Kreis Rendsburg-Eckernförde
Informationssicherheitsbeauftragter
Behördlicher Datenschutzbeauftragter

01. April 2021

Stellungnahme zur digitalen Erfassungs-App „Luca“ für Teilnehmer- u. Gästelisten

Sachverhalt
Zur Vereinfachung der Kontaktnachverfolgung, die gemäß der Corona Bekämpfungsverordnung Schleswig-Holstein bei Veranstaltungen vorgeschrieben ist wird, derzeit häufig das Verfahren der „Luca App“ vorgeschlagen. Seitdem das Gesundheitsamt des Kreises Rendsburg-Eckernförde an dem Verfahren teilnimmt, steht es für alle potentiellen Gastgeber im Kreis Rendsburg-Eckernförde als Alternative zu den papiergebundenen Kontaktlisten zur Verfügung. Die Corona Bekämpfungsverordnung Schleswig-Holstein wurde dementsprechend angepasst, so dass auch aus rechtlicher Sicht ein softwaregestütztes Verfahren anstatt der Papierlisten verwendet werden kann.

Rechtsgrundlagen:
Die Verarbeitung personenbezogener Daten von COVID19-Infizierten und deren Kontaktpersonen ist zum Zwecke der Nachverfolgung von Infektionsketten und dem Pandemiemanagement auf Grundlage des Art. 6 Abs. 1 S. 1 lit. e, Abs. 3 DSGVO iVm. § 23 Abs. 1 LDSG SH iVm. § 16 Abs. 1 IfSG bzw. Art. 9 Abs. 1 DSGVO iVm. § 12 Nr. 1 und Nr. 3 LDSG SH iVm. § 16 Abs. 1, 6 Abs. 1 S. 1 lit. t IfSG ist rechtmäßig.

Kurzbeschreibung des Verfahrens
die Bürger/innen melden sich mit der Luca App an dem System an und hinterlegen Ihre personenbezogenen Daten (Name, Anschrift, Telefonnummer, optional E-Mail). Die Rufnummer wird durch das Verfahren selbst verifiziert. Optional können die Bürger/innen die GPS Standorterfassung für die App aktivieren, sie werden dann automatisch ausgeloggt, wenn sie den Bereich des Gastgebers verlassen.

Alle Daten werden mehrfach den verschlüsselt zentral in System abgespeichert. Es gibt hierbei drei Parteien:
a) Nutzer/innen
b) Gastgeber
c) Gesundheitsamt

Die jeweiligen Schlüssel liegen nur der zugehörigen Partei vor. Eine Entschlüsselung und damit Freigabe der Daten ist nur durch zwei Parteien möglich:
a) Das Gesundheitsamt fragt Kontaktlisten bei einem Gastgeber ab, dieser muss mit seinem Schlüssel die Daten freigeben, das Gesundheitsamt kann dann mit seinem Schlüssel die Daten entschlüsseln.
b) das Gesundheitsamt möchte auf freiwilliger Basis die 14-tägige Besuchshistorie eines/r Nutzer/in abfragen. Dieses geht nur mit seiner/ihrer Zustimmung und Freigabe.

Nur das Gesundheitsamt kann die Kontakt Daten auslesen, die Gastgeber haben, im Gegensatz zu dem Papierlisten, keinen Zugriff. Hierdurch erhöht sich der Datenschutz für die Besucher/innen.

Rechtliche Wertung
Verantwortlich für die Einhaltung des Datenschutzes sowie die Aufklärung der Nutzer/innen gemäß Art. 15 DSGVO ist der Anbieter des Verfahrens. Die Nutzer melden sich freiwillig an dem Verfahren an und schließen somit ein Vertragsverhältnis mit dem Anbieter ab.

Die Gastgeber bedienen sich dieses Verfahrens in Form einer Auftragsdatenverarbeitung und übernehmen beim Check-In der Gäste hierdurch die Verantwortung und Aufklärungspflicht den Gästen gegenüber. Dies betrifft auch auf Behörden zu, die das Luca Verfahren als Gastgeber, zum Beispiel im Rahmen von Gremiensitzungen, anwenden möchten

Die Gesundheitsämter als Empfänger der Daten sind nicht für das Verfahren verantwortlich, solange es nicht die Bürger/innen zur Nutzung verpflichtet. Die Daten werden den Gesundheitsämtern über das Verfahren nur nach Zustimmung entweder der Nutzer/innen oder der Gastgeber zur Verfügung gestellt, die Gesundheitsämter sind somit nur für die Datenverarbeitung ihrem Bereich ab Übergabe der Daten verantwortlich, so wie sie es bisher auch zum Beispiel bei der papierbehaftet der Kontaktliste sind.

Für das Verfahren wurde bisher keine Datenschutzfolgeabschätzung durchgeführt, da lediglich die Variante c) Gesundheitsamt Verwendung findet. Dieses wäre bei der Variante b) Gastgeber gemäß Art. 35 DSGVO erforderlich. Zudem weist das Verfahren bekanntermaßen einige sicherheitstechnische sowie datenschutzrechtliche Mängel auf. Es entspricht somit nicht den Anforderungen der DSGVO.

Abwägung:
Das Verfahren entspricht nicht den Anforderungen der DSGVO. Zudem werden in dem Verfahren teilweise sogar besonders schützenswerte Gesundheitsdaten gemäß Art. 9 DSGVO verarbeitet. Dies ist dann der Fall, wenn das Gesundheitsamt die Besuchshistorie eines/r Nutzer/in abfragt, da damit zugleich feststeht dass diese Person positiv auf das Corona Virus getestet wurde.

Auf der anderen Seite wurde das Verfahren in der Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 26.03.2021 trotz bestehender Mängel insgesamt positiv bewertet auch der Landesbeauftragte für Datenschutz Baden-Württemberg, Herr Dr. Stefan Brink, kommt in seine Beurteilung vom 17.02.2021 zu einem positiven Ergebnis. Dieses wurde allerdings im Nachgang kontrovers diskutiert, ebenso wie die zunächst anfänglich positive Äußerung der Landesbeauftragte für Datenschutz Schleswig-Holstein, Frau Hansen. Diese hat ihre Äußerung im Nachgang relativiert, da sie nicht im Quellcode gesehen habe und ihre Aussage lediglich als Empfehlung zum Vergleich zu anderen Kontaktdaten Apps verstanden lassen will.

Für das Verfahren sprechen darüber hinaus folgende Aspekte:

1. Das Verfahren ist nur für einen begrenzten Zeitraum angelegt. Es verliert nach dem absehbaren Auslaufen der Corona-Bekämpfungsverordnung SH seine Berechtigung.

2. Die Datenschutzerklärung des Verfahrens ist umfangreich und umfassend aussagekräftig. Es werden keine Unterauftragnehmer außerhalb des Geltungsbereichs der DSGVO aufgeführt. Die Löschfristen sind klar beschrieben, ebenso der Umfang der erfassten Daten. Der Verfahrensanbieter unterliegt somit vollständig der DSGVO.

3. Das Verfahren wird lediglich auf freiwilliger Basis als Alternative zu den papiergebundenen Kontaktlisten angeboten.

4. Für das Verfahren wird eine mehrfach Verschlüsselung der Daten geschrieben, wobei Entschlüsselung nur unter Einsatz von zwei Schlüsseln möglich ist. Dies bietet zunächst eine gute Sicherheit. Diese wird jedoch leider dadurch verringert, dass für die Gesundheitsämter offensichtlich stets der gleiche Schlüssel verwendet wird.

5. Die erfassten Daten enthalten lediglich Namen, Anschrift, Telefonnummer sowie optional eine E-Mail-Adresse, sowie die jeweils besuchten Aufenthaltsorte. Es wird also nicht mehr erfasst, als den Anbietern der den Smartphone zugrunde liegende Betriebssystem (iOS, Android) regelmäßig sowieso bekannt ist, beziehungsweise sein könnte. Zusätzlich werden derartige Daten über zahlreiche social-media-/Messenger-Apps ebenfalls mit erfasst. Es dürfte über alles betrachtet nur sehr wenig Smartphones geben, für die die Luca-App eine zusätzliche Datenerhebung bedeuten dürfte. Diese erweitert lediglich den Empfängerkreis der sowieso erhobene Daten von bisher nicht der DSGVO unterliegenden US-Unternehmen mit unzureichendem Datenschutzniveau um ein vollständig der DSGVO unterliegendem Unternehmen in einem ausführlich beschrieben Verfahren.

6. Die Gastgeber haben beim Einsatz des Verfahrens keinen Zugriff mehr auf die Kontaktdaten ihrer Gäste. Hierdurch erhöht sich das Datenschutzniveau für die Nutzer/innen. Missbrauchsfälle, wie unerwünschte Zusendung von Werbung, sind somit nicht mehr möglich.

Fazit:
Obwohl das Verfahren „Luca App“ nicht den Anforderungen der DSGVO entspricht, halten die Verfasser einen Einsatz der Variante c) Gesundheitsamt, unter den gegebenen Umständen für verantwortbar. Zudem besteht nur eine geringe datenschutzrechtliche Eingriffstiefe für die einzelnen Bürger.

Sollte das Verfahren als zusätzliches Angebot, nach der Variante b) Gastgeber, zur Erfassung von Kontaktdaten zum Beispiel im Bereich der Erfassung von Bürger/innen bei Besuchen der Kreisverwaltung oder zur Durchführung von Gremiensitzung zum Einsatz kommen, muss eine erneute Abwägung erfolgen.

Christian Kock (BDSB) Micha Mark Knierim (ISB)