Erklärung

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Erklärung über die Datenschutzfolgen der Interoperabilität von Kontaktnachverfolgungs-Apps

Angenommen am 16. Juni 2020

Der Europäische Datenschutzausschuss (EDSA) hat folgende Erklärung angenommen:

1. In den Leitlinien 04/2020[1] für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 hat der EDSA angeregt, dass „ein gemeinsames europäisches Konzept ausgearbeitet oder zumindest ein interoperabler Rahmen geschaffen werden [sollte]".

2. Der EDSA hat die am 13. Mai 2020 vom Netzwerk für elektronische Gesundheitsdienste angenommenen Interoperabilitätsleitlinien für genehmigte mobile Anwendungen zur Ermittlung von Kontaktpersonen in der EU[2] zur Kenntnis genommen; darin wird die Interoperabilität im Zusammenhang mit Anwendungen zur Kontaktnachverfolgung wie folgt beschrieben:

> „die Möglichkeit, die *erforderliche Mindestmenge an Informationen* auszutauschen, damit einzelne App-Nutzer, unabhängig davon, wo sie sich in der EU aufhalten, Warnmeldungen erhalten, wenn sie sich im relevanten Zeitraum in der Nähe eines anderen Nutzers aufgehalten haben, der der App einen Positiv-Status für COVID-19 gemeldet hat." (Hervorhebung hinzugefügt.)

[1] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en

[2] https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf – Bitte beachten, dass dies ein lebendes Dokument ist, das von der Europäischen Kommission laufend überarbeitet wird und deshalb Änderungen unterliegt (siehe Seite 3 der Fassung vom 13. Mai 2020).

3. Des Weiteren sehen die Interoperabilitätsleitlinien vor, dass die Warnmeldung und die Nachverfolgung nach den von den Gesundheitsbehörden festgelegten Verfahren erfolgen sollten, wobei eine Einschätzung der potenziellen Folgen für den Schutz der Privatsphäre und die Datensicherheit und angemessener Schutzvorkehrungen vorzunehmen ist.

4. In dieser Erklärung macht der EDSA weitere Ausführungen zum Umfang der Folgen für das Recht auf Datenschutz, die eine interoperable Implementierung, je nach Implementierung, mit sich bringen kann. Die in dieser Erklärung gegebenen Empfehlungen ergänzen diejenigen in den Leitlinien 04/2020 des EDSA, die weiterhin Bestand haben.

Allgemeine Erwägungen

5. Zunächst möchte der EDSA daran erinnern, dass die Verwendung von Anwendungen zur Kontaktnachverfolgung auf der Verarbeitung pseudonymisierter personenbezogener Daten der App-Nutzer beruht.[3] Dazu zählen auch Gesundheitsdaten, z. B., wenn der Positiv-Status eines Nutzers von einem Angehörigen eines Gesundheitsberufs bestätigt wird oder wenn Expositionsinformationen vom System verarbeitet werden. Entsprechend dem, was zur allgemeinen Verwendung von Anwendungen zur Kontaktnachverfolgung[4] gesagt wurde, ist der EDSA der Ansicht, dass die Ermöglichung des Austauschs von Daten über Einzelpersonen, bei denen ein Positiv-Status diagnostiziert oder durch Test festgestellt wurde („Infektionsdaten"), mit solchen interoperablen Anwendungen nur durch eine freiwillige Handlung des Nutzers ausgelöst werden sollte. Die betroffenen Personen[5] müssen die Kontrolle über ihre Daten haben. Das Ziel der Interoperabilität darf nicht als Argument dafür genutzt werden, über das erforderliche Maß hinaus personenbezogene Daten zu erfassen.

6. Grundsätzlich kann die Interoperabilität von Anwendungen zur Kontaktnachverfolgung innerhalb des EWR deren Effektivität für die Unterstützung bereits vorhandener Maßnahmen erhöhen, da sie, unabhängig von der verwendeten App, die Nachverfolgung von mehr möglichen Kontaktpersonen und mehr potenzielle Warnmeldungen ermöglicht. Dies würde die Verwendung insbesondere für Menschen in Grenzregionen, auf Reisen oder bei der Arbeit in Berufen oder Gegenden, in denen sie unter Umständen vielen Menschen aus anderen Mitgliedstaaten ausgesetzt sind (wie z. B. im Tourismusbereich), erleichtern. Da jedoch, wie nachstehend erörtert wird, mit der Interoperabilität auch ein erhöhtes Datenschutzrisiko einhergeht, sollten die Verantwortlichen daneben andere Möglichkeiten erkunden.

7. Außerdem müssten solche Lösungen, so wie es auch für die Anwendungen selbst gilt, Teil einer umfassenden öffentlichen Gesundheitsstrategie zur Pandemiebekämpfung sein, die unter anderem Tests und anschließende manuelle Kontaktnachverfolgung beinhaltet, um die Effektivität der ergriffenen Maßnahmen zu verbessern.

8. Der EDSA ist sich bewusst, dass es in den verschiedenen Mitgliedstaaten unterschiedliche Anwendungen zur Kontaktnachverfolgung gibt, und erkennt an, dass die Gewährleistung der Interoperabilität verschiedener Implementierungen technisch schwierig ist und unter Umständen erheblichen finanziellen und technischen Aufwand erfordert. Um sicherzustellen, dass Datenaustausch und Datenverarbeitung, wie in der DSGVO vorgesehen, auf das Mindestmaß beschränkt sind, werden sich die Entwickler von Apps zur Kontaktnachverfolgung auf ein

[3] Siehe Erwägungsgrund 26 DSGVO, wo angegeben ist, welche Daten als personenbezogene Daten anzusehen sind.
[4] Hierin im Folgenden synonym mit dem Begriff „App" und „Anwendungen" verwendet.
[5] Hierin im Folgenden synonym mit dem Begriff „Nutzer" verwendet.

gemeinsames Protokoll und kompatible Datenstrukturen einigen müssen. Für Anwendungen, die bereits auf einem gemeinsamen Rahmen oder zumindest auf derselben technologischen Grundlage beruhen, mag das Ziel der Interoperabilität daher leichter zu erreichen sein als für diejenigen, bei denen dies nicht der Fall ist. Wegen der Unterschiede zwischen den Ansätzen mag es sich erweisen, dass die Implementierung der Interoperabilität in der Praxis nicht ohne unverhältnismäßige Kompromisse möglich ist.

Kernpunkte

Transparenz

9. Die Interoperabilität wird zu zusätzlicher Verarbeitung und Offenlegung von Daten gegenüber zusätzlichen Stellen führen. Die betroffenen Personen sind, wie stets, über jede zusätzliche Verarbeitung ihrer personenbezogenen Daten und die daran beteiligten Parteien aufzuklären.[6] Für die Nutzer sollte stets klar ersichtlich sein, was die Benutzung der Anwendung mit sich bringt, und sie sollten stets die Kontrolle über ihre Daten behalten.

10. Spätestens zu dem Zeitpunkt, zu dem einer oder sämtliche der für die Verarbeitung Verantwortlichen personenbezogene Daten erlangt, sind der betroffenen Person klare Informationen über die zusätzliche Verarbeitung zu geben, die sich durch die Nutzung der Interoperabilität ergibt. Zu diesem Zeitpunkt muss der Nutzer über die Bedingungen und den Umfang der Datenverarbeitung informiert werden.

11. Es gelten die Standardregeln in Bezug auf Transparenz; die Informationen sind in klarer und einfacher Sprache mitzuteilen.[6] Dies beinhaltet Informationen darüber, wie die ausgetauschten Daten von der interoperablen Anwendung zur Kontaktnachverfolgung, die die Daten empfängt, verarbeitet werden.

Rechtsgrundlage

12. Die einschlägigen Rechtsgrundlagen sind dieselben wie die, die in den Leitlinien 04/2020 erörtert wurden. Soweit sich das nationale Recht auf ein öffentliches Interesse stützt, muss es unter Umständen angepasst werden, um den Datenaustausch mit anderen Diensten vorzusehen. Im Falle der Einwilligung wird für die im Rahmen der Interoperabilität erfolgende Verarbeitung eine zusätzliche Einwilligung einzuholen sein, die alle dafür geltenden Anforderungen erfüllt. Insbesondere muss die Einwilligung spezifisch und somit ausreichend granular sein.[7] Wenn sich die verschiedenen für die Verarbeitung Verantwortlichen der Kontaktnachverfolgungs-Apps auf unterschiedliche Rechtsgrundlagen stützen, sind unter Umständen zusätzliche Maßnahmen erforderlich, um die Rechtsgrundlage betreffende Rechte der betroffenen Personen zu implementieren. Soweit es um Gesundheitsdaten geht, findet Artikel 9 DSGVO Anwendung, und die Verantwortlichen werden einen der dort aufgeführten Ausnahmetatbestände erfüllen müssen.

Verantwortlichkeit

13. Der EDSA möchte klarstellen, dass eine abschließende Erklärung bezüglich der jeweiligen Rollen der verschiedenen an der Verarbeitung mitwirkenden Akteure im Einzelfall auf Grundlage der

---

[6] Siehe auch: Artikel-29-Datenschutzgruppe, „Leitlinien für Transparenz gemäß der Verordnung“, WP260 rev.01, 11. April 2018 – vom EDSA gebilligt.

[7] Siehe auch Abschnitt 3.1.3 Granularität der Leitlinien 05/2020 des EDSA über Einwilligung im Sinne der Verordnung 2016/679.

tatsächlichen Umstände der ausgeführten Verarbeitung zu bewerten ist. Der EDSA möchte jedoch hervorheben, dass es wichtig ist, bei der Gestaltung einer Lösung diese Rollen und Verantwortlichkeiten mit der gebotenen Sorgfalt zu berücksichtigen. Die folgenden Ausführungen können daher nur als allgemeine Richtschnur dienen.

14. Nach Meinung des EDSA ist jeder Vorgang oder jede Vorgangsreihe, die der Sicherstellung der Interoperabilität dient und zusätzlich zur Verarbeitung für die Zwecke der Funktionalität von Anwendungen auf der Mitgliedstaatsebene erfolgt, getrennt von den vorherigen oder anschließenden Verarbeitungsvorgängen zu bewerten, weil es sich um einen zusätzlichen Zweck handelt. Diese zusätzliche Verarbeitung sollte daher als gesonderte Verarbeitung betrachtet werden. Hinsichtlich dieses gesonderten Verarbeitungsvorgangs können die Parteien jeweils einzeln oder gemeinsam für die Verarbeitung Verantwortliche sein; sie können auch Auftragsverarbeiter einschalten. Jede nach dem Austausch der Kennungen erfolgende Verarbeitung (Expositionsberechnung, Versenden von Warnmeldungen an festgestellte Kontaktpersonen usw.) fände unter der gesonderten Verantwortung des App-Anbieters statt, der die Daten empfängt.

15. Die jeweiligen Rollen, Beziehungen und Verantwortlichkeiten der gemeinsam für die Verarbeitung Verantwortlichen gegenüber der betroffenen Person sind festzulegen, und diese Informationen sollten dann der betroffenen Personen mitgeteilt werden.[8] Dies wird Auswirkungen auf den Umfang der durchzuführenden Datenschutz-Folgenabschätzung haben, auch auf die für die Zwecke der Interoperabilität durchgeführte Verarbeitung. Mit der Verarbeitung zum Zwecke der Sicherstellung der Interoperabilität kann ein Auftragsverarbeiter betraut werden, der die in Artikel 28 DSGVO genannten Voraussetzungen erfüllt.

Ausübung der Rechte betroffener Personen

16. Jede interoperable Lösung muss für die betroffenen Personen eine Möglichkeit vorsehen, ihre Rechte auszuüben. Die Rechtsausübung darf den betroffenen Personen nicht erschwert werden, und es sollte klar sein, an wen sich die betroffenen Personen wenden müssen, um ihre Rechte auszuüben. Beschränkungen der Ausübung der Rechte betroffener Personen sind in den in den Artikeln 11[9] und 23 DSGVO vorgesehenen Ausnahmefällen möglich.

Datenspeicherung und Datenminimierung

17. Unterschiede bezüglich des festgelegten Datenspeicherungszeitraums sollten nicht dazu führen, dass die Daten länger aufbewahrt werden als notwendig.[10] Im Hinblick auf die wirksame Anwendung der Datenschutzgrundsätze sollten ein gemeinsames Niveau der Datenminimierung und ein gemeinsamer Datenspeicherungszeitraum in Betracht gezogen werden. Wie bereits erwähnt, sollte die Interoperabilität nicht dazu führen, dass mehr Informationen gesammelt werden, weil es an einem koordinierten Ansatz fehlt. Dies ist dem Nutzer klar mitzuteilen, bevor der Datenaustausch beginnt.

---

[8] Der EDSA wird die Verarbeitung in gemeinsamer Verantwortlichkeit in seinen Leitlinien zu den Begriffen des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters im Sinne der DSGVO, die demnächst erlassen werden, näher ausführen.

[9] Wie in den Allgemeinen Erwägungen ausgeführt wurde, geht mit der Interoperabilität die Verarbeitung pseudonymisierter personenbezogener Daten einher.

[10] Siehe dazu auch die Leitlinien 03/2020 des EDSA für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch.

Informationssicherheit

18. Die Interoperabilität sollte keine Beeinträchtigung der Datensicherheit und des Schutzes personenbezogener Daten bewirken. Der EDSA empfiehlt den Anbietern von Anwendungen zur Kontaktnachverfolgung, jede Erhöhung der Risiken in Bezug auf die Informationssicherheit, die sich durch die zusätzliche Verarbeitung und die Mitwirkung zusätzlicher Akteure ergibt, zu berücksichtigen. Dies betrifft vor allem die Sicherheit der Daten im Transit wegen der möglichen Kopplung von Back-End-Servern. In der Datenschutz-Folgenabschätzung ist insbesondere auf die mit der Interoperabilität verbundenen Sicherheitsrisiken einzugehen, die Auswirkungen auf die Rechte und Freiheiten natürlicher Personen haben.

Richtigkeit der Daten

19. Anbieter, die darüber nachdenken, ihre Anwendungen zur Kontaktnachverfolgung interoperabel zu gestalten, sollten soweit wie möglich sicherstellen, dass dies weder die Qualität noch die Richtigkeit der Daten beeinträchtigt. Wo große Unterschiede bestehen, kann die Interoperabilität zu Einbußen bei der Datenqualität führen (z. B. Falschbeurteilungen, schlechte Risikoeinstufung), was wiederum zu mehr falschen Positivmeldungen führen könnte. Diese zusätzlichen Risiken bezüglich der Richtigkeit der Daten müssen den betroffenen Personen klar mitgeteilt werden.

20. Die Maßnahmen, die die Richtigkeit der Daten sicherstellen sollen, müssen auch im interoperablen System erhalten bleiben.

Schlussfolgerung

21. Der EDSA ist sich bewusst, dass die Schaffung eines interoperablen Anwendungsnetzwerks nicht einfach ist. Die Interoperabilität könnte die Effektivität der Anwendungen erhöhen; unter Umständen erfordert sie jedoch grundlegende Änderungen der bereits bestehenden oder in Entwicklung befindlichen Anwendungen. Unter dem Gesichtspunkt des Datenschutzes ist Interoperabilität möglich, sofern die Empfehlungen in dieser Erklärung wie auch diejenigen in den Leitlinien 04/2020 des EDSA[1] befolgt werden. Wenn man die betroffenen Personen informiert und ihnen Kontrolle einräumt, werden sie den Lösungen mehr vertrauen und die Anwendungen eher benutzen.

22. Anwendungen zur Kontaktnachverfolgung können nur eine vorübergehende Lösung einer umfassenden öffentlichen Gesundheitsstrategie zur Pandemiebekämpfung sein. Für jede eingeführte Maßnahmen ist zu beurteilen, ob eine weniger in die Rechte eingreifende Alternative denselben Zweck erreichen kann, und es ist sicherzustellen, dass jede angewandte Maßnahme wirksam und verhältnismäßig ist.

Für den Europäischen Datenschutzausschuss

Vorsitz

(Andrea Jelinek)