

Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 2021

Stellungnahme zu Kontaktnachverfolgungssystemen – insbesondere zu „Luca“ der culture4life GMBH¹

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) unterstützt die Entwicklung und den datenschutzkonformen Einsatz von Kontaktnachverfolgungssystemen. Digitale Anwendungen für diesen Zweck erleichtern die Erfüllung der Aufzeichnungspflichten von Veranstaltern und können die Kontaktnachverfolgung durch die Gesundheitsämter beschleunigen. Zudem können sie im Vergleich zur Führung von schriftlichen Listen den Vorteil bieten, dass den Veranstaltern keine Namen oder andere identifizierende Angaben über ihre Gäste bekannt werden und diese Angaben auch gegenüber Dritten durch Verschlüsselung geschützt werden. Die DSK hat daher zeitgleich eine Orientierungshilfe zu digitalen Kontaktnachverfolgungssystemen veröffentlicht, in der die datenschutzrechtlichen Anforderungen aufgezeigt werden, die an derartige Systeme und ihren Betrieb anzulegen sind.

Die Mehrzahl der Länder der Bundesrepublik Deutschland hat sich dafür entschieden, vertragliche Vereinbarungen mit dem Diensteanbieter culture4life GmbH über das Kontaktnachverfolgungssystem „Luca“ einzugehen. Dadurch ist „Luca“ Gegenstand verschiedener datenschutzaufsichtlicher Untersuchungen geworden. Die DSK hat in ihrer Stellungnahme „Kontaktnachverfolgung in Zeiten der Corona-Pandemie – Praxis-taugliche Lösungen mit einem hohen Schutz personenbezogener Daten verbinden“ vom 26.03.2021 eine erste vorläufige Bewertung dieses Systems vorgenommen.

Weitere Untersuchungen der Aufsichtsbehörden haben gezeigt, dass manche Risiken, die sich - trotz der dem Grunde nach tragfähigen Konzeption des Luca-Systems - insbesondere im Bereich der durchgängig verschlüsselten Kontaktdaten durch den nun geplanten weitverbreiteten Einsatz mit erhöhten Wahrscheinlichkeiten von missbräuchlicher Nutzung ergeben, weitere technische Schutzmaßnahmen erforderlich machen. Seit der Veröffentlichung der Stellungnahme der DSK sind auch weitere Kritikpunkte in der Öffentlichkeit und Presse erörtert worden, die einzuordnen sind.

Wie bei den bisher eingesetzten Papierdokumenten auch können Fake-Identitäten bei der Inbetriebnahme der Luca-App auf dem Smartphone eines Nutzers statt der eigenen verwendet werden. Dies führt aufgrund der Möglichkeit von beispielsweise automatisierten Angriffen zu einem erhöhten Missbrauchsrisiko.

¹ Die Stellungnahme wurde durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder unter der Enthaltung von Baden-Württemberg beschlossen.

Wird eine dritte Person z. B. so missbräuchlich in das System eingetragen, kann dies dazu führen, dass sie im Zuge der Kontaktnachverfolgung von einem Gesundheitsamt angesprochen und unter Umständen sogar verpflichtet wird, ihre Wohnung nicht oder nur unter bestimmten Bedingungen zu verlassen, obwohl es nie zu einem Kontakt mit einer infizierten Person gekommen ist. Die zur Verhinderung genau dieses Umstands eingesetzte Rufnummernüberprüfung lässt sich für technisch versierte Angreifer umgehen und kann ihrerseits zur Belästigung von Personen missbraucht werden, die dann SMS-Nachrichten mit Bestätigungs-codes erhalten würden. Die Konferenz weist die Gesundheitsämter darauf hin, dass sie bis zur Korrektur dieses Verhaltens des Systems - wie bei Papierdokumenten auch - nicht von der Korrektheit der ihnen vorgelegten Kontaktdaten ausgehen können. Unabhängig davon bleiben durch den Anbieter technische Abhilfemaßnahmen umzusetzen. Dies wurde gegenüber den Aufsichtsbehörden durch den Anbieter bereits angekündigt.

Darüber hinaus kann es insbesondere bei Aushang ausgedruckter QR-Codes durch Veranstalter zu einer massenhaft missbräuchlichen Vornahme von Eintragungen in das System kommen, ohne dass sich die eintragenden Personen tatsächlich am angegebenen Ort aufgehalten haben. Daraus können sich Überlastungen der Gesundheitsämter mit Daten ergeben, die für die Kontaktnachverfolgung nutzlos sind, ohne dass dies von vornherein erkannt werden kann. Ein Kontaktnachverfolgungssystem, das nicht in der Lage ist, den Gesundheitsämtern valide Daten zu liefern, die diese für die Kontaktnachverfolgung effizient einsetzen können, wird seiner Zwecksetzung nicht gerecht. Es sollte derart abgesichert werden, dass zumindest das Gesundheitsamt beim Kontakt-Tracing missbräuchliche Einträge erkennen kann.

Zusätzliche Absicherungserfordernisse für Anbieter, Veranstalter aber auch für die betroffenen Personen ergeben sich außerdem, wenn als Ersatz für Smartphones von Luca bereitgestellte Schlüsselanhänger eingesetzt werden. Ziel muss es sein, auch diese Personen vor der Nachverfolgung ihrer Aufenthalte zu schützen.

Die genannten Sachverhalte treten zu den Grundrisiken, die in der zentralen Datenhaltung des Systems begründet sind, noch hinzu. Wie bereits in der Stellungnahme festgehalten, werden nicht alle Risiken durch die eingesetzten zweistufigen Verschlüsselungsmechanismen vollständig ausgeräumt. Nach dem derzeitigen Stand kann daher ein qualifizierter Angriff von Dritten gegen die zentralen IT-Systeme des Dienstes dazu führen, dass ab dem Zeitpunkt eines erfolgreichen Cyberangriffs die Funktionsweise des Luca-Systems manipuliert wird und im schlimmsten Fall die Angreifenden in großem Umfang Daten über die Anwesenheit von Personen bei Veranstaltungen etc. entschlüsseln und ausleiten können.

Die culture4life GmbH hat inzwischen eine Datenschutz-Folgenabschätzung und einen Arbeitsplan vorgelegt, mit dem in mehreren Schritten Nachbesserungen erreicht werden sollen. Die Konferenz anerkennt die Anstrengungen und die Kooperationsbereitschaft des Unternehmens und erwartet, dass dieser Arbeitsplan unverzüglich und mit der größtmöglichen Sorgfalt abzarbeiten ist. Das System weist dem Grunde nach

eine tragfähige technische Architektur auf. Dennoch erforderliche Weiterentwicklungen des Systems werden die zuständigen Aufsichtsbehörden fortlaufend kritisch prüfen.

Zugleich wird die Konferenz generell den Einsatz von Kontaktnachverfolgungssystemen beobachten, um ihrer Beratungsaufgabe gegenüber den Regierungen gerecht werden zu können. Dabei kommt der Anbindung der Kontaktnachverfolgungssysteme der Gesundheitsämter besondere Bedeutung zu. Neben der Nutzung von einer oder mehreren digitalen Anwendungen sollten den Veranstaltern auch alternative Möglichkeiten offenstehen und von ihnen ihren Gästen zur Verfügung gestellt werden.

Im Einklang mit der Position des Europäischen Datenschutzausschusses zu digitalen Werkzeugen für die Kontaktnachverfolgung betont die Konferenz, dass unabhängig von den beschriebenen Problemen die Nutzung von digitalen Kontaktnachverfolgungsdiensten in jedem Fall freiwillig sein muss, um das Risiko der Diskriminierung bei der Teilnahme am gesellschaftlichen Leben zu vermeiden und eine hohe Kooperationsbereitschaft zu fördern.