zu gewährleisten, die gemeinsame Struktur der eindeutigen Zertifikatkennung sicherzustellen und einen gültigen, sicheren und interoperablen Strichcode zu erstellen.

(5) Gemäß Artikel 4 der Verordnung (EU) 2021/953 mussten die Kommission und die Mitgliedstaaten einen Vertrauensrahmen für das digitale COVID-Zertifikat der EU errichten und pflegen. Dieser Vertrauensrahmen kann auch den bilateralen Austausch von Zertifikatswiderrufslisten mit den eindeutigen Zertifikatkennungen widerrufener Zertifikate unterstützen.

([1]) ABl. L 211 vom 15.6.2021, S. 1.

([2]) Verordnung (EU) 2021/954 des Europäischen Parlaments und des Rates vom 14. Juni 2021 über einen Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von COVID-19-Impfungen und -Tests sowie der Genesung von einer COVID-19-Infektion (digitales COVID-Zertifikat der EU) für Drittstaatsangehörige mit rechtmäßigem Aufenthalt oder Wohnsitz im Hoheitsgebiet der Mitgliedstaaten während der COVID-19-Pandemie (ABl. L 211 vom 15.6.2021, S. 24).

([3]) Empfehlung (EU) 2022/290 des Rates vom 22. Februar 2022 zur Änderung der Empfehlung (EU) 2020/912 des Rates zur vorübergehenden Beschränkung nicht unbedingt notwendiger Reisen in die EU und möglichen Aufhebung dieser Beschränkung (ABl. L 43 vom 24.2.2022, S. 79).

([4]) Durchführungsbeschluss (EU) 2021/1073 der Kommission vom 28. Juni 2021 zur Festlegung technischer Spezifikationen und Vorschriften für die Umsetzung des mit der Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates geschaffenen Vertrauensrahmens für das digitale COVID-Zertifikat der EU (ABl. L 230 vom 30.6.2021, S. 32).

(6) Am 1. Juli 2021 wurde das Gateway für das digitale COVID-Zertifikat der EU (im Folgenden das „Gateway“) in Betrieb genommen, das der Kernbestandteil des Vertrauensrahmens ist und über das öffentliche Schlüssel zur Überprüfung der digitalen COVID-Zertifikate der EU auf sichere und vertrauenswürdige Weise zwischen den Mitgliedstaaten ausgetauscht werden können.

(7) Aufgrund ihrer erfolgreichen und breit angelegten Einführung sind die digitalen COVID-Zertifikate der EU in das Interesse von Betrügern gerückt, die nach Möglichkeiten suchen, Zertifikate auf betrügerische Weise auszustellen. Solche betrügerisch ausgestellten Zertifikate müssen daher widerrufen werden. Darüber hinaus können die Mitgliedstaaten bestimmte digitale COVID-Zertifikate der EU auf nationaler Ebene aus medizinischen Gründen und aus Gründen der öffentlichen Gesundheit widerrufen, beispielsweise weil sich eine Impfstoffcharge nachträglich als fehlerhaft herausstellt.

(8) Das System der digitalen COVID-Zertifikate der EU erkennt gefälschte Zertifikate sofort, doch echte Zertifikate, die unrechtmäßig auf der Grundlage falscher Dokumente, durch unbefugten Zugriff oder mit betrügerischer Absicht ausgestellt wurden, können in anderen Mitgliedstaaten nur erkannt werden, wenn die auf nationaler Ebene erstellten Listen widerrufener Zertifikate zwischen den Mitgliedstaaten ausgetauscht werden. Gleiches gilt für Zertifikate, die aus medizinischen Gründen und aus Gründen der öffentlichen Gesundheit widerrufen wurden. Wenn die Anwendungen der Mitgliedstaaten zur Überprüfung der Zertifikate die von anderen Mitgliedstaaten widerrufenen Zertifikate nicht erkennen, stellt dies eine Gefahr für die öffentliche Gesundheit dar und untergräbt das Vertrauen der Bürger in das System der digitalen COVID-Zertifikate der EU.

(9) Wie in Erwägungsgrund 19 der Verordnung (EU) 2021/953 dargelegt, sollten die Mitgliedstaaten aus medizinischen Gründen und aus Gründen der öffentlichen Gesundheit und im Falle betrügerisch ausgestellter oder erlangter Zertifikate für die Zwecke dieser Verordnung Zertifikatswiderrufslisten erstellen und mit anderen Mitgliedstaaten austauschen können, insbesondere um Zertifikate zu widerrufen, die irrtümlich, in betrügerischer Absicht oder nach der Aussetzung einer COVID-19-Impfstoffcharge, die sich als fehlerhaft herausgestellt hat, ausgestellt wurden. Den Mitgliedstaaten sollte es nicht möglich sein, von anderen Mitgliedstaaten ausgestellte Zertifikate zu widerrufen. Ausgetauschte Zertifikatswiderrufslisten sollten keine anderen personenbezogenen Daten enthalten, als die eindeutigen Zertifikatkennungen. Insbesondere sollte nicht angegeben werden, warum ein Zertifikat widerrufen wurde.

(10) Zusätzlich zu der allgemeinen Information darüber, dass und aus welchen Gründen Zertifikate widerrufen werden können, sollten Inhaber widerrufener Zertifikate von der für die Ausstellung zuständigen Behörde unverzüglich über den Widerruf ihrer Zertifikate und die Gründe für den Widerruf informiert werden. Allerdings kann es sich in manchen Fällen, insbesondere bei digitalen COVID-Zertifikaten der EU, die in Papierform ausgestellt werden, als unmöglich erweisen oder mit einem unverhältnismäßigen Aufwand verbunden sein, den Inhaber ausfindig zu machen und über den Widerruf zu informieren. Die Mitgliedstaaten sollten keine zusätzlichen personenbezogenen Daten erheben, die zur Ausstellung nicht benötigt werden, nur um Zertifikatinhaber informieren zu können, wenn ihre Zertifikate widerrufen werden.

(11) Daher muss der Vertrauensrahmen für das digitale COVID-Zertifikate der EU verbessert werden, indem der bilaterale Austausch von Zertifikatswiderrufslisten zwischen den Mitgliedstaaten unterstützt wird.

(12) Dieser Beschluss gilt nicht für die vorübergehende Aussetzung von Zertifikaten für nationale Anwendungsfälle, die nicht in den Anwendungsbereich der Verordnung über das digitale COVID-Zertifikat der EU fallen, beispielsweise weil der Inhaber eines Impfzertifikats positiv auf SARS-CoV-2 getestet wurde. Der Beschluss lässt die festgelegten Verfahren zur Überprüfung der Verfahrensvorschriften für die Gültigkeit von Zertifikaten unberührt.

(13) Während aus technischer Sicht unterschiedliche Architekturen für den Austausch von Widerrufslisten möglich sind, eignet sich das Gateway am besten für diesen Austausch, da hierdurch der Datenaustausch auf den bereits bestehenden Vertrauensrahmen beschränkt bleibt und im Vergleich zu einem alternativen Peer-to-Peer-System sowohl die möglichen Schwachstellen als auch die Anzahl der Übermittlungsvorgänge zwischen Mitgliedstaaten minimiert werden.

(14) Dementsprechend sollte das Gateway für das digitale COVID-Zertifikat der EU ausgeweitet werden, um den sicheren Austausch von Informationen über widerrufene digitale COVID-Zertifikate der EU für die Zwecke ihrer sicheren Überprüfung über das Gateway zu unterstützen. In diesem Zusammenhang sollten geeignete Sicherheitsmaßnahmen zum Schutz der im Gateway verarbeiteten personenbezogenen Daten ergriffen werden. Um ein hohes Schutzniveau zu gewährleisten, sollten die Mitgliedstaaten Zertifikatsattribute durch einen unumkehrbaren Hashwert in den Widerrufslisten pseudonymisieren. Die eindeutigen Kennungen sollten für die Zwecke der Verarbeitung im Rahmen des Gateways als pseudonymisierte Daten gelten.

(15) Darüber hinaus sollten Bestimmungen über die Rolle der Mitgliedstaaten und der Kommission beim Austausch von Zertifikatswiderrufslisten festgelegt werden.

(16) Die Verarbeitung personenbezogener Daten von Zertifikatinhabern, die unter der Verantwortung der Mitgliedstaaten oder anderer öffentlicher Organisationen oder amtlicher Stellen in den Mitgliedstaaten erfolgt, sollte mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([5]) im Einklang stehen. Die Verarbeitung personenbezogener Daten unter der Verantwortung der Kommission zum Zweck der Verwaltung und der Gewährleistung der Sicherheit des Gateways für das digitale COVID-Zertifikat der EU sollte im Einklang mit der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([6]) erfolgen.

(17) Die Mitgliedstaaten, vertreten durch die benannten nationalen Behörden oder amtlichen Stellen, legen gemeinsam den Zweck der und die Mittel zur Verarbeitung personenbezogener Daten über das Gateway für das digitale COVID-Zertifikat der EU fest und sind daher gemeinsam Verantwortliche. Artikel 26 der Verordnung (EU) 2016/679 verpflichtet die gemeinsam für die Verarbeitung personenbezogener Daten Verantwortlichen, in transparenter Form festzulegen, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt. Ferner ist darin die Möglichkeit vorgesehen, dass diese Zuständigkeiten durch Rechtsvorschriften der Union oder der Mitgliedstaaten festgelegt werden, denen die Verantwortlichen unterliegen. Die Regelung gemäß Artikel 26 sollte in Anhang III dieses Beschlusses aufgenommen werden.

(18) Mit der Verordnung (EU) 2021/953 wird der Kommission die Aufgabe übertragen, einen solchen Austausch zu unterstützen. Dieser Auftrag lässt sich am besten erfüllen, indem die Kommission die vorgelegten Zertifikatswiderrufslisten im Auftrag der Mitgliedstaaten zusammenführt. Daher sollte der Kommission eine Rolle als Auftragsverarbeiterin zugewiesen werden, damit sie den Austausch von Listen über das Gateway für das digitale COVID-Zertifikat der EU im Auftrag der Mitgliedstaaten erleichtern kann.

(19) Als Anbieterin technischer und organisatorischer Lösungen für das Gateway für das digitale COVID-Zertifikat der EU verarbeitet die Kommission im Auftrag der Mitgliedstaaten als gemeinsam Verantwortliche die personenbezogenen Daten in den Widerrufslisten im Gateway. Daher handelt sie als deren Auftragsverarbeiterin. Gemäß Artikel 28 der Verordnung (EU) 2016/679 und Artikel 29 der Verordnung (EU) 2018/1725 erfolgt die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines Rechtsinstruments nach dem Recht der Union oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und die Verarbeitung regelt. Daher ist es erforderlich, Vorschriften für die Verarbeitung durch die Kommission als Auftragsverarbeiterin festzulegen.

(20) Die unterstützende Rolle der Kommission umfasst nicht die Einrichtung einer zentralen Datenbank gemäß Erwägungsgrund 52 der Verordnung (EU) 2021/953. Dadurch soll verhindert werden, dass alle ausgestellten digitalen COVID-Zertifikate der EU zentral gespeichert werden; gleichzeitig werden die Mitgliedstaaten nicht daran gehindert, Widerrufslisten auszutauschen, wie dies in Artikel 4 Absatz 2 der Verordnung (EU) 2021/953 ausdrücklich vorgesehen ist.

(21) Bei der Verarbeitung personenbezogener Daten im Gateway für das digitale COVID-Zertifikat der EU ist die Kommission an den Beschluss (EU, Euratom) 2017/46 der Kommission gebunden ([7]).

(22) Gemäß Artikel 3 Absatz 10 der Verordnung (EU) 2021/953 kann die Kommission Durchführungsrechtsakte erlassen, um COVID-19-Zertifikate, die von einem Drittland ausgestellt wurden, mit dem die Union und die Mitgliedstaaten ein Abkommen über den freien Personenverkehr geschlossen haben, das es den Vertragsparteien gestattet, die Freizügigkeit aus Gründen der öffentlichen Gesundheit nichtdiskriminierend zu beschränken, und das keinen Mechanismus zur Aufnahme von Rechtsakten der Union enthält, als den gemäß dieser Verordnung ausgestellten Zertifikaten gleichwertig anzuerkennen. Auf dieser Grundlage erließ die Kommission am 8. Juli 2021 den Durchführungsbeschluss (EU) 2021/1126 ([8]) zur Feststellung der Gleichwertigkeit der von der Schweiz ausgestellten COVID-19-Zertifikate.

([5]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

([6]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

([7]) Weitere Informationen über Sicherheitsstandards, die für alle Informationssysteme der Europäischen Kommission gelten, veröffentlicht die Kommission unter https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en.

([8]) Durchführungsbeschluss (EU) 2021/1126 der Kommission vom 8. Juli 2021 zur Feststellung der Gleichwertigkeit der von der Schweiz ausgestellten COVID-19-Zertifikate mit den gemäß der Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates ausgestellten Zertifikaten (ABl. L 243 vom 9.7.2021, S. 49).

(23) Gemäß Artikel 8 Absatz 2 der Verordnung (EU) 2021/953 kann die Kommission Durchführungsrechtsakte erlassen, in denen festgelegt wird, dass COVID-19-Zertifikate, die von einem Drittland im Einklang mit Standards und technologischen Systemen ausgestellt werden, die mit dem Vertrauensrahmen für das digitale COVID-Zertifikat der EU interoperabel sind und die Überprüfung der Echtheit, Gültigkeit und Integrität des Zertifikats ermöglichen, und die die im Anhang der Verordnung aufgeführten Daten enthalten, als den digitalen COVID-Zertifikaten der EU gleichwertig zu betrachten sind, um den Inhabern die Ausübung ihres Rechts auf Freizügigkeit innerhalb der Union zu erleichtern. Wie in Erwägungsgrund 28 der Verordnung (EU) 2021/953 erwähnt, betrifft Artikel 8 Absatz 2 der genannten Verordnung die Anerkennung von Zertifikaten, die Unionsbürgern und ihren Familienangehörigen von Drittländern ausgestellt werden. Die Kommission hat bereits mehrere solche Durchführungsrechtsakte erlassen.

(24) Um Lücken bei der Erkennung widerrufener Zertifikate zu vermeiden, die unter solche Durchführungsrechtsakte fallen, sollten Drittländer, deren COVID-19-Zertifikate gemäß Artikel 3 Absatz 10 und Artikel 8 Absatz 2 der Verordnung (EU) 2021/953 als gleichwertig anerkannt wurden, auch die Möglichkeit haben, entsprechende Zertifikatswiderrufslisten an das Gateway für das digitale COVID-Zertifikat der EU zu übermitteln.

(25) Einige Drittstaatsangehörige, die Inhaber widerrufener COVID-19-Zertifikate sind, die von einem Drittland ausgestellt wurden, dessen COVID-19-Zertifikate gemäß der Verordnung (EU) 2021/953 als gleichwertig anerkannt wurden, fallen zu dem Zeitpunkt, zu dem das betreffende Drittland eine Widerrufsliste erstellt, die auch ihr Zertifikat enthält, möglicherweise weder unter die genannte Verordnung noch unter die Verordnung (EU) 2021/954. Zu dem Zeitpunkt, zu dem ein Drittland eine Zertifikatswiderrufsliste erstellt, ist jedoch nicht bekannt, ob alle Drittstaatsangehörigen, die Inhaber widerrufener Zertifikate sind, unter eine der beiden Verordnungen fallen. Es ist daher nicht möglich, Personen, die zum Zeitpunkt der Erstellung der Zertifikatswiderrufslisten dieser Länder nicht unter eine der genannten Verordnungen fallen, auszuschließen, und ein entsprechender Versuch würde dazu führen, dass die Mitgliedstaaten widerrufene Zertifikate von Drittstaatsangehörigen, die erstmals in die Union einreisen, nicht erkennen könnten. Doch auch die widerrufenen Zertifikate dieser Drittstaatsangehörigen würden von den Mitgliedstaaten bei der Einreise der Zertifikatinhaber in die Union und bei Reisen innerhalb der Union überprüft. Die Drittländer, deren Zertifikate gemäß der Verordnung (EU) 2021/953 als gleichwertig anerkannt wurden, sind nicht an der Verwaltung des Gateways beteiligt und gelten daher nicht als gemeinsam Verantwortliche.

(26) Darüber hinaus hat sich das System des digitalen COVID-Zertifikats der EU als das einzige international umfassend funktionierende COVID-19-Zertifikatsystem erwiesen Das digitale COVID-Zertifikat der EU hat daher weltweit an Bedeutung gewonnen und dazu beigetragen, die Pandemie auf internationaler Ebene zu bekämpfen, da sicheres internationales Reisen und die weltweite Erholung erleichtert werden. Bei der Annahme weiterer Durchführungsrechtsakte gemäß Artikel 8 Absatz 2 der Verordnung (EU) 2021/953 ergeben sich neue Erfordernisse beim Füllen des digitalen COVID-Zertifikats der EU. Gemäß den Vorschriften des Durchführungsbeschlusses (EU) 2021/1073 ist der Nachname im technischen Inhalt des Zertifikats ein Pflichtfeld. Damit andere Systeme eingebunden werden können und interoperabel sind, muss diese Anforderung geändert werden, denn in einigen Drittländern gibt es Personen ohne Nachnamen. In Fällen, in denen sich der Name des Zertifikatinhabers nicht in zwei Teile unterteilen lässt, sollte der Name in das Feld (Name bzw. Vorname) des digitalen COVID-Zertifikats der EU eingetragen werden, in dem er auch im Reise- oder Ausweisdokument des Inhabers steht. Durch diese Änderung würde der technische Inhalt der Zertifikate auch besser an die derzeit gültigen Spezifikationen für maschinenlesbare Reisedokumente angepasst, die von der Internationalen Zivilluftfahrt-Organisation herausgegeben wurden.

(27) Der Durchführungsbeschluss (EU) 2021/1073 sollte daher entsprechend geändert werden.

(28) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 konsultiert und hat am 11. März 2022 eine Stellungnahme abgegeben.

(29) Damit die Mitgliedstaaten und die Kommission genügend Zeit haben, um die für den Austausch von Zertifikatswiderrufslisten über das Gateway für das digitale COVID-Zertifikat der EU erforderlichen Änderungen umzusetzen, sollte der Geltungsbeginn dieses Beschlusses vier Wochen nach seinem Inkrafttreten liegen.

(30) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des nach Artikel 14 der Verordnung (EU) 2021/953 eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Der Durchführungsbeschluss (EU) 2021/1073 wird wie folgt geändert:

1. Die folgenden Artikel 5a, 5b und 5c werden eingefügt:

„*Artikel 5a*

Austausch von Zertifikatswiderrufslisten

(1) Der Vertrauensrahmen für das digitale COVID-Zertifikat der EU ermöglicht den Austausch von Zertifikatswiderrufslisten über das zentrale Gateway für das digitale COVID-Zertifikat der EU (im Folgenden das ‚Gateway') im Einklang mit den technischen Spezifikationen in Anhang I.

(2) Wenn Mitgliedstaaten digitale COVID-Zertifikate der EU widerrufen, können sie Zertifikatswiderrufslisten an das Gateway übermitteln.

(3) Übermitteln Mitgliedstaaten Zertifikatswiderruflisten, so führen die ausstellenden Behörden eine Liste der widerrufenen Zertifikate.

(4) Werden personenbezogene Daten über das Gateway ausgetauscht, ist die Verarbeitung darauf beschränkt, den Austausch von Informationen über den Widerruf zu unterstützen. Diese personenbezogenen Daten dürfen nur zur Überprüfung des Widerrufsstatus von im Rahmen der Verordnung (EU) 2021/953 ausgestellten digitalen COVID-Zertifikaten der EU verwendet werden.

(5) Die an das Gateway übermittelten Informationen enthalten gemäß den technischen Spezifikationen in Anhang I folgende Angaben:

a) die pseudonymisierten eindeutigen Zertifikatkennungen der widerrufenen Zertifikate,

b) das Ablaufdatum der übermittelten Zertifikatswiderrufsliste.

(6) Widerruft eine ausstellende Behörde digitale COVID-Zertifikate der EU, die sie gemäß der Verordnung (EU) 2021/953 oder der Verordnung (EU) 2021/954 ausgestellt hat, und möchte sie entsprechende Informationen über das Gateway austauschen, so übermittelt sie die in Absatz 5 genannten Informationen im Einklang mit den technischen Spezifikationen in Anhang I in Form von Zertifikatswiderrufslisten in einem sicheren Format an das Gateway.

(7) Die ausstellenden Behörden bieten so weit wie möglich eine Lösung an, um die Inhaber widerrufener Zertifikate zum Zeitpunkt des Widerrufs über den Widerrufsstatus ihrer Zertifikate und den Grund für den Widerruf zu informieren.

(8) Über das Gateway werden die eingegangenen Zertifikatswiderrufslisten zusammengetragen. Zudem werden darüber Instrumente bereitgestellt, um die Listen an die Mitgliedstaaten weiterzugeben. Das Gateway löscht die Listen automatisch, wenn das von den übermittelnden Behörden für jede Liste angegebene Ablaufdatum erreicht ist.

(9) Die benannten nationalen Behörden oder amtlichen Stellen der Mitgliedstaaten, die personenbezogene Daten im Gateway verarbeiten, sind gemeinsam Verantwortliche für die verarbeiteten Daten. Die jeweiligen Zuständigkeiten der gemeinsam Verantwortlichen werden gemäß Anhang VI zugewiesen.

(10) Die Kommission ist die Auftragsverarbeiterin der personenbezogenen Daten, die im Gateway verarbeitet werden. In ihrer Eigenschaft als Auftragsverarbeiterin im Auftrag der Mitgliedstaaten gewährleistet die Kommission die sichere Übermittlung und das sichere Hosting personenbezogener Daten innerhalb des Gateways und erfüllt die Pflichten des Auftragsverarbeiters gemäß Anhang VII.

(11) Die Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit bei der Verarbeitung personenbezogener Daten im Gateway wird von der Kommission und den gemeinsam Verantwortlichen regelmäßig geprüft, beurteilt und bewertet.

Artikel 5b

Übermittlung von Zertifikatswiderruflisten durch Drittländer

Drittländer, die COVID-19-Zertifikate ausstellen, für die die Kommission einen Durchführungsrechtsakt gemäß Artikel 3 Absatz 10 oder Artikel 8 Absatz 2 der Verordnung (EU) 2021/953 erlassen hat, können im Einklang mit den technischen Spezifikationen in Anhang I Listen widerrufener COVID-19-Zertifikate, die unter einen solchen Durchführungsrechtsakt fallen, zur Verarbeitung durch die Kommission im Auftrag der gemeinsam Verantwortlichen gemäß Artikel 5a über das Gateway übermitteln.

Artikel 5c

Verwaltung der Verarbeitung personenbezogener Daten im zentralen Gateway für das digitale COVID-Zertifikat der EU

(1) Der Entscheidungsprozess der gemeinsam Verantwortlichen wird von einer Arbeitsgruppe geregelt, die im Rahmen des in Artikel 14 der Verordnung (EU) 2021/953 genannten Ausschusses eingesetzt wird.

(2) Die benannten nationalen Behörden oder amtlichen Stellen der Mitgliedstaaten, die als gemeinsam Verantwortliche personenbezogene Daten im Gateway verarbeiten, entsenden Vertreter in diese Gruppe."

2. Anhang I wird gemäß Anhang I dieses Beschlusses geändert.

3. Anhang V wird gemäß Anhang II dieses Beschlusses geändert.

4. Der Wortlaut des Anhangs III dieses Beschlusses wird als Anhang VI angefügt.

5. Der Wortlaut des Anhangs IV dieses Beschlusses wird als Anhang VII angefügt.

Artikel 2

Dieser Beschluss tritt am dritten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Der Geltungsbeginn liegt vier Wochen nach seinem Inkrafttreten.

Brüssel, den 21. März 2022

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

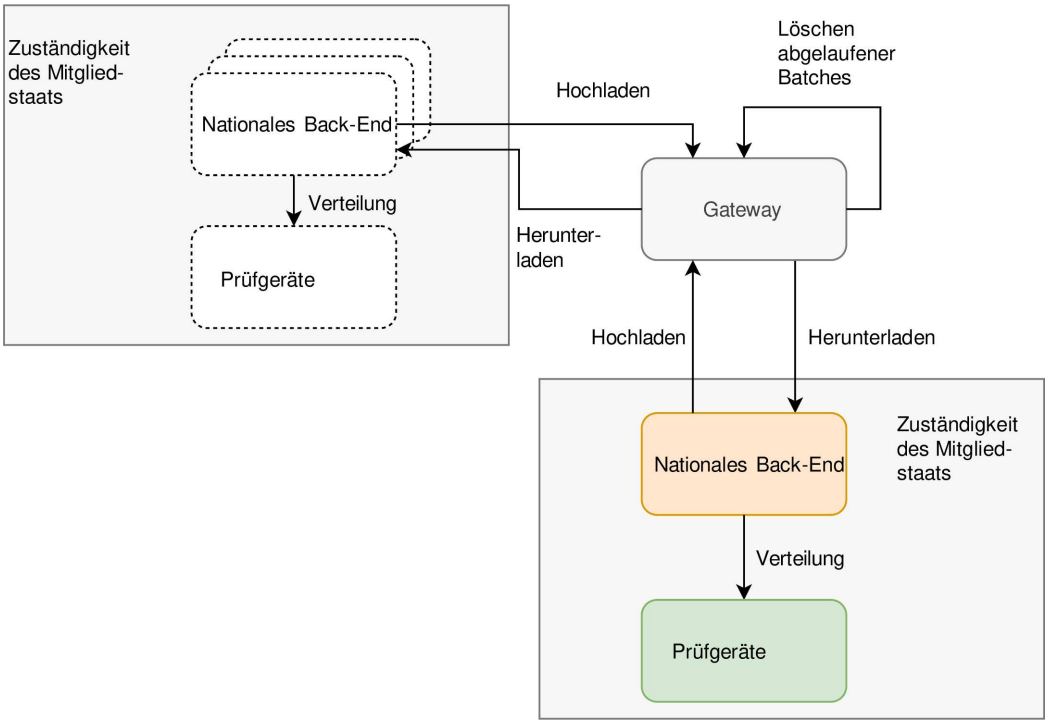
ANHANG I

In Anhang I des Durchführungsbeschlusses (EU) 2021/1073 wird der folgende Abschnitt 9 angefügt:

„9. **WIDERRUFSLÖSUNG**

9.1. **Bereitstellung der DCC-Widerrufsliste (DRL)**

Das Gateway stellt Endpunkte und Funktionen zur Speicherung und Verwaltung der Zertifikatswiderrufslisten bereit:



9.2. **Vertrauensmodell**

Alle Verbindungen werden vom Standard-DCCG-Vertrauensmodell mithilfe von NB_{TLS}- und NB_{UP}-Zertifikaten hergestellt (siehe Verwaltung der Zertifikate). Alle Informationen werden in CMS-Nachrichten verpackt hochgeladen, um ihre Integrität zu gewährleisten.

9.3. **Erstellung der Batches**

9.3.1. *Batch*

Jede Widerrufsliste muss einen oder mehrere Einträge enthalten und wird in Batches verpackt, die eine Reihe von Hashwerten und ihre Metadaten enthalten. Ein Batch ist unveränderlich und definiert ein Ablaufdatum, an dem der Batch gelöscht werden kann. Das Ablaufdatum aller Elemente des Batches muss genau gleich sein, d. h., die Batches werden nach Ablaufdatum und dem Signatur-DSC gruppiert. Jeder Batch kann höchstens 1 000 Einträge enthalten. Umfasst die Widerrufsliste mehr als 1 000 Einträge, werden mehrere Batches erstellt. Jeder Eintrag kann in höchstens einem Batch erscheinen. Der Batch wird in einer CMS-Struktur verpackt und mit dem NB_{UP}-Zertifikat des hochladenden Landes signiert.

9.3.2. *Batch-Index*

Bei der Erstellung erhält der Batch vom Gateway eine eindeutige Kennung, die dem Index automatisch hinzugefügt wird. Der Batch-Index wird in aufsteigender chronologischer Reihenfolge des Änderungsdatums geordnet.

9.3.3. *Gateway-Verhalten*

Das Gateway verarbeitet Widerrufs-Batches ohne jegliche Änderung: Es kann Batches weder aktualisieren noch entfernen oder sie um weitere Informationen ergänzen. Die Batches werden an alle zugelassenen Länder weitergeleitet (siehe Kapitel 9.6).

Das Gateway beobachtet aktiv die Ablaufdaten der Batches und entfernt die abgelaufenen Batches. Wenn ein Batch gelöscht ist, gibt das Gateway für die gelöschte Batch-URL die Antwort ‚HTTP 410 Gone' aus. Der Batch erscheint im Batch-Index daher als ‚gelöscht'.

9.4. **Hash-Typen**

Die Widerrufsliste enthält Hashwerte, die verschiedenen Arten/Attributen von Widerrufen entsprechen können. Diese Arten oder Attribute sind bei der Bereitstellung der Widerrufslisten anzugeben. Derzeit gibt es folgende Arten:

Art	Attribut	Hashwert-Berechnung
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing CountryCode + UCI

Es werden nur die ersten 128 Bits der als Base64-Strings kodierten Hashwerte in die Batches aufgenommen und zur Identifizierung des widerrufenen DCC verwendet ([1]).

9.4.1. *Hash-Typ: SHA256(DCC Signature)*

In diesem Fall wird der Hashwert über die Bytes der COSE_SIGN1-Signatur des CWT berechnet. Bei RSA-Signaturen wird die gesamte Signatur verwendet. Die Formel für EC-DSA-signierte Zertifikate mit dem Wert r als Eingabe lautet:

SHA256(r)

[für alle neuen Umsetzungen vorgeschrieben]

9.4.2. *Hash-Typ: SHA256(UCI)*

In diesem Fall wird der Hashwert über den in UTF-8 kodierten UCI-String berechnet und in ein Byte-Array konvertiert.

[überholt ([2]), wird aber zur Gewährleistung der Rückwärtskompatibilität unterstützt]

9.4.3. *Hash-Typ: SHA256(Issuing CountryCode+UCI)*

In diesem Fall ist der als UTF-8-String kodierte Ländercode mit der als UTF-8-String kodierten UCI verkettet. Dies wird zu einem Byte-Array konvertiert und als Eingabe für die Hash-Funktion verwendet.

[überholt[2], wird aber zur Gewährleistung der Rückwärtskompatibilität unterstützt]

9.5. **API-Struktur**

9.5.1. *API für die Bereitstellung von Widerrufseinträgen*

9.5.1.1. Zweck

Die API stellt die Einträge der Widerrufslisten in Batches zusammen mit einem Batch-Index bereit.

9.5.1.2. Endpunkte

([1]) Für detaillierte API-Beschreibungen siehe auch Abschnitt 9.5.1.2.

([2]) ‚Überholt' bedeutet, dass diese Funktion bei neuen Umsetzungen nicht enthalten ist, aber für einen bestimmten Zeitraum für bestehende Umsetzungen unterstützt wird.

9.5.1.2.1. Endpunkt zum Download der Batch-Liste

Die Endpunkte sind einfach strukturiert und geben eine Liste von Batches zusammen mit einem kleinen Wrapper mit Metadaten aus. Die Batches werden nach *Datum* in *aufsteigender (chronologischer)* Reihenfolge geordnet:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    'more':true|false,
    'batches':
        [{
            'batchId': '{uuid}',
            'country': 'XY',
            'date': '2021-11-01T00:00:00Z'
            'deleted': true | false
        }, ..
        ]
}
```

Anmerkung: Das Ergebnis ist standardmäßig auf 1 000 begrenzt. Ist das Flag ‚more' auf ‚true' gesetzt, besteht die Antwort darin, dass weitere Batches heruntergeladen werden können. Um weitere Elemente herunterzuladen, muss der Client den Header If-Modified-Since auf ein Datum setzen, das nicht vor dem letzten abgerufenen Eintrag liegen kann.

Die Antwort enthält ein JSON-Array mit folgender Struktur:

Feld	Definition
more	Boolesches Flag, das angibt, dass es weitere Batches gibt
batches	Array der vorhandenen Batches
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Ländercode nach ISO 3166
date	Datum (UTC) nach ISO 8601. Datum, an dem der Batch hinzugefügt oder gelöscht wurde.
deleted	Boolesches Flag. Wahr, falls gelöscht. Wenn das Flag ‚deleted' gesetzt wurde, kann der Eintrag nach 7 Tagen endgültig aus den Abfrageergebnissen entfernt werden.

9.5.1.2.1.1. Antwort*codes*

Code	Beschreibung
200	Alles ok
204	Kein Inhalt, wenn der Inhalt unter dem Header ‚If-Modified-Since' keine Übereinstimmung aufweist.

Anfrage-Header

Header	Pflichtfeld	Beschreibung
If-Modified-Since	Ja	Dieser Header enthält das letzte Download-Datum, damit nur die neuesten Ergebnisse angezeigt werden. Bei Erstaufruf sollte der Header auf ‚2021-06-01T00:00:00Z' gesetzt werden.

9.5.1.2.2. Endpunkt für den Batch-Download

Die Batches enthalten eine Liste von Zertifikatskennungen:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

'country': 'XY',

'expires': '2022-11-01T00:00:00Z',

'kid':'23S+33f=',

'hashType':'SIGNATURE',

'entries':[{

'hash':'e2e2e2e2e2e2e2e2'

}, ..]

}

Die Antwort enthält eine CMS mit einer Signatur, die mit dem NB_{UP}-Zertifikat des Landes übereinstimmen muss. Alle Elemente des JSON-Array umfassen folgende Struktur:

Feld	Pflichtfeld	Art	Definition
expires	Ja	String	Datum, an dem das Element entfernt werden kann. Datum/Uhrzeit (UTC) nach ISO 8601
country	Ja	String	Ländercode nach ISO 3166
hashType	Ja	String	Hash-Typ der bereitgestellten Einträge (siehe Hash-Typen)
entries	Ja	JSON Object Array	Siehe die Tabelle Einträge
kid	Ja	String	Base64-kodierte Schlüsselkennung (KID) des für die Signatur des DCC verwendeten DSC. Ist die KID nicht bekannt, kann der String `UNKNOWN_KID` (ohne das Zeichen `) verwendet werden.

Anmerkungen:

— Die Batches werden nach Ablaufdatum und DSC gruppiert — alle Elemente laufen zum gleichen Zeitpunkt ab und wurden mit demselben Schlüssel signiert.

— Der Ablaufzeitpunkt wird als Datum/Uhrzeit in UTC angegeben, da das EUDCC ein weltweites System ist und der Zeitpunkt eindeutig sein muss.

— Das Ablaufdatum eines endgültig widerrufen DCC wird auf das Ablaufdatum des entsprechenden DSC, mit dem das DCC signiert wurde, oder auf das Ablaufdatum des widerrufenen DCC gesetzt (in letzterem Fall werden die numerischen Datums-/Epoch-Zeit-Angaben wie UTC-Zeitangaben behandelt).

— Das nationale Back-End (NB) entfernt Elemente aus der Widerrufsliste, wenn das **Ablauf**datum erreicht ist.

— Das NB kann Elemente aus seiner Widerrufsliste entfernen, wenn die für die Signatur des DCC verwendete **kid** widerrufen wird.

9.5.1.2.2.1. Einträge

Feld	Pflichtfeld	Art	Definition
hash	Ja	String	Die ersten 128 Bits des als base64-String kodierten SHA256-Hashwerts

Anmerkung: Das Objekt Einträge enthält derzeit nur einen Hash, aber zur Gewährleistung der Kompatibilität mit künftigen Änderungen wurde anstelle eines JSON-Arrays ein Objekt gewählt.

9.5.1.2.2.2. Antwort-Codes

Code	Beschreibung
200	Alles ok
410	Batch entfernt. Batch kann im nationalen Back-End gelöscht werden.

9.5.1.2.2.3. Antwort-Header

Header	Beschreibung
ETag	Batch-Kennung

9.5.1.2.3. Endpunkt zum Hochladen von Batches

Das Hochladen erfolgt mit demselben Endpunkt über das Verb POST:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

{

‘country‘: ‘XY‘,

‘expires‘: ‘2022-11-01T00:00:00Z‘,

‘kid‘:‘23S+33f=‘,

‘hashType‘:‘SIGNATURE‘,

‘entries‘:[{

‘hash‘:‘e2e2e2e2e2e2e2e2‘

}, ..]

}

Der Batch wird mit dem NB_{UP}-Zertifikat signiert. Das Gateway überprüft, ob die Signatur vom NB_{UP} des jeweiligen *Landes* gesetzt wurde. Wird dies bei der Überprüfung der Signatur nicht festgestellt, ist das Hochladen nicht möglich.

ANMERKUNG: Jeder Batch ist unveränderlich und kann nach dem Hochladen nicht mehr geändert werden. Er kann jedoch gelöscht werden. Die Kennung jedes gelöschten Batches wird gespeichert, und es kann kein neuer Batch mit derselben Kennung hochgeladen werden.

9.5.1.2.4. Endpunkt zum Löschen von Batches

Ein Batch kann mit demselben Endpunkt über das Verb DELETE gelöscht werden:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

‘batchId‘: ‘...‘

}

Im Interesse der Kompatibilität kann der Batch auch mit dem folgenden Endpunkt über das Verb POST gelöscht werden:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

‘batchId‘: ‘...‘

}

9.6. **API-Schutz/DSGVO**

In diesem Abschnitt sind für die Umsetzung Maßnahmen zur Einhaltung der Bestimmungen der Verordnung (EU) 2021/953 hinsichtlich der Verarbeitung personenbezogener Daten festgelegt.

9.6.1. *Vorhandene Authentifizierung*

Das Gateway nutzt derzeit das NB_{TLS}-Zertifikat für die Authentifizierung von Ländern bei der Verbindung mit dem Gateway. Diese Authentifizierung kann verwendet werden, um die Identität des mit dem Gateway verbundenen Landes zu bestimmen. Diese Identität kann dann für die Zugangskontrolle genutzt werden.

9.6.2. *Zugangskontrolle*

Um personenbezogene Daten rechtmäßig verarbeiten zu können, wendet das Gateway einen Zugangskontrollmechanismus an.

Das Gateway nutzt eine Zugriffskontrollliste in Kombination mit einem rollenbasierten Sicherheitssystem (Role Based Security). Dabei werden zwei Tabellen geführt — eine Tabelle, die beschreibt, welche Rollen welche Vorgänge an welchen Ressourcen durchführen können, die andere beschreibt, welche Rollen welchen Nutzern zugewiesen sind.

Für die nach diesem Dokument vorgeschriebenen Kontrollen sind die folgenden drei Rollen erforderlich:

RevocationListReader

RevocationUploader

RevocationDeleter

Die folgenden Endpunkte prüfen, ob der Nutzer die Rolle RevocationListReader hat; ist dies der Fall, wird der Zugang gewährt; falls nicht, erscheint HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Die folgenden Endpunkte prüfen, ob der Nutzer die Rolle RevocationUploader hat; ist dies der Fall, wird der Zugang gewährt; ist dies nicht der Fall, erscheint HTTP 403 Forbidden:

POST/revocation-list

Die folgenden Endpunkte prüfen, ob der Nutzer die Rolle RevocationDeleter hat; ist dies der Fall, wird der Zugang gewährt; ist dies nicht der Fall, erscheint HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

Zudem bietet das Gateway eine zuverlässige Methode, mit der die Administratoren die mit den Nutzern verknüpften Rolle so verwalten können, dass die Wahrscheinlichkeit menschlicher Fehler verringert wird und die funktionalen Administratoren gleichzeitig nicht belastet werden.“

ANHANG II

Anhang V Abschnitt 3 des Durchführungsbeschlusses (EU) 2021/1073 erhält folgende Fassung:

„3. ***Gemeinsame Strukturen und allgemeine Anforderungen***

Ein digitales COVID-Zertifikat der EU darf nicht ausgestellt werden, wenn aufgrund fehlender Informationen nicht alle Datenfelder entsprechend dieser Spezifikation korrekt gefüllt werden können. **Die Pflicht der Mitgliedstaaten zur Ausstellung digitaler COVID-Zertifikate der EU bleibt hiervon unberührt.**

In allen Feldern können Informationen unter Verwendung des vollständigen Zeichensatzes UNICODE 13.0 im Format UTF-8 eingegeben werden, sofern keine besonderen Beschränkungen auf Wertesätze oder begrenztere Zeichensätze gelten.

Die gemeinsame Struktur stellt sich wie folgt dar:

‚JSON':{

‚ver':<Versionsinformationen>,

‚nam':{

<Informationen zum Namen der Person>

},

‚dob':<Geburtsdatum>,

‚v' or ‚t' or ‚r':[

{<Informationen zu Impfdosis, Test oder Genesung, ein Eintrag>}

]

}

Nähere Informationen zu einzelnen Gruppen und Feldern finden sich in den nachfolgenden Abschnitten.

Ist nach den Regeln ein Feld zu überspringen, bedeutet dies, dass sein Inhalt leer sein muss und es weder die Bezeichnung noch den Wert des Feldes aufweisen darf.

3.1. ***Version***

Informationen zur Version sind anzugeben. Die Versionierung erfolgt nach dem Konzept der semantischen Versionierung (semver: https://semver.org). Bei der genutzten Version muss es sich um eine der offiziell freigegebenen Versionen (die aktuelle oder eine ältere offiziell freigegebene Version) handeln. Siehe Abschnitt ‚Lokalisierung des JSON-Schemas' für weitere Einzelheiten.

Feldkennung	Feldbezeichnung	Erläuterungen
ver	Schemaversion	Muss der Kennung der für die Erstellung des EUDCC verwendeten Schemaversion entsprechen. Beispiel: ‚ver':‚1.3.0'

3.2. ***Name und Geburtsdatum der Person***

Der Name der Person ist ihr amtlicher vollständiger Name, der dem in Reisedokumenten eingetragenen Namen entspricht. Die Kennung der Struktur ist *nam*. Es ist genau 1 (ein) Personenname anzugeben.

Feldkennung	Feldbezeichnung	Erläuterungen
nam/fn	Nachname(n)	Nachname(n) des Inhabers. Hat der Inhaber keine Nachnamen, aber einen Vornamen, so ist das Feld zu überspringen. In allen anderen Fällen muss genau 1 (ein) nicht leeres Feld vorhanden sein, das alle Nachnamen enthält. Im Fall mehrerer Nachnamen sind diese durch ein Leerzeichen voneinander zu trennen. Zusammengesetzte Namen mit Bindestrichen oder ähnlichen Zeichen müssen jedoch unverändert bleiben.

		Beispiele: ‚fn':‚Musterfrau-Gößinger' ‚fn':‚Musterfrau-Gößinger Müller'
nam/fnt	Standardisierte (r) Nachname(n)	Nachname(n) des Inhabers, der/die nach derselben Konvention transliteriert wurde(n) wie in den maschinenlesbaren Reisedokumenten des Inhabers (zum Beispiel nach den von der ICAO in ihrem Dokument 9303 Teil 3 festgelegten Regeln). Hat der Inhaber keine Nachnamen, aber einen Vornamen, so ist das Feld zu überspringen. In allen anderen Fällen muss genau 1 (ein) nicht leeres Feld vorhanden sein, das nur die Zeichen A-Z und < enthält. Maximale Länge: 80 Zeichen (gemäß der ICAO-Spezifikation im Dokument 9303). Beispiele: ‚fnt':‚MUSTERFRAU<GOESSINGER' ‚fnt':‚MUSTERFRAU<GOESSINGER<MUELLER'
nam/gn	Vorname(n)	Vorname(n) des Inhabers. Hat der Inhaber keine Vornamen, aber einen Nachnamen, so ist das Feld zu überspringen. In allen anderen Fällen muss genau 1 (ein) nicht leeres Feld vorhanden sein, das alle Vornamen enthält. Im Fall mehrerer Vornamen sind diese durch ein Leerzeichen voneinander zu trennen. Beispiel: ‚gn':‚Isolde Erika'
nam/gnt	Standardisierte (r) Vorname(n)	Vorname(n) des Inhabers, der/die nach derselben Konvention transliteriert wurde(n) wie in den maschinenlesbaren Reisedokumenten des Inhabers (zum Beispiel nach den von der ICAO in ihrem Dokument 9303 Teil 3 festgelegten Regeln). Hat der Inhaber keine Vornamen, aber einen Nachnamen, so ist das Feld zu überspringen. In allen anderen Fällen muss genau 1 (ein) nicht leeres Feld vorhanden sein, das nur die Zeichen A-Z und < enthält. Maximale Länge: 80 Zeichen. Beispiel: ‚gnt':‚ISOLDE<ERIKA'
dob	Geburtsdatum	Geburtsdatum des Inhabers des digitalen COVID-Zertifikats der EU. Vollständiges Datum oder Teildatum ohne Uhrzeit, beschränkt auf den Bereich von 1900-01-01 bis 2099-12-31. Wenn das Geburtsdatum vollständig oder teilweise bekannt ist, muss genau 1 (ein) nicht leeres Feld vorhanden sein. Wenn das Geburtsdatum auch nicht teilweise bekannt ist, muss das Feld auf eine leere Zeichenfolge ‚' gesetzt werden. Dies sollte mit den Angaben in den Reisedokumenten übereinstimmen. Wenn Informationen zum Geburtsdatum vorliegen, ist eines der nachstehenden ISO-8601-Formate zu verwenden. Andere Optionen werden nicht unterstützt. YYYY-MM-DD YYYY-MM YYYY (Die Prüf-App kann unter Verwendung der XX-Konvention, die in maschinenlesbaren Reisedokumenten verwendet wird, fehlende Teile des Geburtsdatums anzeigen, z. B. 1990-XX-XX.) Beispiele: ‚dob':‚1979-04-14' ‚dob':‚1901-08' ‚dob': ‚1939' ‚dob': ‚'

3.3. ***Gruppen für spezifische Informationen je nach Zertifikatstyp***

Das JSON-Schema unterstützt drei Gruppen von Einträgen mit spezifischen Informationen je nach Zertifikatstyp. Jedes EUDCC muss genau 1 (eine) Gruppe enthalten. Leere Gruppen sind nicht zulässig.

Gruppen-kennung	**Bezeichnung der Gruppe**	**Einträge**
v	Gruppe Impfung	Sie muss, falls vorhanden, genau 1 (einen) Eintrag enthalten, der genau 1 (eine) Impfdosis (eine Dosis) beschreibt.
t	Gruppe Test	Sie muss, falls vorhanden, genau 1 (einen) Eintrag enthalten, der genau 1 (ein) Testergebnis beschreibt.
r	Gruppe Genesung	Sie muss, falls vorhanden, genau 1 (einen) Eintrag enthalten, der genau 1 (eine) Genesungsbestätigung beschreibt.“

ANHANG III

„ANHANG VI

ZUSTÄNDIGKEITEN DER MITGLIEDSTAATEN FÜR DEN AUSTAUSCH VON EUDCC-WIDERRUFSLISTEN ALS GEMEINSAM VERANTWORTLICHE FÜR DAS GATEWAY FÜR DAS DIGITALE COVID-ZERTIFIKAT DER EU

ABSCHNITT 1

Unterabschnitt 1

Aufteilung der Zuständigkeiten

(1) Die gemeinsam Verantwortlichen verarbeiten personenbezogene Daten über das Gateway im Einklang mit den technischen Spezifikationen aus Anhang I.

(2) Die für die Ausstellung zuständigen Behörden der Mitgliedstaaten bleiben weiterhin alleine verantwortlich für die Erhebung, Nutzung, Offenlegung und jede sonstige Verarbeitung von Widerrufsinformationen außerhalb des Gateways, einschließlich des Verfahrens für den Widerruf von Zertifikaten.

(3) Jeder Verantwortliche ist dafür verantwortlich, dass die Verarbeitung personenbezogener Daten im Gateway des Vertrauensrahmens im Einklang mit den Artikeln 5, 24 und 26 der Datenschutz-Grundverordnung erfolgt.

(4) Jeder Verantwortliche richtet eine Anlaufstelle mit einer Funktions-Mailbox ein, die der Kommunikation zwischen den gemeinsam Verantwortlichen sowie zwischen den gemeinsam Verantwortlichen und dem Auftragsverarbeiter dient.

(5) Eine von dem in Artikel 14 der Verordnung (EU) 2021/953 genannten Ausschuss eingesetzte Arbeitsgruppe wird damit beauftragt, über alle Fragen zu entscheiden, die sich in Bezug auf den Austausch von Widerrufslisten und die gemeinsame Verantwortlichkeit für die Verarbeitung der personenbezogenen Daten ergeben können, und an der Erstellung koordinierter Weisungen für die Kommission als Auftragsverarbeiterin mitzuwirken. Der Entscheidungsprozess der gemeinsam Verantwortlichen wird von dieser Arbeitsgruppe und der von ihr zu verabschiedenden Verfahrensordnung geregelt. Grundsätzlich führt die Nichtteilnahme eines der gemeinsam Verantwortlichen an einer Sitzung dieser Arbeitsgruppe, die mindestens sieben (7) Tage vor ihrer Einberufung schriftlich angekündigt wurde, zur stillschweigenden Zustimmung zu den Ergebnissen dieser Sitzung der Arbeitsgruppe. Jeder der gemeinsam Verantwortlichen kann eine Sitzung dieser Arbeitsgruppe einberufen.

(6) Weisungen an die Auftragsverarbeiterin werden im Einvernehmen mit den anderen gemeinsam Verantwortlichen gemäß dem unter Nummer 5 beschriebenen Entscheidungsprozess der Arbeitsgruppe von einer der Anlaufstellen der gemeinsam Verantwortlichen übermittelt. Der gemeinsam Verantwortliche, der die Weisung erteilt, übermittelt sie der Auftragsverarbeiterin schriftlich und informiert alle anderen gemeinsam Verantwortlichen darüber. Ist die betreffende Angelegenheit so zeitkritisch, dass eine Sitzung der Arbeitsgruppe gemäß Nummer 5 nicht mehr einberufen werden kann, so kann dennoch eine Weisung erteilt werden, die jedoch von der Arbeitsgruppe zurückgenommen werden kann. Diese Weisung sollte schriftlich erteilt werden, und alle anderen gemeinsam Verantwortlichen sollten zum Zeitpunkt der Erteilung der Anweisung darüber informiert werden.

(7) Durch die Einrichtung der Arbeitsgruppe gemäß Nummer 5 wird die Zuständigkeit eines gemeinsam Verantwortlichen nicht berührt, seine zuständige Aufsichtsbehörde gemäß den Artikeln 33 und 24 der Datenschutz-Grundverordnung zu unterrichten. Für diese Unterrichtung ist keine Zustimmung eines anderen gemeinsam Verantwortlichen erforderlich.

(8) Im Rahmen des Gateways des Vertrauensrahmens dürfen nur Personen, die von den benannten nationalen Behörden oder amtlichen Stellen dazu ermächtigt wurden, auf die ausgetauschten personenbezogenen Daten von Nutzern zugreifen.

(9) Jede ausstellende Behörde führt ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Der Status als gemeinsam Verantwortlicher kann in dem Verzeichnis angegeben werden.

Unterabschnitt 2

Zuständigkeiten und Funktionen bei der Bearbeitung von Anfragen/Anträgen und der Unterrichtung betroffener Personen

(1) In seiner Rolle als ausstellende Behörde informiert jeder Verantwortliche natürliche Personen, deren Zertifikat(e) er widerrufen hat, (im Folgenden die ‚betroffenen Personen') über diesen Widerruf und die Verarbeitung ihrer personenbezogenen Daten im Gateway für das digitale COVID-Zertifikat der EU zur Unterstützung des Austauschs von Widerrufslisten gemäß Artikel 14 der Datenschutz-Grundverordnung, außer wenn sich dies als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden wäre.

(2) Jeder Verantwortliche dient als Anlaufstelle für natürliche Personen, deren Zertifikat er widerrufen hat, und bearbeitet die von betroffenen Personen oder ihren Vertretern gestellten Anfragen/Anträge im Zusammenhang mit der Ausübung ihrer Rechte im Einklang mit der Datenschutz-Grundverordnung. Erhält ein gemeinsam Verantwortlicher eine Anfrage/einen Antrag einer betroffenen Person in Bezug auf ein Zertifikat, das von einem anderen gemeinsam Verantwortlichen ausgestellt wurde, teilt er der betroffenen Person die Identität und die Kontaktdaten dieses zuständigen gemeinsam Verantwortlichen mit. Auf Anfrage eines anderen gemeinsam Verantwortlichen unterstützen sich die gemeinsam Verantwortlichen gegenseitig bei der Bearbeitung von Anfragen/Anträgen betroffener Personen und antworten einander unverzüglich, spätestens jedoch innerhalb von 1 Monat nach Eingang eines Amtshilfeersuchens. Geht bei einem Verantwortlichen eine Anfrage/ein Antrag zu von einem Drittland übermittelten Daten ein, so bearbeitet der Verantwortliche die Anfrage/den Antrag und teilt der betroffenen Person die Identität und die Kontaktdaten der ausstellenden Behörde des Drittlands mit.

(3) Jeder Verantwortliche stellt den betroffenen Personen den Inhalt dieses Anhangs einschließlich der Bestimmungen der Nummern 1 und 2 zur Verfügung.

ABSCHNITT 2

Management von Sicherheitsvorfällen, einschließlich Verletzungen des Schutzes personenbezogener Daten

(1) Die gemeinsam Verantwortlichen unterstützen einander bei der Ermittlung und Behandlung von Sicherheitsvorfällen im Zusammenhang mit der Verarbeitung im Gateway für das digitale COVID-Zertifikat der EU, einschließlich Verletzungen des Schutzes personenbezogener Daten.

(2) Insbesondere teilen die gemeinsam Verantwortlichen einander Folgendes mit:

a) potenzielle oder tatsächliche Risiken für die Verfügbarkeit, Vertraulichkeit und/oder Integrität der personenbezogenen Daten, die im Gateway des Vertrauensrahmens verarbeitet werden;

b) jede Verletzung des Schutzes personenbezogener Daten, die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und die Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen sowie alle Maßnahmen, die ergriffen wurden, um gegen die Verletzung des Schutzes personenbezogener Daten vorzugehen und das Risiko für die Rechte und Freiheiten natürlicher Personen zu mindern;

c) jeden Verstoß gegen die technischen und/oder organisatorischen Vorkehrungen für die Verarbeitungsvorgänge im Gateway des Vertrauensrahmens.

(3) Die gemeinsam Verantwortlichen unterrichten die Kommission, die zuständigen Aufsichtsbehörden und, falls erforderlich, die betroffenen Personen im Einklang mit den Artikeln 33 und 34 der Datenschutz-Grundverordnung oder nach Mitteilung der Kommission über alle Verletzungen des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung im Gateway des Vertrauensrahmens.

(4) Jede ausstellende Behörde trifft geeignete technische und organisatorische Maßnahmen, um

a) die Verfügbarkeit, Integrität und Vertraulichkeit der gemeinsam verarbeiteten personenbezogenen Daten zu gewährleisten und zu schützen;

b) alle in ihrem Besitz befindlichen personenbezogenen Daten vor jeglicher unbefugten oder unrechtmäßigen Form der Verarbeitung, des Verlusts, der Verwendung, der Offenlegung, des Erwerbs oder Zugriffs zu schützen;

c) zu gewährleisten, dass der Zugriff auf die personenbezogenen Daten nicht an andere Personen als die Empfänger oder Auftragsverarbeiter weitergegeben oder gewährt wird.

ABSCHNITT 3

Datenschutzfolgenabschätzung

(1) Benötigt ein Verantwortlicher zur Erfüllung seiner Pflichten nach den Artikeln 35 und 36 der Verordnung (EU) 2016/679 Informationen von einem anderen Verantwortlichen, so übermittelt er eine besondere Anfrage an die in Abschnitt 1 Unterabschnitt 1 Nummer 4 genannte Funktions-Mailbox. Letzterer bemüht sich nach besten Kräften, diese Informationen zur Verfügung zu stellen."

ANHANG IV

„*ANHANG VII*

ZUSTÄNDIGKEITEN DER KOMMISSION FÜR DIE UNTERSTÜTZUNG DES AUSTAUSCHS VON EUDCC-WIDERRUFSLISTEN ALS AUFTRAGSVERARBEITERIN FÜR DAS GATEWAY FÜR DAS DIGITALE COVID-ZERTIFIKAT DER EU

Die Kommission

(1) schafft und gewährleistet im Auftrag der Mitgliedstaaten eine sichere und zuverlässige Kommunikationsinfrastruktur, die den Austausch der an das Gateway für das digitale COVID-Zertifikat der EU übermittelten Widerrufslisten unterstützt;

(2) kann Dritte als Unterauftragsverarbeiter beauftragen, um ihren Verpflichtungen als Auftragsverarbeiterin im Gateway des Vertrauensrahmens für die Mitgliedstaaten nachzukommen; die Kommission informiert die gemeinsam Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragsverarbeiter, wodurch die Verantwortlichen die Möglichkeit erhalten, gemeinsam gegen derartige Änderungen Einspruch zu erheben. Die Kommission stellt sicher, dass dieselben Datenschutzverpflichtungen, die in diesem Beschluss festgelegt sind, auch für diese Unterauftragsverarbeiter gelten;

(3) verarbeitet personenbezogene Daten nur auf dokumentierte Weisung der Verantwortlichen, es sei denn, dass eine Verarbeitung nach Unionsrecht oder nationalem Recht erfolgen muss; in einem solchen Fall teilt die Kommission den gemeinsam Verantwortlichen diese rechtliche Anforderung vor der Durchführung der Verarbeitungstätigkeit mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

verarbeitet die Daten wie folgt:

a) Authentifizierung nationaler Back-End-Server auf der Grundlage nationaler Back-End-Server-Zertifikate;

b) Empfang der in Artikel 5a Absatz 3 des Durchführungsbeschlusses genannten Daten von nationalen Back-End-Servern über eine von ihr bereitgestellte Anwendungsprogrammierschnittstelle, die es nationalen Back-End-Servern ermöglicht, die betreffenden Daten hochzuladen;

c) Speicherung der Daten im Gateway für das digitale COVID-Zertifikat der EU;

d) Bereitstellung der Daten zum Herunterladen durch nationale Back-End-Server;

e) Löschung der Daten an ihrem Ablaufdatum oder auf Anweisung des Verantwortlichen, der sie übermittelt hat;

f) Löschung aller verbleibenden Daten nach Beendigung der Leistung, es sei denn, das Unionsrecht oder das Recht der Mitgliedstaaten schreibt eine Speicherung der personenbezogenen Daten vor;

(4) trifft alle organisatorischen, physischen und logischen Sicherheitsmaßnahmen auf der Grundlage des aktuellen Stands der Technik, um das Gateway für das digitale COVID-Zertifikat der EU zu erhalten. Zu diesem Zweck wird die Kommission

a) eine für das Sicherheitsmanagement beim Gateway für das digitale COVID-Zertifikat der EU zuständige Stelle benennen, den gemeinsam Verantwortlichen deren Kontaktdaten mitteilen und deren Verfügbarkeit zur Reaktion auf Sicherheitsbedrohungen gewährleisten;

b) die Verantwortung für die Sicherheit des Gateways für das digitale COVID-Zertifikat der EU übernehmen, einschließlich regelmäßiger Prüfungen, Beurteilungen und Bewertungen der Sicherheitsmaßnahmen;

c) sicherstellen, dass alle Personen, denen der Zugriff auf das Gateway für das digitale COVID-Zertifikat der EU gewährt wird, vertraglichen, beruflichen oder gesetzlichen Vertraulichkeitsverpflichtungen unterliegen;

(5) trifft alle erforderlichen Sicherheitsmaßnahmen, damit das reibungslose Funktionieren der nationalen Back-End-Server nicht beeinträchtigt wird. Zu diesem Zweck richtet die Kommission besondere Verfahren für den Anschluss der Back-End-Server an das Gateway für das digitale COVID-Zertifikat der EU ein. Dies umfasst:

a) ein Verfahren zur Risikobewertung, um potenzielle Bedrohungen des Systems zu ermitteln und abzuschätzen;

b) ein Audit- und Überprüfungsverfahren

i) zur Überprüfung der Übereinstimmung der umgesetzten Sicherheitsmaßnahmen mit den geltenden Sicherheitsvorgaben;

ii) zur regelmäßigen Kontrolle der Integrität der Systemdateien, der Sicherheitsparameter und der erteilten Genehmigungen;

iii) zur Überwachung zwecks Feststellung von Sicherheitsverstößen und von unbefugtem Eindringen;

iv) zur Umsetzung von Änderungen zur Behebung bestehender Sicherheitslücken und

v) zur Festlegung der Bedingungen, unter denen — auch auf Anfrage der Verantwortlichen — unabhängige Audits einschließlich Inspektionen sowie Überprüfungen von Sicherheitsmaßnahmen im Einklang mit den Bedingungen des Protokolls (Nr. 7) zum AEUV über die Vorrechte und Befreiungen der Europäischen Union durchgeführt werden können und die Mitwirkung an diesen Audits und Überprüfungen zulässig ist;

c) ein Änderungskontrollverfahren, um die Auswirkungen einer Änderung vor ihrer Umsetzung zu dokumentieren und abzuschätzen und die gemeinsam Verantwortlichen über alle Änderungen auf dem Laufenden zu halten, die sich auf die Kommunikation mit ihren Infrastrukturen und/oder deren Sicherheit auswirken können;

d) die Festlegung eines Wartungs- und Reparaturverfahrens mit Regeln und Bedingungen für die Wartung und/oder Reparatur von Ausrüstungen;

e) die Festlegung eines Verfahrens in Bezug auf Sicherheitsvorfälle zur Festlegung des Melde- und Eskalationsprogramms, zur unverzüglichen Unterrichtung der Verantwortlichen über jegliche Verletzung des Schutzes personenbezogener Daten, unter anderem, damit diese die nationalen Datenschutzaufsichtsbehörden informieren können, sowie zur Festlegung eines Disziplinarverfahrens, um gegen Sicherheitsverletzungen vorzugehen;

(6) ergreift physische und/oder logische Sicherheitsmaßnahmen auf der Grundlage des aktuellen Stands der Technik für die Einrichtungen, in denen die Ausrüstung für das Gateway für das digitale COVID-Zertifikat der EU untergebracht ist, und für die Kontrollen der logischen Daten und der Zugriffssicherheit. Zu diesem Zweck wird die Kommission

a) die physische Sicherheit durchsetzen, um abgegrenzte Sicherheitsbereiche einzurichten und das Erkennen von Verstößen zu ermöglichen;

b) den Zugang zu den Einrichtungen kontrollieren und ein Besucherregister für Rückverfolgungszwecke führen;

c) sicherstellen, dass die externen Personen, denen Zugang zu den Räumlichkeiten gewährt wird, von entsprechend bevollmächtigten Mitarbeitern begleitet werden;

d) sicherstellen, dass Ausrüstungen nicht ohne Vorabgenehmigung durch die benannten zuständigen Stellen hinzugefügt, ersetzt oder entfernt werden können;

e) den beiderseitigen Zugriff auf nationale Back-End-Server und das Gateway des Vertrauensrahmens kontrollieren;

f) sicherstellen, dass Personen, die Zugriff auf das Gateway für das digitale COVID-Zertifikat der EU haben, identifiziert und authentifiziert werden;

g) die Rechte für den Zugriff auf das Gateway für das digitale COVID-Zertifikat der EU überprüfen, falls eine Sicherheitsverletzung in Bezug auf diese Infrastruktur eintritt;

h) die Integrität der über das Gateway für das digitale COVID-Zertifikat der EU übermittelten Informationen wahren;

i) technische und organisatorische Sicherheitsmaßnahmen umsetzen, um unbefugten Zugriff auf personenbezogene Daten zu verhindern;

j) bei Bedarf Maßnahmen zur Verhinderung des unbefugten Zugriffs auf das Gateway für das digitale COVID-Zertifikat der EU von der Netzdomäne der nationalen Behörden aus ergreifen (d. h. Sperrung eines Standorts/einer IP-Adresse);

(7) ergreift Maßnahmen zum Schutz ihrer Netzdomäne, einschließlich der Trennung von Anschlüssen, im Falle einer erheblichen Abweichung von den Qualitäts- oder Sicherheitsgrundsätzen und -konzepten;

(8) führt einen Risikomanagementplan in Bezug auf ihren Zuständigkeitsbereich;

(9) überwacht — in Echtzeit — die Leistung aller Dienstkomponenten ihrer Dienste für das Gateway des Vertrauensrahmens, erstellt regelmäßige Statistiken und führt Aufzeichnungen;

(10) leistet Unterstützung für alle Dienste des Gateways des Vertrauensrahmens in englischer Sprache rund um die Uhr über Telefon, E-Mail oder das Web-Portal und nimmt Anrufe von autorisierten Anrufern entgegen: von den Koordinatoren des Gateways für das digitale COVID-Zertifikat der EU und ihren jeweiligen Helpdesks, von Projektbeauftragten und benannten Mitarbeitern der Kommission;

(11) unterstützt, soweit dies gemäß Artikel 12 der Verordnung (EU) 2018/1725 möglich ist, die gemeinsam Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von deren Verpflichtung zur Bearbeitung von Anfragen/Anträgen in Bezug auf die Ausübung der Rechte der betroffenen Person gemäß Kapitel III der Datenschutz-Grundverordnung;

(12) unterstützt die gemeinsam Verantwortlichen durch die Bereitstellung von Informationen über das Gateway für das digitale COVID-Zertifikat der EU dabei, den Verpflichtungen gemäß den Artikeln 32, 33, 34, 35 und 36 der Datenschutz-Grundverordnung nachzukommen;

(13) stellt sicher, dass die im Gateway für das digitale COVID-Zertifikat der EU verarbeiteten Daten für Personen, die nicht zugriffsbefugt sind, unverständlich sind;

(14) ergreift alle erforderlichen Maßnahmen, damit die Betreiber des Gateways für das digitale COVID-Zertifikat der EU keinen unbefugten Zugriff auf übermittelte Daten haben;

(15) ergreift Maßnahmen, um die Interoperabilität und die Kommunikation zwischen den benannten Verantwortlichen des Gateways für das digitale COVID-Zertifikat der EU zu erleichtern;

(16) führt gemäß Artikel 31 Absatz 2 der Verordnung (EU) 2018/1725 ein Verzeichnis aller im Auftrag der gemeinsam Verantwortlichen durchgeführten Verarbeitungsvorgänge."