II

(Rechtsakte ohne Gesetzescharakter)

BESCHLÜSSE

DURCHFÜHRUNGSBESCHLUSS (EU) 2020/1023 DER KOMMISSION

vom 15. Juli 2020

zur Änderung des Durchführungsbeschlusses (EU) 2019/1765 hinsichtlich des grenzüberschreitenden Datenaustauschs zwischen nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung zwecks Bekämpfung der COVID-19-Pandemie

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung ([1]), insbesondere auf Artikel 14 Absatz 3,

in Erwägung nachstehender Gründe:

(1) Mit Artikel 14 der Richtlinie 2011/24/EU wurde die Union beauftragt, die Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten im Rahmen eines freiwilligen Netzwerks, mit dem die von den Mitgliedstaaten benannten, für elektronische Gesundheitsdienste zuständigen nationalen Behörden vernetzt werden, (im Folgenden „Netzwerk für elektronische Gesundheitsdienste“, auch „Gesundheitstelematiknetz“) zu unterstützen und zu erleichtern.

(2) Der Durchführungsbeschluss (EU) 2019/1765 der Kommission ([2]) enthält Vorschriften für die Errichtung, die Verwaltung und die Funktionsweise des Netzwerks der für elektronische Gesundheitsdienste zuständigen nationalen Behörden. Mit Artikel 4 des Beschlusses erhält das Netzwerk für elektronische Gesundheitsdienste den Auftrag, eine größere Interoperabilität der nationalen Informations- und Kommunikationstechnologiesysteme und die grenzüberschreitende Übertragbarkeit elektronischer Gesundheitsdaten im Rahmen der grenzüberschreitenden Gesundheitsversorgung zu fördern.

(3) Angesichts der durch die COVID-19-Pandemie verursachten Krise im Bereich der öffentlichen Gesundheit haben mehrere Mitgliedstaaten Mobil-Apps entwickelt, die die Kontaktnachverfolgung unterstützen und durch die ihre Nutzer gewarnt und so in die Lage versetzt werden, geeignete Maßnahmen wie Tests oder Selbstisolierung zu treffen, wenn sie durch den Aufenthalt in der Nähe eines anderen Nutzers solcher Apps, der eine positive Diagnose gemeldet hat, potenziell dem Virus ausgesetzt waren. Diese Apps verwenden die Bluetooth-Technologie, um in der Nähe befindliche Geräte zu erkennen. Angesichts der Aufhebung von Reisebeschränkungen zwischen den Mitgliedstaaten im Juni 2020 sollte darauf hingearbeitet werden, die Interoperabilität der nationalen Systeme der Informations- und Kommunikationstechnologie zwischen den am Netzwerk für elektronische Gesundheitsdienste teilnehmenden Mitgliedstaaten zu verbessern, indem eine digitale Infrastruktur eingerichtet wird, die die Interoperabilität zwischen den nationalen Mobil-Apps zur Kontaknachverfolgung und Warnung unterstützt.

([1]) ABl. L 88 vom 4.4.2011, S. 45.

([2]) Durchführungsbeschluss (EU) 2019/1765 der Kommission vom 22. Oktober 2019 mit Vorschriften für die Errichtung, die Verwaltung und die Funktionsweise des Netzwerks der für elektronische Gesundheitsdienste zuständigen nationalen Behörden und zur Aufhebung des Durchführungsbeschlusses 2011/890/EU (ABl. L 270 vom 24.10.2019, S. 83).

(4) Die Kommission hat die Mitgliedstaaten in Bezug auf die oben genannten Mobil-Apps unterstützt. Am 8. April 2020 nahm sie eine Empfehlung für ein gemeinsames Instrumentarium der Union für den Einsatz von Technik und Daten zur Bekämpfung und Überwindung der COVID-19-Krise, insbesondere im Hinblick auf Mobil-Apps und die Verwendung anonymisierter Mobilitätsdaten ([3]), an (im Folgenden „Kommissionsempfehlung"). Die am Netzwerk für elektronische Gesundheitsdienste teilnehmenden Mitgliedstaaten haben mit Unterstützung der Kommission ein gemeinsames für die Mitgliedstaaten bestimmtes EU-Instrumentarium für Mobil-Apps zur Unterstützung der Kontaktnachverfolgung ([4]) sowie Interoperabilitätsleitlinien für zugelassene Mobil-Apps zur Kontaknachverfolgung in der EU ([5]) angenommen. Das Instrumentarium bietet Erläuterungen zu den nationalen Anforderungen an nationale Mobil-Apps zur Kontaknachverfolgung und Warnung, insbesondere, dass sie auf Freiwilligkeit basieren sollten, von der jeweiligen nationalen Gesundheitsbehörde zugelassen sein sollten, die Privatsphäre wahren und sie entfernt werden sollten, sobald sie nicht mehr benötigt werden. Nach den jüngsten Entwicklungen der COVID-19-Krise haben sowohl die Kommission ([6]) als auch der Europäische Datenschutzausschuss ([7]) Datenschutz-Leitlinien zu Mobil-Apps und Instrumenten zur Kontaktnachverfolgung herausgegeben. Das Design der Mobil-Apps der Mitgliedstaaten und der digitalen Interoperabilitätsinfrastruktur baut auf dem gemeinsamen EU-Instrumentarium, den oben genannten Leitlinien und den im Netzwerk für elektronische Gesundheitsdienste vereinbarten technischen Spezifikationen auf.

(5) Um die Interoperabilität nationaler Mobil-Apps zur Kontaktnachverfolgung und Warnung zu erleichtern, haben die am Netzwerk für elektronische Gesundheitsdienste teilnehmenden Mitgliedstaaten nach ihrem Beschluss, ihre Zusammenarbeit in diesem Bereich auf freiwilliger Basis voranzubringen, mit Unterstützung der Kommission eine digitale Infrastruktur als IT-Tool für den Austausch von Daten entwickelt. Diese digitale Infrastruktur wird als *Federation Gateway* bezeichnet.

(6) In diesem Beschluss werden Bestimmungen über die Rolle der teilnehmenden Mitgliedstaaten und der Kommission beim Betreiben des *Federation Gateway* für die grenzüberschreitende Interoperabilität nationaler Mobil-Apps zur Kontaktnachverfolgung und Warnung festgelegt.

(7) Die Verarbeitung personenbezogener Daten der Nutzer von Mobil-Apps zur Kontaktnachverfolgung und Warnung, die unter der Verantwortung der Mitgliedstaaten oder anderer öffentlicher Organisationen oder Stellen in den Mitgliedstaaten erfolgt, sollte im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([8]) (im Folgenden „Datenschutz-Grundverordnung") und der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([9]) durchgeführt werden. Die Verarbeitung personenbezogener Daten unter der Verantwortung der Kommission zum Zweck der Verwaltung und zur Gewährleistung der Sicherheit des *Federation Gateway* sollte im Einklang mit der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([10]) erfolgen.

(8) Das *Federation Gateway* sollte aus einer sicheren IT-Infrastruktur bestehen, die eine gemeinsame Schnittstelle bietet, über die benannte nationale Behörden oder amtliche Stellen einen Mindestdatensatz in Bezug auf Kontakte mit SARS-CoV-2-infizierten Personen austauschen können, um andere über ihre potenzielle Exposition gegenüber dieser Infektion zu informieren, und die eine wirksame Zusammenarbeit im Gesundheitsbereich zwischen den Mitgliedstaaten fördert, indem der Austausch einschlägiger Informationen erleichtert wird.

(9) In diesem Beschluss sollten daher die Modalitäten für den grenzüberschreitenden Datenaustausch zwischen benannten nationalen Behörden oder amtlichen Stellen über das *Federation Gateway* innerhalb der EU festgelegt werden.

([3]) Empfehlung (EU) 2020/518 der Kommission vom 8. April 2020 für ein gemeinsames Instrumentarium der Union für den Einsatz von Technik und Daten zur Bekämpfung und Überwindung der COVID-19-Krise, insbesondere im Hinblick auf Mobil-Apps und die Verwendung anonymisierter Mobilitätsdaten (ABl. L 114 vom 14.4.2020, S. 7).

([4]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_de.pdf

([5]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

([6]) Mitteilung der Kommission — Leitlinien zum Datenschutz bei Mobil-Apps zur Unterstützung der Bekämpfung der COVID-19-Pandemie (ABl. C 124 I vom 17.4.2020, S. 1).

([7]) Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 sowie Erklärung des EDSA vom 16. Juni 2020 zu den datenschutzrechtlichen Auswirkungen der Interoperabilität von Kontaktnachverfolgungsapps, beides abrufbar unter: https://edpb.europa.eu.

([8]) 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).

([9]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

([10]) 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).

(10) Die teilnehmenden Mitgliedstaaten, vertreten durch die benannten nationalen Behörden oder amtlichen Stellen, legen gemeinsam den Zweck der und die Mittel zur Verarbeitung personenbezogener Daten über das *Federation Gateway* fest und sind daher gemeinsam Verantwortliche. Artikel 26 der Datenschutz-Grundverordnung 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 Aufgaben durch Rechtsvorschriften der Union oder der Mitgliedstaaten festgelegt werden, denen die Verantwortlichen unterliegen. Jeder Verantwortliche sollte sicherstellen, dass er auf nationaler Ebene über eine Rechtsgrundlage für die Verarbeitung im *Federation Gateway* verfügt.

(11) Die Kommission, die technische und organisatorische Lösungen für das *Federation Gateway* bereitstellt, verarbeitet im Namen der am *Federation Gateway* als gemeinsam Verantwortliche teilnehmenden Mitgliedstaaten pseudonymisierte personenbezogene Daten und ist daher Auftragsverarbeiterin. Gemäß Artikel 28 der Datenschutz-Grundverordnung 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. Dieser Beschluss enthält Vorschriften für die Verarbeitung durch die Kommission als Auftragsverarbeiterin.

(12) Bei der Verarbeitung personenbezogener Daten im Rahmen des *Federation Gateway* ist die Kommission an den Beschluss (EU, Euratom) 2017/46 der Kommission ([11]) gebunden.

(13) Da die Zwecke, für die die Verantwortlichen personenbezogene Daten in den nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung verarbeiten, nicht unbedingt die Identifizierung einer betroffenen Person erfordern, sind die Verantwortlichen möglicherweise nicht immer in der Lage, die Anwendung der Rechte der betroffenen Personen zu gewährleisten. Die in den Artikeln 15 bis 20 der Datenschutz-Grundverordnung genannten Rechte finden daher gegebenenfalls keine Anwendung, wenn die Bedingungen gemäß Artikel 11 der genannten Verordnung erfüllt sind.

(14) Es ist erforderlich, den bestehenden Anhang des Durchführungsbeschlusses (EU) 2019/1765 aufgrund der Aufnahme von zwei neuen Anhängen neu zu nummerieren.

(15) Der Durchführungsbeschluss (EU) 2019/1765 sollte daher entsprechend geändert werden.

(16) Angesichts der Dringlichkeit der Lage infolge der COVID-19-Pandemie sollte dieser Beschluss am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft treten.

(17) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 angehört und hat am 9. Juli 2020 eine Stellungnahme abgegeben.

(18) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 16 der Richtlinie 2011/24/EU eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Der Durchführungsbeschluss (EU) 2019/1765 wird wie folgt geändert:

1. In Artikel 2 Absatz 1 werden die folgenden Buchstaben g, h, i, j, k, l, m, n und o eingefügt:

„g) ‚App-Nutzer' eine Person, die im Besitz eines intelligenten Geräts ist und eine zugelassene Mobil-App zur Kontaktnachverfolgung und Warnung heruntergeladen hat und verwendet;

h) ‚Kontaktnachverfolgung' Maßnahmen zur Nachverfolgung von Personen, die der Quelle einer schwerwiegenden grenzüberschreitenden Gesundheitsbedrohung im Sinne von Artikel 3 Buchstabe c des Beschlusses Nr. 1082/2013/EU des Europäischen Parlaments und des Rates (*) ausgesetzt waren;

([11]) Beschluss (EU, Euratom) 2017/46 der Kommission vom 10. Januar 2017 über die Sicherheit von Kommunikations- und Informationssystemen in der Europäischen Kommission (ABl. L 6 vom 11.1.2017, S. 40). 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.

i) ‚nationale Mobil-App zur Kontaktnachverfolgung und Warnung' eine auf nationaler Ebene zugelassene Softwareanwendung, die in intelligenten Geräten, insbesondere in Smartphones, läuft und in der Regel für eine vielfältige und gezielte Interaktion mit Webressourcen konzipiert ist, über die die von vielen in intelligenten Geräten vorhandenen Sensoren erfassten Näherungsdaten und andere kontextbezogene Informationen zu dem Zweck verarbeitet werden, Kontakte mit Personen zu ermitteln, die mit SARS-CoV-2 infiziert sind, und Personen zu warnen, die möglicherweise SARS-CoV-2 ausgesetzt waren. Diese Mobil-Apps sind in der Lage, andere Bluetooth verwendende Geräte in der Nähe zu erkennen und Informationen mit Back-End-Servern über das Internet auszutauschen;

j) ‚*Federation Gateway*' ein von der Kommission mithilfe eines gesicherten IT-Tools betriebenes Netzwerk-Gateway, das einen Mindestsatz personenbezogener Daten von den Back-End-Servern der Mitgliedstaaten empfängt, speichert und zur Verfügung stellt, um die Interoperabilität der nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung zu gewährleisten;

k) ‚Schlüssel' eine eindeutige kurzlebige Kennung für einen App-Nutzer, der meldet, mit SARS-CoV-2 infiziert zu sein oder möglicherweise SARS-CoV-2 ausgesetzt gewesen zu sein;

l) ‚Infektionsverifizierung' die zur Bestätigung einer Infektion mit SARS-CoV-2 verwendete Methode, d. h. Eigenmeldung durch den App-Nutzer oder Bestätigung durch eine nationale Gesundheitsbehörde oder einen Labortest;

m) ‚relevante Länder' den Mitgliedstaat oder die Mitgliedstaaten, in dem bzw. denen sich ein App-Nutzer in den 14 Tagen vor dem Datum des Hochladens der Schlüssel aufgehalten hat, die zugelassene Mobil-App zur Kontaktnachverfolgung und Warnung heruntergeladen hat sowie in den bzw. in die er gereist ist;

n) ‚Ursprungsland der Schlüssel' den Mitgliedstaat, in dem sich der Back-End-Server befindet, der die Schlüssel in das *Federation Gateway* hochgeladen hat;

o) ‚Protokolldaten' eine automatische Aufzeichnung eines Vorgangs im Zusammenhang mit dem Austausch von über das *Federation Gateway* verarbeiteten Daten und den Zugriff darauf, aus der insbesondere die Art der Verarbeitung, das Datum und die Uhrzeit der Verarbeitung sowie die Kennung der Person, die die Daten verarbeitet, hervorgehen.

_____

(*) Beschluss Nr. 1082/2013/EU des Europäischen Parlaments und des Rates vom 22. Oktober 2013 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung der Entscheidung Nr. 2119/98/EG (ABl. L 293 vom 5.11.2013, S. 1)."

2. In Artikel 4 Absatz 1 wird folgender Buchstabe h eingefügt:

„h) Bereitstellung von Leitlinien für die Mitgliedstaaten zum grenzüberschreitenden Austausch personenbezogener Daten über das *Federation Gateway* zwischen nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung."

3. In Artikel 6 Absatz 1 werden die folgenden Buchstaben f und g eingefügt:

„f) entwickelt geeignete technische und organisatorische Maßnahmen in Bezug auf die Sicherheit der Übermittlung und Bereithaltung personenbezogener Daten im *Federation Gateway* für die Zwecke der grenzüberschreitenden Interoperabilität nationaler Mobil-Apps zur Kontaktnachverfolgung und Warnung, führt diese durch und erhält sie aufrecht;

g) unterstützt das Netzwerk für elektronische Gesundheitsdienste bei der Einigung über die Einhaltung der technischen und organisatorischen Anforderungen an den grenzüberschreitenden Austausch personenbezogener Daten im *Federation Gateway* seitens der nationalen Behörden, indem sie die erforderlichen Tests und Audits bereitstellt und durchführt. Experten der Mitgliedstaaten können die Auditoren der Kommission unterstützen."

4. Artikel 7 wird wie folgt geändert:

a) Der Titel erhält folgende Fassung: „Schutz personenbezogener Daten, die über die digitale eHealth-Service-Infrastruktur verarbeitet werden";

b) in Absatz 2 wird das Wort „Anhang" durch „Anhang I" ersetzt.

5. Folgender Artikel 7a wird eingefügt:

„*Artikel 7a*

Grenzüberschreitender Datenaustausch zwischen nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung über das *Federation Gateway*

(1) Werden personenbezogene Daten über das *Federation Gateway* ausgetauscht, so beschränkt sich die Verarbeitung auf die Ermöglichung der Interoperabilität nationaler Mobil-Apps zur Kontaktnachverfolgung und Warnung im *Federation Gateway* sowie der Kontinuität der Ermittlung von Kontaktpersonen in einem grenzüberschreitenden Kontext.

(2) Die in Absatz 3 genannten personenbezogenen Daten werden dem *Federation Gateway* in einem pseudonymisierten Format übermittelt.

(3) Die pseudonymisierten personenbezogenen Daten, die über das *Federation Gateway* ausgetauscht und darin verarbeitet werden, dürfen nur folgende Informationen enthalten:

a) die Schlüssel, die bis zu 14 Tage vor dem Datum des Hochladens der Schlüssel von den nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung übermittelt wurden;

b) Protokolldaten zu den Schlüsseln gemäß den technischen Spezifikationen, die im Ursprungsland der Schlüssel verwendet werden;

c) die Verifizierung der Infektion;

d) die relevanten Länder und das Ursprungsland der Schlüssel.

(4) Die benannten nationalen Behörden oder amtlichen Stellen, die personenbezogene Daten im *Federation Gateway* verarbeiten, sind gemeinsam Verantwortliche für die im *Federation Gateway* verarbeiteten Daten. Die Zuständigkeiten der gemeinsam Verantwortlichen sind in Anhang II geregelt. Jeder Mitgliedstaat, der am grenzüberschreitenden Datenaustausch zwischen nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung teilnehmen möchte, teilt der Kommission im Vorfeld seine Absicht mit und gibt die nationale Behörde oder amtliche Stelle an, die als Verantwortliche benannt wurde.

(5) Die Kommission ist die Auftragsverarbeiterin der personenbezogenen Daten, die im *Federation Gateway* verarbeitet werden. In ihrer Eigenschaft als Auftragsverarbeiterin gewährleistet die Kommission die Sicherheit der Verarbeitung personenbezogener Daten im *Federation Gateway*, einschließlich ihrer Übermittlung und Bereithaltung, und nimmt die in Anhang III festgelegten Zuständigkeiten eines Auftragsverarbeiters wahr.

(6) Die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten im *Federation Gateway* wird von der Kommission und den zum Zugriff auf das *Federation Gateway* befugten nationalen Behörden regelmäßig geprüft, beurteilt und bewertet.

(7) Unbeschadet der Entscheidung der gemeinsamen Verantwortlichen, die Verarbeitung im *Federation Gateway* zu beenden, wird das Federation Gateway spätestens 14 Tage, nachdem alle verbundenen nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung die Übermittlung von Schlüsseln über das *Federation Gateway* eingestellt haben, deaktiviert."

6. Der bisherige Anhang wird zu Anhang I.

7. Die Anhänge II und III werden im Wortlaut des Anhangs des vorliegenden Beschlusses angefügt.

Artikel 2

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

Brüssel, den 15. Juli 2020

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG

Im Durchführungsbeschluss (EU) 2019/1765 werden die folgenden Anhänge II und III angefügt:

„*ANHANG II*

ZUSTÄNDIGKEITEN DER TEILNEHMENDEN MITGLIEDSTAATEN ALS GEMEINSAM VERANTWORTLICHE FÜR DAS *FEDERATION GATEWAY* ZUR GRENZÜBERSCHREITENDEN DATENVERARBEITUNG ZWISCHEN NATIONALEN MOBIL-APPS ZUR KONTAKTNACHVERFOLGUNG UND WARNUNG

ABSCHNITT 1

Unterabschnitt 1

Verteilung der Zuständigkeiten

1. Die gemeinsam Verantwortlichen verarbeiten personenbezogene Daten über das *Federation Gateway* (Datenabgleichstelle) im Einklang mit den vom Netzwerk für elektronische Gesundheitsdienste festgelegten technischen Spezifikationen ([1]).

2. Jeder Verantwortliche ist dafür verantwortlich, dass die Verarbeitung personenbezogener Daten im *Federation Gateway* im Einklang mit der Datenschutz-Grundverordnung und der Richtlinie 2002/58/EG erfolgt.

3. Jeder Verantwortliche richtet eine Anlaufstelle mit einem Funktionspostfach ein, das der Kommunikation zwischen den gemeinsam Verantwortlichen und zwischen den gemeinsam Verantwortlichen und dem Auftragsverarbeiter dient.

4. Eine vom Netzwerk für elektronische Gesundheitsdienste gemäß Artikel 5 Absatz 4 eingesetzte nichtständige Untergruppe wird damit beauftragt, alle Fragen zu prüfen, die sich in Bezug auf die Interoperabilität der nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung und auf die gemeinsame Verantwortlichkeit für die Verarbeitung der personenbezogenen Daten ergeben, sowie an der Erstellung koordinierter Weisungen für die Kommission als Auftragsverarbeiterin mitzuwirken. Unter anderem können die Verantwortlichen im Rahmen der nichtständigen Untergruppe auf einen gemeinsamen Ansatz für die Vorratsspeicherung von Daten in ihren nationalen Back-End-Servern hinarbeiten, wobei die im *Federation Gateway* festgelegte Speicherfrist zu berücksichtigen ist.

5. Weisungen für die Auftragsverarbeiterin werden im Einvernehmen mit den anderen gemeinsam Verantwortlichen in der oben genannten Untergruppe von der Anlaufstelle eines gemeinsam Verantwortlichen übermittelt.

6. Nur Personen, die von den benannten nationalen Behörden oder amtlichen Stellen dazu ermächtigt wurden, dürfen auf die über das *Federation Gateway* ausgetauschten personenbezogenen Daten von Nutzern zugreifen.

7. Jede benannte nationale Behörde oder amtliche Stelle verliert ab dem Tag, an dem sie ihre Teilnahme am *Federation Gateway* zurückzieht, ihre Funktion als gemeinsam Verantwortliche. Sie bleibt jedoch für die vor dem Rückzug erfolgte Verarbeitung im *Federation Gateway* verantwortlich.

Unterabschnitt 2

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

1. Jeder Verantwortliche stellt den Nutzern der jeweiligen nationalen Mobil-App zur Kontaktnachverfolgung und Warnung (im Folgenden ‚betroffene Personen') im Einklang mit den Artikeln 13 und 14 der Datenschutz-Grundverordnung Informationen über die Verarbeitung ihrer personenbezogenen Daten im *Federation Gateway* für die Zwecke der grenzüberschreitenden Interoperabilität der nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung zur Verfügung.

2. Jeder Verantwortliche dient als Anlaufstelle für die Nutzer der jeweiligen nationalen Mobil-App zur Kontaktnachverfolgung und Warnung und bearbeitet die von diesen Nutzern oder ihren Vertretern gestellten Anfragen/Anträge im Zusammenhang mit der Ausübung der Rechte betroffener Personen im Einklang mit der Datenschutz-Grundverordnung. Jeder Verantwortliche bestimmt eine spezielle Anlaufstelle für Anfragen/Anträge von betroffenen Personen. Erhält ein gemeinsam Verantwortlicher eine Anfrage/einen Antrag einer betroffenen Person, die/der nicht seiner Zuständigkeit unterliegt, so leitet er sie/ihn umgehend an den zuständigen gemeinsam Verantwortlichen weiter. Auf Anfrage unterstützen sich die gemeinsam Verantwortlichen gegenseitig bei der Bearbeitung von Anfragen/Anträgen betroffener Personen und antworten einander unverzüglich, spätestens jedoch innerhalb von 15 Tagen nach Eingang eines Amtshilfeersuchens.

([1]) Insbesondere die Interoperabilitätsspezifikationen für den Abgleich grenzüberschreitender Übertragungsketten zwischen zugelassenen Apps vom 16. Juni 2020, abrufbar unter: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0

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 sich gegenseitig bei der Ermittlung und Behandlung von Sicherheitsvorfällen, einschließlich Verletzungen des Schutzes personenbezogener Daten, im Zusammenhang mit der Verarbeitung im *Federation Gateway*.

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 *Federation Gateway* verarbeitet werden;

b) Sicherheitsvorfälle, die mit der Verarbeitung im *Federation Gateway* in Verbindung stehen;

c) 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;

d) jeden Verstoß gegen die technischen und/oder organisatorischen Vorkehrungen für die Verarbeitungsvorgänge im *Federation Gateway*.

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 Verordnung (EU) 2016/679 oder nach Mitteilung der Kommission über alle Verletzungen des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung im *Federation Gateway*.

ABSCHNITT 3

Datenschutzfolgenabschätzungen

Benötigt ein Verantwortlicher zur Erfüllung seiner Pflichten nach den Artikeln 35 und 36 der Datenschutz-Grundverordnung Informationen von einem anderen Verantwortlichen, so übermittelt er eine besondere Anfrage an das in Abschnitt 1 Unterabschnitt 1 Nummer 3 genannte Funktionspostfach. Letzterer bemüht sich nach besten Kräften, diese Informationen zur Verfügung zu stellen.

ANHANG III

ZUSTÄNDIGKEITEN DER KOMMISSION ALS AUFTRAGSVERARBEITERIN FÜR DAS *FEDERATION GATEWAY* ZUR GRENZÜBERSCHREITENDEN DATENVERARBEITUNG ZWISCHEN NATIONALEN MOBIL-APPS ZUR KONTAKTNACHVERFOLGUNG UND WARNUNG

Die Kommission:

1. schafft und gewährleistet eine sichere und zuverlässige Kommunikationsinfrastruktur, die die nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung der am *Federation Gateway* teilnehmenden Mitgliedstaaten miteinander verbindet. Um ihren Verpflichtungen als Auftragsverarbeiterin im *Federation Gateway* nachzukommen, kann die Kommission Dritte als Unterauftragsverarbeiter beauftragen; die Kommission unterrichtet die gemeinsam Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Beauftragung oder Ersetzung anderer Auftragsverarbeiter und gibt dabei den Verantwortlichen gemäß Anhang II Abschnitt 1 Unterabschnitt 1 Nummer 4 die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben. Die Kommission stellt sicher, dass dieselben Datenschutzverpflichtungen, wie sie in diesem Beschluss festgelegt sind, auch für diese Unterauftragsverarbeiter gelten;
2. 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 Verantwortlichen diese rechtliche Anforderung vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
3. verarbeitet die Daten wie folgt:

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

b) Empfang der in Artikel 7a 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 *Federation Gateway* nach dem Empfang von den nationalen Back-End-Servern;

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

e) Löschung der Daten, sobald alle teilnehmenden Back-End-Server sie heruntergeladen haben, oder 14 Tage nach ihrem Empfang, wobei der frühere der beiden Zeitpunkte gilt;

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

Die Auftragsverarbeiterin trifft die zur Wahrung der Integrität der verarbeiteten Daten erforderlichen Maßnahmen;

4. trifft alle organisatorischen, physischen und logischen Sicherheitsmaßnahmen auf Grundlage des aktuellen Stands der Technik, um das *Federation Gateway* aufrechtzuerhalten. Zu diesem Zweck wird die Kommission:

a) eine für das Sicherheitsmanagement beim *Federation Gateway* zuständige Stelle benennen, den Verantwortlichen deren Kontaktdaten mitteilen und deren Verfügbarkeit zur Reaktion auf Sicherheitsbedrohungen gewährleisten;

b) die Verantwortung für die Sicherheit des *Federation Gateway* übernehmen;

c) sicherstellen, dass alle Personen, denen der Zugriff auf das *Federation Gateway* 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 *Federation Gateway* ein. Dazu gehören:

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 Ermöglichung — auch auf Anfrage der Verantwortlichen — und zur Mitwirkung an der Durchführung unabhängiger Audits, einschließlich Inspektionen, sowie von Überprüfungen von Sicherheitsmaßnahmen im Einklang mit den Bedingungen des Protokolls (Nr. 7) zum AEUV über die Vorrechte und Befreiungen der Europäischen Union ([2]);

([2]) Protokoll (Nr. 7) über die Vorrechte und Befreiungen der Europäischen Union (ABl. C 326 vom 26.10.2012, S. 266).

c) ein Änderungskontrollverfahren, um die Auswirkungen einer Änderung vor ihrer Umsetzung zu dokumentieren und abzuschätzen und die 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 sowie des Europäischen Datenschutzbeauftragten über jegliche Verletzung des Schutzes personenbezogener Daten sowie zur Festlegung eines Disziplinarverfahrens, um gegen Sicherheitsverletzungen vorzugehen;

6. ergreift physische und/oder logische Sicherheitsmaßnahmen auf Grundlage des aktuellen Stands der Technik für die Einrichtungen, in denen die Ausrüstung für das *Federation Gateway* 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 ohne Vorabgenehmigung durch die benannten zuständigen Stellen nicht hinzugefügt, ersetzt oder entfernt werden können;

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

f) sicherstellen, dass Personen, die Zugriff auf das *Federation Gateway* haben, identifiziert und authentifiziert werden;

g) die Rechte für den Zugriff auf das *Federation Gateway* überprüfen, falls eine Sicherheitsverletzung in Bezug auf diese Infrastruktur eintritt;

h) die Integrität der über das *Federation Gateway* 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 *Federation Gateway* 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 ihres *Federation Gateways*, erstellt regelmäßige Statistiken und führt Aufzeichnungen;

10. leistet Unterstützung für alle Dienste des *Federation Gateways* 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 *Federation Gateways* und ihren jeweiligen Helpdesks, von Projektbeauftragten und benannten Mitarbeitern der Kommission;

11. unterstützt, soweit dies möglich ist, die Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung ihrer 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 Verantwortlichen durch die Bereitstellung von Informationen über das *Federation Gateway* dabei, den Verpflichtungen gemäß den Artikeln 32, 35 und 36 der Datenschutz-Grundverordnung nachzukommen;

13. stellt sicher, dass die im *Federation Gateway* verarbeiteten Daten für Personen, die nicht zugriffsbefugt sind, unverständlich sind;

14. ergreift alle erforderlichen Maßnahmen, damit die Betreiber des *Federation Gateways* keinen unbefugten Zugriff auf übermittelte Daten haben;

15. ergreift Maßnahmen, um die Interoperabilität und die Kommunikation zwischen den benannten Verantwortlichen des *Federation Gateway* zu erleichtern;

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