II

(Mitteilungen)

MITTEILUNGEN DER ORGANE, EINRICHTUNGEN UND SONSTIGEN STELLEN DER EUROPÄISCHEN UNION

EUROPÄISCHE KOMMISSION

MITTEILUNG DER KOMMISSION

Leitlinien zum Datenschutz bei Mobil-Apps zur Unterstützung der Bekämpfung der COVID-19-Pandemie

(2020/C 124 I/01)

1 KONTEXT

Angesichts der COVID-19-Pandemie stehen die Union und die Mitgliedstaaten vor einer beispiellosen Herausforderung für ihre Gesundheitssysteme, ihre Lebensweise, ihre wirtschaftliche Stabilität und ihre Werte. Digitalen Technologien und Daten kommt bei der Bekämpfung der COVID-19-Krise eine wichtige Rolle zu. Normalerweise auf Smartphones installierte Mobil-Apps können den Gesundheitsbehörden auf nationaler und EU-Ebene eine Hilfe bei der Beobachtung und Eindämmung der COVID-19-Pandemie sein. Besonders relevant sind sie in der Phase der Aufhebung der Eindämmungsmaßnahmen. Über diese Apps kann den Bürgern unmittelbar Orientierungshilfe vermittelt werden, und sie können bei den Bemühungen zur Nachverfolgung von Kontakten hilfreich sein. In einer Reihe von Ländern, sowohl innerhalb der EU als auch weltweit, haben nationale oder regionale Behörden oder Entwickler die Einführung von Apps mit unterschiedlichen Funktionen angekündigt, mit denen die Bekämpfung des Virus unterstützt werden soll.

Am 8. April 2020 nahm die Kommission 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 ([1]) (im Folgenden „Empfehlung“) an. Die Empfehlung zielt unter anderem auf ein gemeinsames europäisches Konzept (ein Instrumentarium) zur Nutzung von Mobil-Apps ab, damit die Bürger in die Lage versetzt werden, wirksame Vorkehrungen zur sozialen Distanzierung zu treffen. Ferner sollen die Warnung, die Prävention und die Nachverfolgung von Kontakten ermöglicht werden, um zur Eindämmung der Ausbreitung der COVID-19-Erkrankung beizutragen. Die Empfehlung enthält die allgemeinen Grundsätze, an denen sich die Entwicklung eines solchen Instrumentariums orientieren sollte; des Weiteren wird darauf hingewiesen, dass die Kommission weitere Leitlinien veröffentlichen wird, unter anderem zu den Auswirkungen der Nutzung von Apps auf den Schutz personenbezogener Daten und den Schutz der Privatsphäre in diesem Bereich.

Mit dem gemeinsamen europäischen Fahrplan für die Aufhebung der Maßnahmen zur Eindämmung des Coronavirus hat die Kommission in Zusammenarbeit mit dem Präsidenten des Europäischen Rates eine Reihe von Grundsätzen festgelegt, an denen sich die schrittweise Einstellung der aufgrund des Ausbruchs von COVID-19 erlassenen Eindämmungsmaßnahmen orientieren soll. Mobil-Apps, auch solche mit Kontaktnachverfolgungsfunktionen, können in diesem Zusammenhang eine wichtige Rolle spielen. Je nach den Merkmalen der Apps und deren Nutzung in der Bevölkerung lassen sich mit diesen Anwendungen Diagnose, Behandlung und Handhabung von COVID-19-Fällen innerhalb und außerhalb von Krankenhäusern wesentlich beeinflussen. Besonders relevant sind die Apps, wenn Eindämmungsmaßnahmen aufgehoben werden und das Infektionsrisiko zunimmt, da immer mehr Menschen miteinander in Kontakt kommen. Die Apps können dazu beitragen, Infektionsketten schneller und effizienter zu unterbrechen als allgemeine Eindämmungsmaßnahmen, und verringern möglicherweise das Risiko einer Ausbreitung des Virus erheblich. Sie sollten daher ein wichtiges Element der Strategie zur Überwindung der Pandemie bilden und andere Maßnahmen wie die Erhöhung der Testkapazitäten ergänzen. ([2]) Eine wichtige Voraussetzung für die Entwicklung und Akzeptanz solcher Apps sowie für die konkrete Nutzung durch Privatpersonen ist Vertrauen. Die Menschen müssen sicher sein können, dass die Einhaltung der Grundrechte gewährleistet ist, dass die Apps nur für die spezifisch festgelegten Zwecke und nicht zur Massenüberwachung eingesetzt werden und dass die betroffenen Personen die Kontrolle über ihre Daten behalten. Darauf beruht die Präzision und Wirksamkeit solcher Apps bei der Eindämmung der Ausbreitung des Virus. Daher ist es von

([1]) Empfehlung C(2020) 2296 final vom 8. April 2020 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.
([2]) https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

entscheidender Bedeutung, Lösungen zu finden, die am wenigsten in die Privatsphäre eingreifen und den Anforderungen des EU-Rechts an den Schutz personenbezogener Daten und den Schutz der Privatsphäre in vollem Umfang entsprechen. Darüber hinaus sollten die Apps spätestens dann deaktiviert werden, wenn die Pandemie als unter Kontrolle gebracht erklärt worden ist. Ferner sollte die Apps Vorrichtungen zum Schutz der Informationssicherheit auf dem neuesten Stand enthalten.

Diese Leitlinien berücksichtigen den Beitrag des Europäischen Datenschutzausschusses (EDSA) ([3]) sowie die Erörterungen innerhalb des Netzwerks für elektronische Gesundheitsdienste. Der Ausschuss plant, in den kommenden Tagen Leitlinien zur Geolokalisierung und zu anderen Instrumenten zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 zu veröffentlichen.

Anwendungsbereich der Leitlinien

Um ein kohärentes Vorgehen in der gesamten EU zu gewährleisten und den Mitgliedstaaten und den App-Entwicklern Leitlinien an die Hand zu geben, werden in diesem Dokument die Merkmale und Anforderungen dargelegt, denen Apps gerecht werden sollten, damit die EU-Rechtsvorschriften zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten, insbesondere der Datenschutz-Grundverordnung (DSGVO) ([4]) und der Datenschutzrichtlinie für elektronische Kommunikation ([5]), eingehalten werden. Diese Leitlinien befassen sich nicht mit weiteren Bedingungen, etwa Beschränkungen, die Mitgliedstaaten im Hinblick auf die Verarbeitung von Gesundheitsdaten in ihre nationalen Rechtsvorschriften aufgenommen haben könnten.

Die Leitlinien sind rechtlich nicht bindend. Sie lassen die Rolle des Gerichtshofs der Europäischen Union, der als einziges Organ die verbindliche Auslegung des EU-Rechts vornehmen kann, unberührt.

Die vorliegenden Leitlinien beziehen sich nur auf Anwendungen zur Unterstützung der Bekämpfung der COVID-19-Pandemie, die ohne Zwang eingesetzt werden (Apps, die von Einzelpersonen auf freiwilliger Basis heruntergeladen, installiert und genutzt werden) und eine oder mehrere der folgenden Funktionen aufweisen:

— Bereitstellung präziser Informationen über die COVID-19-Pandemie für Einzelpersonen,

— Bereitstellung von Fragebögen zur Selbstbewertung und als Orientierungshilfe für Einzelpersonen (Symptomkontrollfunktion) ([6]),

— Warnung von Personen, die sich während einer bestimmten Zeit in der Nähe einer infizierten Person befanden, um Informationen über die Möglichkeit einer freiwilligen Quarantäne und den Ort für einen Test zur Verfügung zu stellen (Kontaktnachverfolgungs- und Warnfunktion),

— Bereitstellung eines Forums für die Kommunikation zwischen Ärzten und Patienten, die sich in Selbstisolierung befinden oder denen weitere Diagnose- und Therapiehinweise angeboten werden (verstärkter Einsatz von Telemedizin).

Gemäß der Datenschutzrichtlinie für elektronische Kommunikation kann die Verwendung einer App, die die Vertraulichkeit der in Artikel 5 genannten Kommunikationsrechte berührt, nur durch ein Gesetz vorgeschrieben werden, das notwendig, angemessen und verhältnismäßig ist, um bestimmte spezifische Ziele zu schützen. Angesichts der hohen Eingriffsintensität eines solchen Ansatzes und der damit verbundenen Herausforderungen, auch im Hinblick auf die Einführung geeigneter Schutzklauseln, ist nach Auffassung der Kommission eine sorgfältige Analyse erforderlich, bevor diese Option herangezogen wird. Aus diesen Gründen empfiehlt die Kommission die Verwendung von Apps auf freiwilliger Basis.

Diese Leitlinien gelten nicht für Apps zur Durchsetzung von Quarantäneanforderungen (einschließlich solcher, die verbindlich vorgeschrieben sind).

2 BEITRAG DER APPS ZUR BEKÄMPFUNG VON COVID-19

Die Symptomkontrollfunktion ist ein Instrument für Gesundheitsbehörden, um die Bürger über Tests auf COVID-19 zu orientieren und Informationen zur Selbstisolierung, zur Vermeidung einer Übertragung auf andere und zum Zeitpunkt der Inanspruchnahme von Gesundheitsleistungen bereitzustellen. Diese Funktion kann darüber hinaus die Überwachung der Grundversorgung ergänzen und die Informationen über die Übertragungsraten von COVID-19 in der Bevölkerung verbessern.

([3]) https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

([4]) 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.

([5]) 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.

([6]) Wenn die Apps Informationen über Diagnose, Verhütung, Überwachung, Vorhersage oder Prognose liefern, sollte die Möglichkeit der Einstufung als Medizinprodukte gemäß dem Rechtsrahmen für Medizinprodukte bewertet werden. Zu diesem Rahmen siehe Richtlinie 93/42/EWG des Rates vom 14. Juni 1993 über Medizinprodukte (ABl. L 169 vom 12.7.1993, S. 1) und Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte (ABl. L 117 vom 5.5.2017, S. 1).

Kontaktnachverfolgungs- und Warnfunktionen dienen zur Ermittlung von Personen, die mit einer von COVID-19 infizierten Person in Kontakt gekommen sind, und helfen, die Betroffenen über geeignete nächste Schritte zu informieren, zum Beispiel über Selbstisolierung, Tests oder die Vorgehensweise beim Auftreten von Symptomen. Diese Funktion ist daher sowohl für Einzelpersonen als auch für Gesundheitsbehörden nützlich. Sie kann auch bei der Handhabung von Eindämmungsmaßnahmen im Zuge einer Deeskalation eine wichtige Rolle spielen. Ihre Wirkung lässt sich mit einer Strategie steigern, die auf eine breiter angelegte Durchführung von Tests bei Personen mit schwachen Symptomen abzielt.

Die beiden genannten Funktionen können auch eine relevante Datenquelle für die Gesundheitsbehörden sein und die Übermittlung solcher Daten an die nationalen epidemiologischen Stellen und an das Europäische Zentrum für die Prävention und die Kontrolle von Krankheiten (ECDC) erleichtern. Dies würde dazu beitragen, die Übertragungsmuster zu verstehen und bei Kombination mit Testergebnissen den positiven prädiktiven Wert von Atemwegssymptomen in einer bestimmten Gemeinschaft zu schätzen und Informationen über das Ausmaß der Zirkulation des Virus zu liefern.

Wie zuverlässig die Schätzungen sind, hängt unmittelbar mit der Zahl und der Verlässlichkeit der übermittelten Daten zusammen.

Daher können in Verbindung mit geeigneten Teststrategien sowohl die Symptomkontroll- als auch die Kontaktnachverfolgungsfunktion Informationen über das Ausmaß der Zirkulation des Virus liefern und zur Bewertung der Auswirkungen der räumlichen Trennung und der Ausgangsbeschränkungen beitragen. Wie in der Empfehlung dargelegt, sollte die Interoperabilität zwischen den IT-Lösungen der verschiedenen Mitgliedstaaten sichergestellt werden, um die grenzüberschreitende Zusammenarbeit zu ermöglichen und die Erkennung von Kontakten zwischen Nutzern verschiedener Apps zu gewährleisten (dies ist insbesondere relevant, wenn Bürger Landesgrenzen überschreiten). Bei Kontakten einer infizierten Person mit einem Nutzer einer App eines anderen Mitgliedstaats sollte die grenzüberschreitende Übermittlung personenbezogener Daten dieses Nutzers an die Gesundheitsbehörden seines Mitgliedstaats möglich sein, aber auf das unbedingt erforderliche Ausmaß beschränkt bleiben. Die Arbeiten zu diesem Thema werden im Rahmen des in der Empfehlung angekündigten Instrumentariums erfolgen. Interoperabilität sollte sowohl durch technische Anforderungen als auch durch bessere Kommunikation und Zusammenarbeit zwischen den nationalen Gesundheitsbehörden gewährleistet werden. Ein Modell einer besonderen Zusammenarbeit ([7]) könnte darüber hinaus während der COVID-19-Pandemie als Governance-Modell für Kontaktnachverfolgungs-Apps dienen.

3 ELEMENTE FÜR EINE VERTRAUENSVOLLE UND VERANTWORTUNGSBEWUSSTE NUTZUNG VON APPS

Die in den Apps enthaltenen Funktionen können unterschiedliche Auswirkungen auf ein breites Spektrum von Rechten haben, die in der Charta der Grundrechte der EU verankert sind, darunter die Menschenwürde, die Achtung des Privat- und Familienlebens, den Schutz personenbezogener Daten, den freien Personenverkehr, die Nichtdiskriminierung, die unternehmerische Freiheit sowie die Versammlungs- und Vereinigungsfreiheit. Von besonderer Bedeutung können Eingriffe in die Privatsphäre und in das Recht auf Schutz personenbezogener Daten sein, weil einige der Funktionen auf einer intensiven Nutzung solcher Daten beruhen.

Die im Folgenden vorgestellten Elemente sollen als Orientierungshilfe dafür dienen, wie die Eingriffsintensität der App-Funktionen begrenzt werden kann, um die Einhaltung der EU-Rechtsvorschriften zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre zu gewährleisten.

3.1 Nationale Gesundheitsbehörden (oder Einrichtungen, die im öffentlichen Interesse Aufgaben im Gesundheitswesen wahrnehmen) als für die Datenverarbeitung Verantwortliche

Die Feststellung, wer über die Mittel und Zwecke der Datenverarbeitung entscheidet (also für die Datenverarbeitung verantwortlich ist), ist der entscheidende Faktor, um zu bestimmen, wer für die Einhaltung der EU-Vorschriften zum Schutz personenbezogener Daten verantwortlich ist und wer insbesondere die betroffenen Einzelpersonen, die die App herunterladen, darüber informieren sollte, was mit ihren personenbezogenen Daten (die bereits vorhanden sind oder durch das Gerät, z. B. ein Smartphone, auf dem die App installiert wird, generiert werden) geschehen wird, welche Rechte sie haben, wer im Falle einer Verletzung des Datenschutzes verantwortlich ist usw.

Angesichts der Sensibilität der personenbezogenen Daten, um die es hier geht, und des Zwecks der unten beschriebenen Datenverarbeitung sollten die Apps nach Auffassung der Kommission so konzipiert werden, dass die nationalen Gesundheitsbehörden (oder Einrichtungen die im öffentlichen Interesse Aufgaben im Gesundheitswesen wahrnehmen) für die Verarbeitung verantwortlich sind. ([8]) Die Verantwortlichen sind für die Einhaltung der Datenschutz-Grundverordnung verantwortlich („Rechenschaftspflicht"). Der Umfang eines solchen Zugriffs sollte nach den in Abschnitt 3.5 dargelegten Grundsätzen beschränkt werden.

([7]) Eine solche Zusammenarbeit findet bereits im Rahmen des Projekts MyHealth@EU für den Austausch von Patientenkurzakten und elektronischen Verschreibungen statt. Siehe auch Artikel 5 Absatz 5 und Erwägungsgrund 17 des Durchführungsbeschlusses 2019/1765 der Kommission.

([8]) Siehe Erwägungsgrund 45 der DSGVO.

Dies wird auch zu einem größeren Vertrauen in der Bevölkerung und somit zu einer höheren Akzeptanz der Apps (und der ihnen zugrunde liegenden Informationssysteme für Infektionsübertragungsketten) beitragen und sicherstellen, dass sie den angestrebten Zweck (Schutz der öffentlichen Gesundheit) erfüllen. Die zugrunde liegenden Strategien, Anforderungen und Kontrollen sollten von den zuständigen nationalen Gesundheitsbehörden abgestimmt und in koordinierter Weise umgesetzt werden.

3.2 **Gewährleistung, dass die betroffene Person die Kontrolle behält**

Ein entscheidender Faktor für Vertrauen der betroffenen Menschen in solche Apps ist der Nachweis, dass sie die Kontrolle über ihre personenbezogenen Daten behalten. Dafür sollten nach Auffassung der Kommission insbesondere folgende Bedingungen erfüllt sein:

— die Installation der App in ihrem Gerät sollte freiwillig sein, und es darf keine nachteiligen Folgen für Personen geben, die die App nicht herunterladen bzw. nutzen;

— verschiedene App-Funktionen (z. B. Information, Symptomkontrolle, Kontaktnachverfolgung und Warnung) sollten nicht gebündelt werden, damit die betroffene Person ihre Einwilligung speziell zu jeder einzelnen Funktion geben kann. Dies sollte den Nutzer nicht daran hindern, verschiedene App-Funktionen miteinander zu kombinieren, wenn dies vom Anbieter als Option angeboten wird;

— falls Umkreisdaten verwendet werden, d. h. Daten, die durch den Austausch von BLE-Signalen (*Bluetooth Low Energy*) zwischen Geräten innerhalb einer epidemiologisch relevanten Entfernung und während eines epidemiologisch relevanten Zeitraums generiert werden, sollten diese im Gerät der betroffenen Person gespeichert werden. Falls diese Daten an Gesundheitsbehörden weitergegeben werden sollen, sollten sie erst übermittelt werden, nachdem bei der betroffenen Person eine COVID-19-Infektion bestätigt wurde und unter der Bedingung, dass diese Person der Weitergabe ausdrücklich zustimmt;

— die Gesundheitsbehörden sollten der betroffenen Person alle nötigen Informationen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten zur Verfügung stellen (gemäß den Artikeln 12 und 13 der DSGVO und Artikel 5 der e-Datenschutzrichtlinie);

— die betroffene Person sollte in der Lage sein, ihre Rechte aus der DSGVO auszuüben (insbesondere die Rechte auf Zugang, Berichtigung und Löschung). Jede Einschränkung der Rechte aus der DSGVO und der e-Datenschutzrichtlinie sollte im Einklang mit diesen Vorschriften stehen sowie notwendig, verhältnismäßig und in der entsprechenden Rechtsvorschrift vorgesehen sein;

— die Apps sollten spätestens dann deaktiviert werden, wenn die Pandemie als unter Kontrolle gebracht erklärt worden ist; die Deaktivierung sollte nicht von einer Deinstallation durch den Nutzer abhängen.

3.3 **Rechtsgrundlage der Datenverarbeitung**

Installation der Apps und Speicherung von Informationen im Gerät des Nutzers

Wie bereits erwähnt, ist nach der e-Datenschutzrichtlinie (Artikel 5) die Speicherung von Informationen im Gerät des Nutzers oder der Zugriff auf bereits gespeicherte Informationen nur dann zulässig, wenn i) der Nutzer seine Einwilligung gegeben hat oder ii) die Speicherung und/oder der Zugriff für den Dienst der Informationsgesellschaft (z. B. die App), der vom Nutzer ausdrücklich (z. B. durch Installation und Aktivierung) angefordert wurde, unbedingt erforderlich ist.

Die Speicherung von Informationen im Gerät der betroffenen Person und der Zugriff auf die in dem Gerät bereits gespeicherten Informationen sind in der Regel für das Funktionieren der Apps erforderlich. Darüber hinaus müssen für die Kontaktnachverfolgungs- und Warnfunktion einige weitere Informationen im Gerät des Nutzers gespeichert werden (z. B. flüchtige und regelmäßig wechselnde Alias-Kennungen von anderen Nutzern dieser Funktion, die sich in der Nähe befinden). Darüber hinaus kann diese Funktion es erforderlich machen, dass der (infizierte oder wahrscheinlich infizierte) Nutzer seine Umkreisdaten hochlädt. Ein solches Hochladen ist für das Funktionieren der App als solche aber nicht erforderlich. Deshalb sind die in Ziffer ii genannten Anforderungen hier nicht erfüllt. Bleibt also nur die Einwilligung (Ziffer i) als am besten geeignete Rechtsgrundlage für die betreffenden Tätigkeiten. Diese Einwilligung sollte „freiwillig", „für den bestimmten Fall", „ausdrücklich" und „in informierter Weise" (d. h. nach Aufklärung) im Sinne der Datenschutz-Grundverordnung erfolgen. Außerdem sollte sie durch eine eindeutige bestätigende Handlung der betroffenen Person zum Ausdruck gebracht werden, was stillschweigende Formen der Einwilligung (wie Stillschweigen, Untätigkeit) ausschließt ([9]).

([9]) Siehe die Leitlinien des Europäischen Datenschutzausschusses in Bezug auf die Einwilligung: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

Rechtsgrundlage für die Datenverarbeitung durch nationale Gesundheitsbehörden – Unionsrecht oder Recht der Mitgliedstaaten

Nationale Gesundheitsbehörden verarbeiten personenbezogene Daten in der Regel dann, wenn nach dem Recht der EU oder der Mitgliedstaaten eine solche Verarbeitung vorgeschrieben ist und die Bedingungen in Artikel 6 Absatz 1 Buchstabe c und Artikel 9 Absatz 2 Buchstabe i der DSGVO erfüllt sind oder wenn eine solche Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die nach dem Recht der EU oder der Mitgliedstaaten anerkanntermaßen dem öffentlichen Interesse dient ([10]).

Etwaige einzelstaatliche Rechtsvorschriften müssen besondere Vorkehrungen zum Schutz der Rechte und Freiheiten der betroffenen Personen vorsehen. Je stärker die Auswirkungen auf die Freiheiten der betroffenen Personen sind, desto strikter sollten die entsprechenden Schutzvorkehrungen in den einschlägigen Rechtsvorschriften sein.

Rechtsvorschriften der EU und der Mitgliedstaaten, die bereits vor dem COVID-19-Ausbruch galten, und Vorschriften, die von Mitgliedstaaten speziell zur Bekämpfung der Ausbreitung von Epidemien erlassen werden, können grundsätzlich als Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten betroffener Personen herangezogen werden, wenn sie Maßnahmen vorsehen, die eine Überwachung von Epidemien erlauben, und wenn die betreffenden Vorschriften den Anforderungen in Artikel 6 Absatz 3 der DSGVO genügen.

Angesichts der Art der betreffenden personenbezogenen Daten (insbesondere Gesundheitsdaten als besondere Kategorie personenbezogener Daten) und der Umstände der derzeitigen COVID-19-Pandemie würde die gesetzliche Grundlage zur Rechtssicherheit beitragen, weil dort i) die Verarbeitung spezifischer Gesundheitsdaten im Einzelnen vorgeschrieben und die Zwecke der Verarbeitung eindeutig festgelegt würden, ii) eindeutig angegeben würde, wer für die Datenverarbeitung verantwortlich ist, d. h. welche Stelle die Daten verarbeitet und wer neben dem für die Verarbeitung Verantwortlichen Zugriff auf diese Daten hat, iii) die Möglichkeit ausgeschlossen würde, solche Daten zu anderen als den im Gesetz aufgeführten Zwecken zu verarbeiten, und iv) besondere Schutzvorkehrungen getroffen würden. Um den Nutzen und die Akzeptanz der Apps für die Öffentlichkeit nicht zu untergraben, sollte der nationale Gesetzgeber besonders darauf achten, dass die gewählte Lösung gegenüber den Bürgerinnen und Bürgern so inklusiv wie möglich ist.

Die Verarbeitung durch die Gesundheitsbehörden auf der Grundlage der Rechtsvorschriften ändert nichts daran, dass es den betroffenen Personen freisteht, die App zu installieren oder nicht und ihre Daten an die Gesundheitsbehörden weiterzugeben oder nicht. Das Deinstallieren der App sollte daher keine nachteiligen Folgen für die Nutzer haben.

Kontaktnachverfolgungs- und Warn-Apps ermöglichen es, betroffene Einzelpersonen zu warnen. Für den Fall, dass diese Warnung direkt von der App ausgegeben wird, weist die Kommission auf das Verbot hin, Personen einer Entscheidung zu unterwerfen, die ausschließlich auf einer automatisierten Verarbeitung beruht und ihr gegenüber Rechtswirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (Artikel 22 der DSGVO).

3.4 **Datenminimierung**

Die Daten, die über Geräte erzeugt und bereits zuvor in diesen gespeichert wurden, sind folgendermaßen geschützt:

— Als „personenbezogene Daten“, also Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Artikel 4 Absatz 1 der DSGVO) sind sie nach der DSGVO geschützt. Für Gesundheitsdaten gilt zusätzlicher Schutz (Artikel 9 DSGVO).

— Als „Standortdaten“, also Daten, die in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers angeben, sind sie nach Artikel 5 Absatz 1, Artikel 6 und Artikel 9 der Datenschutzrichtlinie für elektronische Kommunikation ([11]) geschützt.

— Informationen, die im Endgerät eines Nutzers gespeichert werden oder auf die von dort zugegriffen wird, sind nach Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation geschützt.

Nicht personenbezogene Daten (etwa unwiderruflich anonymisierte Daten) sind durch die DSGVO nicht geschützt.

Die Kommission erinnert daran, dass personenbezogene Daten nach dem Grundsatz der Datenminimierung nur verarbeitet werden dürfen, wenn sie dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind. ([12]) Vor dem Hintergrund des verfolgten Zwecks oder der verfolgten Zwecke sollte eine Bewertung der Notwendigkeit der Verarbeitung der personenbezogenen Daten sowie der Erheblichkeit der personenbezogenen Daten durchgeführt werden.

Die Kommission weist beispielsweise darauf hin, dass kein Zugriff auf die Kontaktliste der Person, die Eigentümerin des Geräts ist, erforderlich ist, wenn der Zweck der Funktion in der Kontrolle auf Symptome oder der Telemedizin besteht.

([10]) Artikel 6 Absatz 1 Buchstabe e der DSGVO.

([11]) Nach dem Kodex für die elektronische Kommunikation sind auch funktional gleichwertige elektronischen Kommunikationsdienste erfasst.

([12]) Grundsatz der Datenminimierung

Je weniger Daten erzeugt und verarbeitet werden, desto geringer sind die Sicherheitsrisiken. Die Einhaltung der Maßnahmen zur Datenminimierung ist also auch eine Sicherheitsvorkehrung.

— Informationsfunktion:

In einer App, die nur diese Funktion erfüllt, ist keine Verarbeitung von Gesundheitsdaten von Einzelpersonen erforderlich. Es werden lediglich Informationen zur Verfügung gestellt. Zu diesem Zweck dürfen unter den Informationen, die auf dem Endgerät gespeichert sind oder auf die darüber zugegriffen wird, nur diejenigen verarbeitet werden, die erforderlich sind, um die Informationen zur Verfügung zu stellen.

— Symptomkontroll- und Telemedizinfunktion:

Wenn die App mindestens eine dieser Funktionen umfasst, werden damit personenbezogene Gesundheitsdaten verarbeitet. Daher sollte in den zugrunde liegenden Rechtsvorschriften, die für die Gesundheitsbehörden gelten, aufgeführt werden, welche Daten verarbeitet werden dürfen.

Zusätzlich könnten die Gesundheitsbehörden die Telefonnummern der Personen benötigen, die die Kontrolle auf Symptome durchgeführt und die Ergebnisse hochgeladen haben. Informationen, die auf dem Endgerät gespeichert sind oder auf die darüber zugegriffen wird, dürfen insofern verarbeitet werden, als dies nötig ist, damit die App ihren Zweck erfüllen und funktionieren kann.

— Kontaktnachverfolgungs- und Warnfunktion:

Zu einem Großteil der COVID-19-Infektionen kommt es über Tröpfchen, die nur eine begrenzte Entfernung zurücklegen können. So schnell wie möglich zu ermitteln, wer sich im Umkreis einer infizierten Person aufgehalten hat, ist von erheblicher Bedeutung, um die Infektionskette zu unterbrechen. Kontakte im Umkreis werden über die Funktion aus der Dauer eines Kontakts und der Distanz dabei ermittelt und sollten aus epidemiologischer Sicht bestimmt werden. Insbesondere in der Phase, in der die Krisenmaßnahmen schrittweise abgebaut werden, ist die Unterbrechung von Infektionsketten enorm wichtig, um einen erneuten Anstieg der Infektionszahlen zu vermeiden.

Dafür könnten Umkreisdaten nötig sein. Für die Erfassung des Umkreises und von Kontakten in unmittelbarer Nähe scheint die Nutzung der BLE-Kommunikation (Bluetooth Low Energy) zwischen Geräten genauer und somit geeigneter zu sein als die Nutzung von Geolokalisierungsdaten (GNSS/GPS oder Standortdaten von Mobilgeräten). Über BLE ist (im Gegensatz zu Geolokalisierungsdaten) keine Nachverfolgung möglich. Die Kommission empfiehlt daher die Nutzung von BLE-Kommunikationsdaten (oder von mit gleichwertiger Technik erzeugten Daten) zur Ermittlung von Kontakten im Umkreis.

Für die Zwecke von Kontaktnachverfolgungsfunktionen sind Standortdaten nicht erforderlich, da ihr Ziel nicht darin besteht, die Bewegungen von Einzelpersonen nachzuvollziehen oder Verordnungen durchzusetzen. Zudem wäre die Verarbeitung von Standortdaten im Zusammenhang mit der Kontaktnachverfolgung vor dem Hintergrund des Grundsatzes der Datenminimierung schwer zu rechtfertigen und könnte Anlass zu Bedenken bezüglich der Sicherheit und des Schutzes der Privatsphäre geben. Aus diesem Grund empfiehlt die Kommission, in diesem Zusammenhang keine Standortdaten zu verwenden.

Unabhängig von den technischen Mitteln, die zur Ermittlung von Kontakten im Umkreis genutzt werden, erscheint die Speicherung des genauen Zeitpunkts und (falls verfügbar) des Standorts nicht erforderlich. Die Speicherung des Datums des Kontakts könnte jedoch sinnvoll sein, um feststellen zu können, ob es zu dem Kontakt kam, als die Person bereits Symptome entwickelt hatte (oder in den vorangegangenen 48 Stunden ([13])) und mit einer entsprechenden Nachricht mit Empfehlungen zur Dauer der Selbstquarantäne zu reagieren.

Umkreisdaten sollten nur dann erzeugt und verarbeitet werden, wenn ein tatsächliches Infektionsrisiko besteht (je nach Dauer eines Kontakts und der Distanz dabei).

Anzumerken ist, dass die Notwendigkeit und Verhältnismäßigkeit der Datenerhebung daher von Faktoren wie der Verfügbarkeit von Testinfrastruktur abhängen werden, insbesondere wenn bereits Maßnahmen wie Ausgangsbeschränkungen angeordnet wurden. Personen, die unmittelbaren Kontakt mit einer infizierten Person hatten, können auf zwei Arten gewarnt werden:

Ein Verfahren besteht darin, die Personen, zu denen ein Nutzer unmittelbaren Kontakt hatte, über die App automatisch zu warnen, wenn dieser Nutzer in der App – nach Zustimmung oder Bestätigung durch die Gesundheitsbehörde, etwa über einen QR- oder TAN-Code – ein positives Testergebnis mitteilt (dezentrale Verarbeitung). Der Inhalt der Warnmeldung sollte vorzugsweise von der Gesundheitsbehörde festgelegt werden. Bei dem anderen Verfahren werden zufällig festgelegte, vorübergehende Kennungen auf einem Back-End-Server der Gesundheitsbehörde gespeichert (Back-End-Server-Verfahren). Mit diesen Daten ist keine direkte Identifikation der Nutzer möglich. Über die Kennungen erhalten Nutzer, die unmittelbaren Kontakt mit einem positiv getesteten Nutzer hatten, eine Warnung auf ihrem Gerät. Wenn die Gesundheitsbehörden die Nutzer, die unmittelbaren Kontakt zu einer infizierten Person hatten, auch per Telefon oder SMS kontaktieren möchten, brauchen sie die Einwilligung dieser Nutzer, ihre Telefonnummern anzugeben.

([13]) Die infizierte Person kann bereits in den 48 Stunden vor dem Auftreten der Symptome andere Menschen anstecken.

3.5 **Beschränkung der Offenlegung von/des Zugangs zu Daten**

— Informationsfunktion:

Informationen, die in einem Endgerät gespeichert sind und auf die darüber zugegriffen wird, dürfen nur dann an die Gesundheitsbehörden weitergegeben werden, wenn dies für die Informationsfunktion erforderlich ist. Da mit dieser Funktion nur ein Kommunikationsmittel bereitgestellt wird, erhalten die Gesundheitsbehörden keinen Zugang zu anderen Daten.

— Symptomkontroll- und Telemedizinfunktion:

Die Symptomkontrollfunktion kann für die Mitgliedstaaten nützlich sein, um die Bürgerinnen und Bürger in der Frage zu leiten, ob sie sich testen lassen sollten und ihnen Informationen über Isolierung und, insbesondere bei Risikogruppen, darüber zukommen zu lassen, wann und wie sie sich an Gesundheitseinrichtungen wenden sollten. Diese Funktion kann darüber hinaus grundlegende Gesundheitskontrollen ergänzen und helfen nachzuvollziehen, wie hoch die COVID-19-Infektionsraten in der Bevölkerung sind. Daher könnte beschlossen werden, dass die zuständigen Gesundheitsbehörden und die im Bereich der Epidemiologie tätigen nationalen Behörden Zugang zu den vom Patienten bereitgestellten Informationen erhalten sollten. Das ECDC könnte von den für die epidemiologische Überwachung zuständigen nationalen Behörden aggregierte Daten erhalten.

Wenn entschieden wird, dass ein Kontakt mit Mitarbeitern der Gesundheitsbehörden und nicht nur über die App selbst möglich sein soll, ist auch die Offenlegung der Telefonnummern der App-Nutzer gegenüber den nationalen Gesundheitsbehörden erforderlich.

— Kontaktnachverfolgungs- und Warnfunktion:

— Daten der infizierten Person

Die Apps erzeugen pseudozufällige, vorübergehende und sich regelmäßig ändernde Kennungen für die Telefone, die sich im Umkreis des Nutzers befinden. Eine Option besteht darin, dass die Kennungen auf dem Gerät des Nutzers gespeichert werden (sogenannte dezentrale Verarbeitung). Eine andere Option kann vorsehen, dass diese zufälligen Kennungen auf einem Server gespeichert werden, zu dem die Gesundheitsbehörden Zugang haben (sogenanntes Back-End-Server-Verfahren). Die dezentrale Lösung entspricht eher dem Grundsatz der Datenminimierung. Die Gesundheitsbehörden sollten nur auf die Umkreisdaten vom Gerät einer infizierten Person zugreifen können, um die Personen, für die ein Infektionsrisiko besteht, kontaktieren zu können.

Diese Daten werden den Gesundheitsbehörden erst zur Verfügung stehen, wenn die infizierte Person (nachdem sie getestet wurde) diese Daten proaktiv an sie übermittelt.

Die infizierte Person sollte nicht über die Identität der Personen informiert werden, mit denen sie potenziell epidemiologisch relevanten Kontakt hatte und die gewarnt werden.

— Daten der Personen, die mit der infizierten Person (epidemiologisch relevanten) Kontakt hatten

Die Identität der infizierten Person sollte den Personen, mit denen sie epidemiologisch relevanten Kontakt hatte, nicht offengelegt werden. Es genügt, ihnen mitzuteilen, dass sie in den letzten 16 Tagen epidemiologisch relevanten Kontakt mit einer infizierten Person hatten. Wie oben erwähnt sollten Daten über Zeitpunkt und Ort solcher Kontakte nicht gespeichert werden. Die Übermittlung dieser Daten ist daher weder erforderlich noch möglich.

Für die Nachverfolgung der epidemiologisch relevanten Kontakte eines App-Nutzers, bei dem eine Infektion festgestellt wurde, sollten die nationalen Gesundheitsbehörden nur über die Kennung informiert werden, die die Person betrifft, mit der die infizierte Person zwischen 48 Stunden vor Auftreten der Symptome und 14 Tagen nach Auftreten der Symptome, basierend auf der Dauer des Kontakts und der Distanz dabei, epidemiologisch relevanten Kontakt hatte.

Das ECDC könnte von den für die epidemiologische Überwachung zuständigen nationalen Behörden aggregierte Kontaktnachverfolgungsdaten zu in Zusammenarbeit mit den Mitgliedstaaten festgelegten Kennungen erhalten.

3.6 **Zweckbestimmung der Verarbeitung**

Die Rechtsgrundlage (Unionsrecht oder Recht der Mitgliedstaaten) sollte den Zweck der Verarbeitung bestimmen. Der Zweck sollte genau bestimmt werden, damit kein Zweifel daran besteht, welche Art von personenbezogenen Daten für die Verarbeitung erforderlich ist, um das angestrebte Ziel zu erreichen; außerdem sollte er klar und ausdrücklich beschrieben werden.

Der genaue Zweck wird von den Funktionen der App abhängen. Jede Funktion einer App kann mehreren Zwecken dienen. Um den betroffenen Personen die volle Kontrolle über ihre Daten zu verschaffen, empfiehlt die Kommission, keine Funktionen zu bündeln. In jedem Fall sollte die betroffene Person die Möglichkeit haben, zwischen verschiedenen Funktionen zu wählen, die jeweils unterschiedliche Zwecke verfolgen.

Die Kommission spricht sich dagegen aus, die unter diesen Voraussetzungen erhobenen Daten für andere Zwecke als die Bekämpfung von COVID-19 zu verwenden. Sollte es erforderlich sein, Daten für Zwecke wie wissenschaftliche Forschung oder Statistik zu erheben, sollten sie in die ursprüngliche Liste der Zwecke aufgenommen und den Nutzern klar und deutlich bekanntgemacht werden.

— Informationsfunktion:

Zweck dieser Funktion ist die Bereitstellung der aus Sicht der Gesundheitsbehörden im Kontext der Krise relevanten Informationen.

— Symptomkontroll- und Telemedizinfunktionen:

Die Symptomkontrollfunktion kann Aufschluss darüber geben, welcher Anteil der betroffenen Personen, die mit COVID-19 kompatible Symptome melden, tatsächlich infiziert ist (z. B. durch Vornahme von Abstrich und Test bei allen oder bei einer Stichprobe von betroffenen Personen mit solchen Symptomen, sofern die Kapazitäten vorhanden sind). Aus der Zweckbestimmung sollte klar hervorgehen, dass die personenbezogenen Gesundheitsdaten verarbeitet werden, um i) damit die betroffene Person auf der Grundlage einer Reihe von Fragen selbst auswerten kann, ob sie Symptome von COVID-19 entwickelt hat, oder ii) für ärztliche Beratung zu sorgen, wenn die Person Symptome von COVID-19 entwickelt hat.

— Kontaktnachverfolgungs- und Warnfunktionen:

Die bloße Zweckbestimmung „Verhütung weiterer COVID-19-Infektionen“ ist nicht bestimmt genug. In diesem Fall empfiehlt die Kommission nähere Erläuterungen, etwa in dem Sinne: „Speicherung der Kontakte der Personen, die die App benutzen und möglicherweise einer COVID-19-Infektion ausgesetzt waren, um jene Personen zu warnen, die möglicherweise infiziert sein könnten“.

3.7 **Strenge Begrenzung der Datenspeicherung**

Der Grundsatz der begrenzten Speicherung besagt, dass personenbezogene Daten nicht länger als notwendig gespeichert werden dürfen. Die Fristen sollten auf der medizinischen Relevanz beruhen (je nach Zweck der App: Inkubationszeit usw.) sowie realistische Zeiträume für gegebenenfalls erforderliches Verwaltungshandeln.

— Informationsfunktion:

Daten, die bei der Installation dieser Funktion erhoben werden, sollten unverzüglich gelöscht werden. Für ihre Aufbewahrung gibt es keine Rechtfertigung.

— Symptomkontroll- und Telemedizinfunktionen:

Diese Daten sollten von den Gesundheitsbehörden nach höchstens einem Monat (Inkubationszeit plus Marge) oder nach einem Test der Person mit negativem Ergebnis gelöscht werden. Die Gesundheitsbehörden können Daten länger speichern, sofern sie in anonymisierter Form für die Berichterstattung und Forschung verwendet werden sollen.

— Kontaktnachverfolgungs- und Warnfunktionen:

Umkreisdaten sollten gelöscht werden, sobald sie für die Warnung betroffener Personen nicht mehr erforderlich sind. Das sollte nach höchstens einem Monat (Inkubationszeit plus Marge) oder nach einem Test der Person mit negativem Ergebnis der Fall sein. Die Gesundheitsbehörden können die Umkreisdaten länger speichern, sofern sie in anonymisierter Form für die Berichterstattung und Forschung verwendet werden sollen.

Die Daten sollten im Gerät des Nutzers gespeichert werden, und nur die Daten, die von den Nutzern übermittelt wurden und für die Erfüllung des Zwecks erforderlich sind, sollten auf Server hochgeladen werden, die den Gesundheitsbehörden zur Verfügung stehen, sofern diese Möglichkeit gewählt wurde (d. h. nur Daten über „enge Kontakte“ einer positiv auf COVID-19 getesteten Person sollten hochgeladen werden).

3.8 **Gewährleistung der Datensicherheit**

Die Kommission empfiehlt, die Daten in den Endgeräten der betroffenen Personen in verschlüsselter Form unter Verwendung modernster Verschlüsselungstechnologien zu speichern. Werden die Daten auf einem zentralen Server gespeichert, sollte der Zugriff (auch der administrative Zugriff) protokolliert werden.

Umkreisdaten sollten nur in verschlüsseltem und pseudonymisiertem Format im Endgerät der betroffenen Person generiert und gespeichert werden. Um die Ortung oder Verfolgung durch Dritte auszuschließen, sollte Bluetooth aktiviert werden können, ohne dass andere Standortdienste aktiviert werden.

Bei der Erhebung von Umkreisdaten mittels BLE ist es vorzuziehen, regelmäßig wechselnde vorübergehende Nutzerkennungen zu generieren und anstelle der tatsächlichen Gerätekennung zu speichern. Diese Maßnahme bietet einen zusätzlichen Schutz vor Spionage und Ortung/Verfolgung durch Hacker und erschwert daher die Identifizierung von betroffenen Personen.

Die Kommission empfiehlt, den Quellcode der Apps öffentlich zugänglich zu machen und zur Überprüfung zur Verfügung zu stellen.

Zusätzliche Maßnahmen zur Sicherung der verarbeiteten Daten können in Betracht gezogen werden, insbesondere die automatische Löschung oder Anonymisierung der Daten nach einem bestimmten Zeitpunkt. Im Allgemeinen sollte das Sicherheitsniveau dem Umfang und der Sensibilität der verarbeiteten personenbezogenen Daten entsprechen.

Alle Übertragungen vom einzelnen Endgerät an die nationalen Gesundheitsbehörden sollten verschlüsselt erfolgen.

Erlaubt das innerstaatliche Recht die Verarbeitung der erhobenen personenbezogenen Daten auch für Zwecke der wissenschaftlichen Forschung, sollte grundsätzlich eine Pseudonymisierung erfolgen.

3.9 **Gewährleistung der Datenrichtigkeit**

Die Gewährleistung der Richtigkeit der verarbeiteten personenbezogenen Daten ist nicht nur eine Voraussetzung für die Effizienz der App, sondern auch ein Erfordernis des Datenschutzrechts.

Die Richtigkeit der Informationen darüber, ob ein Kontakt mit einer infizierten Person stattgefunden hat (epidemiologisch relevante Entfernung und Dauer), ist unabdingbar, um das Risiko falscher positiver Befunde möglichst gering zu halten. Dabei sollte berücksichtigt werden, ob zwei Nutzer der App sich auf der Straße, in öffentlichen Verkehrsmitteln oder in einem Gebäude begegnen. Standortdaten aus der Ortung über Mobilfunknetze sind zu diesem Zweck voraussichtlich nicht genau genug.

Daher ist es ratsam, auf Technologien zurückzugreifen, die eine genauere Bewertung des Kontakts ermöglichen (wie Bluetooth).

3.10 **Einbeziehung der Datenschutzbehörden**

Die Datenschutzbehörden sollten umfassend in die Entwicklung der App einbezogen und konsultiert werden und sollten sie anschließend laufend überprüfen. Da die Verarbeitung von Daten im Zusammenhang mit der App als umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten (Gesundheitsdaten) gelten wird, weist die Kommission auf Artikel 35 der DSGVO betreffend die Datenschutz-Folgenabschätzung hin.