Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 26.03.2021

Kontaktnachverfolgung in Zeiten der Corona-Pandemie
Praxistaugliche Lösungen mit einem hohen Schutz personenbezogener Daten verbinden

Mittlerweile bieten verschiedene Unternehmen digitale Lösungen zur Verarbeitung der Kontaktdaten von Kunden, Gästen oder Veranstaltungsteilnehmern an. Die App „luca“ des Unternehmens culture4life GmbH hat dabei in den vergangenen Wochen besonderes mediales Interesse erfahren. Culture4life hat bei mehreren Aufsichtsbehörden um ein datenschutzrechtliches Votum zu der Lösung ersucht. Darüber hinaus haben einige Länder und Landkreise die Absicht bekundet, diese App einzuführen und dann eine Verbindung zu den jeweiligen Gesundheitsämtern herzustellen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist ausdrücklich darauf hin, dass digitale Verfahren zur Verarbeitung von Kontakt- und Anwesenheitsdaten datenschutzkonform betrieben werden müssen. Um eine bundesweit einheitliche datensparsame digitale Infektionsnachverfolgung zu ermöglichen, fehlt es bislang allerdings an gesetzlichen Regelungen. Hierfür sollten bundeseinheitliche normenklare Vorgaben zur digitalen Kontaktnachverfolgung geschaffen werden.

Die Digitalisierung der Kontaktnachverfolgung erlaubt nicht nur, die Arbeit der Gesundheitsämter effizienter zu gestalten und es Veranstalterinnen und Veranstaltern zu erleichtern, ihren Dokumentationspflichten nachzukommen. Sie kann auch im Hinblick auf den Datenschutz zu positiven Effekten führen: Eine digitale Erhebung und Speicherung kann bei entsprechender technischer Ausgestaltung durch eine geeignete dem Stand der Technik entsprechende Verschlüsselung inklusive eines geeigneten sicheren Schlüsselmanagements einen im Vergleich mit Papierformularen besseren Schutz der Kontaktdaten vor unbefugter Kenntnisnahme und Missbrauch gewährleisten. Ideal ist, wenn die Daten auf eine Weise Ende-zu-Ende verschlüsselt werden, dass auch der Betreiber des Kontaktnachverfolgungssystems sie nicht lesen kann. Ein gutes Kontaktnachverfolgungssystem stellt darüber hinaus automatisiert die fristgemäße und datenschutzkonforme Datenlöschung sicher. Ein weiterer Vorteil wird erzielt, wenn das System seinen Nutzerinnen und Nutzern beziehungsweise den Veranstalterinnen und Veranstaltern einen Weg zur sicheren Übermittlung von Daten zur Verfügung stellt, sobald das Gesundheitsamt die Daten zur Kontaktnachverfolgung benötigt. Die vielfach praktizierte Übermittlung per E-Mail oder Fax kann dann minimiert werden. Schließlich können betroffene Personen unverzüglich per App unterrichtet werden, wenn nach einem Besuch einer Einrichtung

oder Veranstaltung ein Infektionsrisiko bekannt wird. Auch diese Benachrichtigung erfolgt in idealer Weise so, dass Systembetreiber und Veranstalter sowie deren Dienstleister keine Rückschlüsse auf das Verhalten einzelner Personen, ihre Anwesenheit bei Veranstaltungen oder ihren Gesundheitszustand ziehen können.

Eine klare Verteilung der datenschutzrechtlichen Verantwortung für die Verarbeitung der personenbezogenen Daten ist Grundvoraussetzung für ein datenschutzkonformes Verfahren. Darüber hinaus muss die Gewährung von Betroffenenrechten transparent und eindeutig geregelt sein und die Freiwilligkeit der Teilnahme an einer digitalen Erhebung sichergestellt werden. Auch gilt wie bei der papiergebundenen Erhebung die im Infektionsschutzgesetz festgelegte strenge Zweckbindung, wonach eine Nutzung der Kontakt- und Anwesenheitsdaten zu anderen Zwecken als der Kontaktnachverfolgung untersagt ist. Dies muss von den Systembetreibern durch technische und organisatorische Maßnahmen abgesichert werden.

Die culture4life GmbH hat nach derzeitiger Kenntnis der DSK in dem Luca-System die oben genannten Vorteile realisiert und bisher identifizierte Risiken teilweise behandelt. Die DSK fordert das Unternehmen dennoch auf, weitere Anpassungen an dem System vorzunehmen, um den Schutz der teilnehmenden Personen weiter zu erhöhen.

Der derzeitigen Ausgestaltung des Luca-Systems zufolge werden die in dem Kontaktnachverfolgungssystem gesammelten Daten an einer zentralen Stelle gespeichert. Es wird dort also eine große Zahl von Informationen über die Anwesenheit von Bürgerinnen und Bürgern in Einrichtungen verschiedenster Art und über ihre Teilnahme an Veranstaltungen unterschiedlichster Natur vorgehalten. Die unbefugte Einsicht in diesen großen Datenbestand kann je nach Umfang zu einer schweren Beeinträchtigung für die Einzelnen und das Gemeinwesen führen. Aufgrund dieses Risikos werden die Mitglieder der DSK mit dem Betreiber des Luca-Systems erörtern, inwieweit mit einer dezentralen Speicherung, die von der DSK prinzipiell für vorzugswürdig erachtet wird, den fachlichen Belangen der Pandemiebekämpfung und den gesetzlichen Vorgaben in gleichem Umfang und mit gleicher Effizienz nachgekommen werden kann.

Die Entwickler des Luca-Systems begegnen dem einer zentralen Speicherung immanenten Risiko durch die Verschlüsselung der gespeicherten Daten. Nach dem Verschlüsselungskonzept muss der Veranstalter mit einem beliebigen Gesundheitsamt zur Entschlüsselung der Daten zusammenwirken. Die DSK begrüßt die Vornahme einer Verschlüsselung grundsätzlich. Allerdings haben alle Gesundheitsämter die gleichen Schlüssel für die Entschlüsselung der Kontaktdaten. Deren Verwaltung liegt in einer Hand, der der culture4life GmbH. Das birgt das vermeidbare Risiko, dass durch das Ausspähen oder den Missbrauch dieser Schlüssel auf eine hohe Anzahl der von dem System zentral verwalteten Daten unberechtigt zugegriffen werden kann. Ebenso ist es für die Veranstalterinnen und Veranstalter

schwierig zu überprüfen, ob eine Anforderung zur Entschlüsselung berechtigt erfolgt, so dass sie dazu gebracht werden könnten, Daten ohne legitime Anforderung zu entschlüsseln. Ein erfolgreicher Angriff auf die Systeme der culture4life GmbH kann daher die Sicherheit des Gesamtsystems in Gefahr bringen.

Die angekündigte Offenlegung des Quellcodes der bereitgestellten Apps, der Webanwendungen und der zentral betriebenen Dienste wird eine Überprüfung durch unabhängige Dritte ermöglichen. Die jüngst bekannt gewordene Fehlfunktion in der Rufnummernüberprüfung unterstreicht allerdings, dass eine systematische Überprüfung auf die Einhaltung grundlegender Sicherheitsprinzipien für die Programmierung von Internetdiensten erfolgen muss. Die DSK betont, dass für zentral betriebene Dienste wie dem Luca-System ein systematischer Nachweis der Sicherheit des Systems unerlässlich und durch die DS-GVO vorgeschrieben ist.

Generell werden die zuständigen Datenschutz-Aufsichtsbehörden mit den Anbietern digitaler Lösungen zur pandemiebedingten Kontaktnachverfolgung im Gespräch bleiben, um vertrauenswürdige, risikoarme und datenschutzkonforme Verfahren sicherzustellen, die den fachlichen Bedürfnissen der Gesundheitsämter genügen.

Die DSK wird außerdem eine eigenständige Orientierungshilfe für alle Betreiber solcher Kontaktverfolgungssysteme mit allgemeinen Anforderungen für die digitale Kontaktnachverfolgung erarbeiten und kurzfristig veröffentlichen. Die DSK fordert die Gesetzgeber auf Landes- und Bundesebene auf, bundeseinheitliche gesetzliche Regelungen zur digitalen Kontaktnachverfolgung zu schaffen. Dabei ist auch zu prüfen, inwieweit mit datensparsameren Verfahren das Ziel der Kontaktnachverfolgung im Rahmen der aktuellen Pandemiebekämpfung erreicht werden kann.