Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg

2. März 2021

Stellungnahme des LfDI Baden-Württemberg zur App „Luca“

Der LfDI wurde von der Landesregierung Baden-Württemberg ersucht, zur rechtlichen und technischen Datenschutzkonformität der App „Luca“ der culture4life GmbH im Rahmen seiner Beratungsfunktion Stellung zu nehmen.

Seit Ende Januar 2021 steht der LfDI mit den App-Anbietern in Kontakt und hat umfangreiche sowohl rechtliche als auch technische Beratungsleistungen gegenüber den App-Anbietern erbracht. Diese haben mit außergewöhnlicher Offenheit die Untersuchungen des LfDI unterstützt und seine Hinweise und Empfehlungen soweit möglich umgesetzt. Auf Grundlage der Angaben der Anbieter der App, aber auch durch eigene Untersuchungen und Prüfvorgänge hat sich der LfDI ein eigenes, trotz der engen zeitlichen Rahmenbedingungen belastbares Bild von der Datenschutzkonformität der App „Luca“ gemacht. Neben dem LfDI hat auch die Konferenz der Datenschutzaufsichtsbehörden der Länder und des Bundes eine Prüfung von Kontaktverfolgungs-Apps angekündigt, die allerdings wesentlich breiter angelegt ist und deren Ergebnisse daher nicht zeitnah zu erwarten sind. Der LfDI selbst setzt seine Beratungsleistungen gegenüber dem App-Anbieter „Luca“ aktuell fort, um weitere Verbesserungen anzustoßen und umzusetzen.

Im Ergebnis empfiehlt der LfDI Baden-Württemberg den Einsatz der App „Luca“, sie ist datenschutzkonform nutzbar und erfüllt die Zwecke der Beschleunigung der Kontaktnachverfolgung durch die Gesundheitsämter und der datenschutzrechtlichen Verbesserung der Kontakterfassung durch Betreiber von gewerblichen, sozialen und künstlerischen Stätten und Veranstaltungen. Für den erfolgversprechenden Einsatz der App „Luca“ ist allerdings zuvor eine Änderung der Corona-VOen der Landesregierung erforderlich. Auch hierzu macht der LfDI Vorschläge.

Hinweis: Diese Stellungnahme enthält Angaben zu Betriebs- und Geschäftsgeheimnissen der culture4life GmbH und ist in dieser Form nicht zur Veröffentlichung bestimmt.

I. Rechtliche Ausführungen zur „Luca-App“ (Darstellung der Rechtmäßigkeit bzgl. Verantwortlichkeit, Rechtsgrundlage, DS-Erklärung und ADV und offene Restfragen)

Die von der culture4life GmbH, Berlin, betriebene „Luca-App“ (zu weiteren Informationen s. https://luca-app.de/) erfüllt im Wesentlichen zwei Funktionen:

Zum einen ermöglicht sie es ihren Nutzern, bei Besuchen von Veranstaltungen und bei sonstigen Gelegenheiten, die einer obligatorischen Erfassung der Besuchs- und Kontaktdaten zum Zweck der Kontaktnachverfolgung durch die Gesundheitsämter im Interesse des Infektionsschutzes unterliegen (wie sie in Umsetzung von § 28a Absatz 1 Nummer 17 des Infektionsschutzgesetzes, IfSG, derzeit etwa in § 6 der Corona-Verordnung des Landes Baden-Württemberg in der ab dem 1. März 2020 gültigen Fassung, CoronaVO, vorgesehen ist), ihre Kontaktdaten in einer Ende-zu-Ende verschlüsselten Art und Weise zu hinterlegen. Die Kontaktdaten können in diesem Falle ausschließlich durch das Gesundheitsamt entschlüsselt werden, wenn der zur Datenverarbeitung Verpflichtete (im Folgenden als pars pro toto ohne Ansehung des Geschlechts als „Veranstalter“ bezeichnet) die vom Gesundheitsamt aufgrund des Verdachts einer Infektion bei mindestens einer teilnehmenden Person konkret angeforderten Daten freigibt. Zum anderen kann der Nutzer – ebenfalls in Ende zu Ende verschlüsselter Weise – die Historie der von ihm aufgesuchten Orte mit verbindlicher Datenverarbeitung nach § 6 CoronaVO (im Folgenden als pars pro toto mit „Veranstaltungen“ bezeichnet) speichern und zusätzlich weitere Kontaktereignisse, die nicht nach § 6 CoronaVO datenverarbeitungspflichtig sind, ablegen. Da so entstandene – Ende zu Ende verschlüsselte – Kontakttagebuch kann jede die App nutzende Person im Falle der Anforderung durch das Gesundheitsamt wegen des Verdachts einer Infektion mit SARS-Cov-19 ebenfalls dem Gesundheitsamt so freigeben.

Einzelne Ergebnisse der rechtlichen Prüfung und Bewertung

Unserer datenschutzrechtlichen Prüfung lagen insbesondere die auf der Webseite https://luca-app.de/ verfügbaren Informationen einschließlich der Datenschutzinformationen und die aktuelle Fassung des Entwurfs eines Auftragsverarbeitungsvertrages zwischen einem Veranstalter und Vertreterin der

culture4life GmbH (im Folgenden: App-Betreiber) sowie verschiedene fernmündliche Auskünfte seitens des App-Betreibers zugrunde.

Der App-Betreiber wählt demnach in datenschutzrechtlicher Hinsicht im Wesentlichen die folgende Gestaltung:

Er schließt im Falle der App-Nutzung einen Nutzungsvertrag mit dem Endnutzer (m/w/d) und erhebt zur Erfüllung des Nutzungsvertrages im Rahmen des Registrierungsvorgangs dessen Kontaktdaten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe b DS-GVO. Die angegebene Telefonnummer validiert er durch ein SMS-TAN-Verfahren ebenfalls zum Zwecke der Vertragsdurchführung mit der nutzenden Person.

Die eingegebenen Kontaktdaten speichert der App-Betreiber (weiterhin zum Zwecke der Vertragsdurchführung mit der die App nutzenden Person) in Ende zu Ende verschlüsselter (also für den App-Betreiber selbst mangels Schlüssels nicht lesbarer) Form. Auch die Historie der besuchten Veranstaltungen (sowie ggf. weitere Einträge der nutzenden Person in ihrem Kontakttagebuch) speichert der App-Betreiber in dieser Form zur Erfüllung des Nutzungsvertrages. Soweit dabei Daten Dritter in Ende-zu-Ende verschlüsselter Form verarbeitet werden (also etwa der Veranstalter oder der sonstigen Personen, die der/die Nutzer[in] in das Kontakttagebuch einträgt), ist fraglich, ob es insoweit einer Rechtsgrundlage bedarf oder ob insoweit Artikel 2 Absatz 2 Buchstabe c DS-GVO greift: Zwar verarbeitet hier der App-Betreiber die Daten, der selbst keine natürliche Person ist und auch nicht persönliche oder familiäre Tätigkeiten ausübt; er tut dies aber für und auf Veranlassung der die App nutzenden Person, deren App-Nutzung insoweit noch als persönlich-familiäre Tätigkeit (Führung eines Kontakttagebuchs für sich selbst) eingestuft werden kann. Wollte man die Privilegierung des App-Nutzers durch Artikel 2 Absatz 2 Buchstabe c DS-GVO hier nicht auf den App-Betreiber „durchschlagen" lassen, könnte die Datenverarbeitung insoweit auf eine rechtliche Verpflichtung des App-Betreibers (Artikel 6 Absatz 1 Buchstabe c DS-GVO) oder seine berechtigten Interessen (Artikel 6 Absatz 1 Buchstabe f DS-GVO) gestützt werden. Die Frage stellt jedoch jedenfalls kein Sonderproblem der „Luca-App" dar, sondern taucht bei jedem zu privaten Zwecken genutzten Cloud-Dienst auf, weswegen sie hier nicht weiter vertieft werden soll (zumal im Rahmen der Abwägung nach Artikel 6 Absatz 1 Buchstabe f DS-GVO

zugunsten des Betreiber der „Luca-App“ noch zu berücksichtigen wäre, dass er selbst wegen der Ende-zu-Ende-Verschlüsselung die Daten nicht lesen kann).

Wenn ein Veranstalter die App als Tool zur Hinterlegung der Kontaktdaten (anstelle einer eigenen Erfassung und Speicherung der Daten i. S. v. § 6 CoronaVO) zulassen will, muss er seinerseits einen (nach Angabe des Betreibers kostenlos bleibenden) Nutzungsvertrag und einen Auftragsdatenverarbeitungsvertrag mit dem App-Betreiber schließen. Registriert sich dann ein App-Nutzer beim Veranstalter (indem entweder der Veranstalter oder der Nutzer einen entsprechenden QR-Code einscannt), wird – nach der derzeitigen technischen Ausführung der App – zu der Veranstaltung Ende-zu-Ende verschlüsselt eine Verknüpfung zur Identität des App-Nutzers (mit seinen beim App-Betreiber hinterlegten und ebenfalls Ende-zu-Ende-verschlüsselten Kontaktdaten) erstellt und gespeichert.

Datenschutzrechtlich ist der Veranstalter infolge der gewählten Konstruktion mit der Auftragsverarbeitung nunmehr i. S. v. Artikel 4 Nummer 7 DS-GVO für die unter seiner Veranstaltung hinterlegte und gespeicherte Verknüpfung zur Identität des App-Nutzers verantwortlich (auch wenn der Veranstalter infolge der Verschlüsselung die gespeicherten Kontaktdaten des Nutzers nicht selbst auslesen kann). In diesem Vorgang liegt mithin datenschutzrechtlich eine Übermittlung der Kontaktdaten des App-Nutzers vom App-Betreiber an den Veranstalter, da der App-Betreiber die Verknüpfung zu den Kontaktdaten insoweit für den Veranstalter als seinem Auftraggeber im Sinne von Artikel 28 DS-GVO speichert. Rechtsgrundlage für diese Übermittlung ist auf Seiten des übermittelnden App-Betreibers ebenfalls Artikel 6 Absatz 2 Buchstabe b DS-GVO, da die Übermittlung in Erfüllung des Nutzungsvertrages zwischen App-Nutzer und App-Betreiber erfolgt. Die Erhebung der Besuchs- und Kontaktdaten auf Seiten des Veranstalters findet dagegen ihre Rechtfertigung in Artikel 6 Absatz 2 Buchstabe c DS-GVO in Verbindung mit § 6 CoronaVO (und den weiteren Bestimmungen der Corona-Verordnung, welche die Datenverarbeitungspflicht normieren). Dasselbe gilt für die Speicherung der Daten durch den verantwortlichen Veranstalter für die gesetzlich vorgesehene Dauer von vier Wochen.

Fordert nunmehr das Gesundheitsamt die Daten des Kontakttagebuchs einer die App nutzenden Person auf der Grundlage von § 25 IfSG an, kann die die App nutzende Person die angeforderten Inhalte freigeben, und sie werden so

verschlüsselt an das Gesundheitsamt übertragen, dass nur das Gesundheitsamt die Daten mit dem bei ihm hinterlegten Schlüssel auslesen kann.

Stellt das Gesundheitsamt fest, dass ein Infizierter im maßgeblichen infektiösen Zeitraum auf einer Veranstaltung (bei der eine Datenverarbeitung nach § 6 CoronaVO vorgeschrieben ist) war, fordert es den Veranstalter zur Freigabe der Kontaktdaten derjenigen Besucher der Veranstaltung auf, die im relevanten Zeitraum anwesend waren. Nur wenn der Veranstalter diese Daten freigibt (wozu er nach §§ 25, 16 bzw. 28a Absatz 4 IfSG verpflichtet ist), kann das Gesundheitsamt sie auslesen (und zwar wegen der Verschlüsselung nur das Gesundheitsamt, nicht auch der Veranstalter oder der App-Betreiber). Zugleich ist das System Luca so gestaltet, dass in diesem Falle diejenigen Besucher der Veranstaltung, deren Daten übermittelt werden, (Ende zu Ende verschlüsselt) benachrichtigt werden, was einerseits der Transparenz im Sinne von Artikel 13 bzw. 14 DS-GVO dient und andererseits den betroffenen Veranstaltungsbesucherinnen und –besuchern frühzeitig ermöglicht, die Frage ihrer eigenen Infektion abzuklären bzw. sich bis dahin vorsorglich in häusliche Absonderung zu begeben.

Die Verwendung der „Luca-App“ bietet in datenschutzrechtlicher Hinsicht gegenüber der bisherigen manuellen Erfassung insbesondere folgende Vorteile:

• Durch die vorgenommene Verschlüsselung können die Kontaktdaten bei Veranstaltungen gespeichert werden, ohne dass der Veranstalter die Daten in für ihn lesbarere Form verarbeitet. Die Nutzung der App stellt daher aus datenschutzrechtlicher Sicht eine ideale technische (und organisatorische) Maßnahme im Sinne von Artikel 32 DS-GVO dar, um eine zweckwidrige Verwendung durch den Veranstalter oder dessen Beschäftigte und eine unbefugte Kenntnisnahme und Verwendung durch Dritte (wie insbesondere andere Teilnehmende der Veranstaltung) zu verhindern.

• Zugleich wird durch die verwendete Verschlüsselung das Risiko eines Missbrauchs durch den App-Betreiber und durch Angreifer von außen auf das System reduziert.

• Die App ermöglicht entsprechend die hinreichend sichere Speicherung eines Kontakttagebuchs für ihre Nutzer.

• Die App ermöglicht die sichere elektronische Übermittlung sowohl der durch Veranstalter gespeicherten Besuchs- und Kontaktdaten als auch ggf. der Daten des Kontakttagebuchs einer sie nutzenden Person auf Anforderung durch das Gesundheitsamt.

• Bei Nutzung der App kann die datenschutzkonforme Vernichtung der durch Veranstalter zu speichernden Besuchs- und Kontaktdaten nach Ablauf der vorgeschriebenen Speicherfrist von vier Wochen sichergestellt werden.

Datenschutzrechtlich problematisch ist bei der derzeitigen technischen Ausgestaltung noch der Umstand, dass beim Veranstalter nicht der zum Zeitpunkt der Veranstaltung aktuelle Kontaktdatenbestand für den Veranstalter abgelegt wird, sondern nur eine Verknüpfung zu dem jeweils aktuellen Kontaktdatenbestand des App-Nutzers bei der App.

Dies hat datenschutzrechtlich insbesondere folgende Nachteile:

• Ändert der App-Nutzers seinen Kontaktdatenbestand (sei es wegen Umzugs oder in böswilliger Absicht, um sich befürchteten Maßnahmen des Gesundheitsamts zu entziehen) nach Besuch der Veranstaltung, wird nicht der bei Besuch der Veranstaltung aktuelle Datenbestand für den Veranstalter gespeichert, sondern der geänderte. Darin liegt u. a. eine Übermittlung der geänderten Daten vom App-Betreiber an den Veranstalter (und eine Änderung der für diesen gespeicherten Daten), deren Rechtsgrundlage fraglich ist. Will allerdings der Nutzer seine Telefonnummer ändern, muss die geänderte Telefonnummer erneut mittels SMS-TAN-Verfahren verifiziert werden, so dass insoweit eine aktuelle Erreichbarkeit in gewissem Umfange gewährleistet ist.

• Wenn der Nutzer den Nutzungsvertrag kündigt, wird nur die Historie (und ggf. seine ergänzenden Eintragungen im Kontakttagebuch) sofort gelöscht. Die Kontaktdaten selbst speichert der App-Betreiber (Ende zu Ende verschlüsselt) vorsorglich 30 Tage lang weiter, um im Falle einer Anforderung seitens des Gesundheitsamtes noch die Besuchs- und Kontaktdaten herausgeben zu können. Die fortdauernde Speicherung der Daten (nicht nur als Auftragnehmerin einer Auftragsverarbeitung, sondern auch in eigener Verantwortung) ist datenschutzrechtlich nicht unproblematisch.

• Die App übermittelt aus demselben Grund bislang uneingeschränkt dem Veranstalter den gesamten zu einer Person hinterlegten Datenbestand, auch wenn nach den – insoweit teilweise unterschiedlichen länderspezifischen Regelungen – der Veranstalter zu deren Verarbeitung nicht verpflichtet ist. So sieht die Corona-Verordnung in Baden-Württemberg zu Recht davon ab, die Veranstaltern zur rhebung der E-Mail-Adresse zu verpflichten, weil die Gesundheitsämter diese mit Blick auf die besondere Schutzbedürftigkeit von Gesundheitsdaten ohnehin nicht datenschutzkonform nutzenden dürften (in anderen Ländern ist dagegen z. B. die Anschrift nicht zu erheben). Die App übermittelt derzeit gleichwohl die E-Mail-Adresse.

Dieses Problem haben wir dem App-Betreiber gegenüber angesprochen. Er hat sich zur Klärung und ggf. Überarbeitung – ggf. unter Berücksichtigung des für den jeweiligen Veranstalter geltenden Landesrechts – bereiterklärt. Für den Infektionsschutz kann die derzeitige technische Gestaltung mit Blick auf die Aktualität der Telefonnummer allerdings auch Vorteile haben.

Im Übrigen sind noch einige kleinere Änderungen der Datenschutzinformation und beim Entwurf des Auftragsverarbeitungsvertrages für die Veranstalter vorzunehmen. Dies hat der App-Betreiber zugesagt und sich – wie generell – sehr kooperativ gezeigt.

Ebenfalls zugesagt hat der App-Betreiber – über seine datenschutzrechtlichen Pflichten hinaus – die Erstellung einer Muster-Datenschutzinformation für die Veranstalter als seine Auftraggeber i. S. v. Artikel 28 DS-GVO und einer Datenschutz-Folgenabschätzung. Insoweit sollen uns in dieser Woche weitere Entwürfe vorgelegt werden.

Aus Sicht des Infektionsschutzes ist noch darauf hinzuweisen, dass bei Nutzung der App die in § 6 Absatz 2 CoronaVO vorgesehene Vollständigkeits- und Plausibilitätskontrolle der bei der App hinterlegten Kontaktdaten durch den Veranstalter grundsätzlich etwas gegenüber dem Istzustand eingeschränkt sein könnte, ebenso die Möglichkeiten der Verfolgung einer Ordnungswidrigkeit nach § 19 Nummer 10 CoronaVO. Allerdings kann der App-Nutzer jederzeit von Berechtigten (z. B. ggf. der Ortspolizeibehörde) angehalten werden, die aktuell bei der App hinterlegten Daten auf seinem Smartphone anzuzeigen. Im Übrigen bietet die App

durch die Verifizierung des Telefonanschlusses im Wege des SMS-TAN-Verfahrens für diese Kontaktmöglichkeit eine gegenüber dem Ist-Zustand erhöhte Richtigkeitsgewähr.

Ergebnis der rechtlichen Prüfung: Die App „Luca" der culture4life GmbH kann als Ersatz der manuellen Führung von Corona-Kontaktlisten in Restaurants und bei Veranstaltungen datenschutzkonform verwendet werden. Insgesamt überwiegen aus unserer Sicht die Vorteile für den Datenschutz bei Zulassung der App-Nutzung die skizzierten möglichen Nachteile bei weitem.

II. Ausführungen zur technischen Prüfung und den technischen Anforderungen an eine solche App

Die App steht sowohl für Android als auch für iOS zur Verfügung. Zusätzlich gibt es eine Web-Version, die mit normalen Browsern genutzt werden kann. Angaben zur Funktionalität der App von Seiten der Betreiber finden sich in Anlage zu dieser Stellungnahme.

Für die kursorische technische Analyse wurden folgende zu prüfende Themenbereiche identifiziert, die üblicherweise bei solchen Apps auftreten:

1. **Tracking**
   Enthalten die Apps Tracking-Elemente von Drittanbietern oder vom Hersteller selbst, mit denen das Nutzungsverhalten der Anwender erfasst und u.U. an Dritte wie Werbedienstleister oder Soziale Netzwerke weitergegeben wird?
2. **App-Sicherheit**
   Einfache statische Analyse der App auf potentielle Sicherheitslücken.
3. **Drittstaatentransfer**
   Werden (personenbezogene) Daten in Staaten außerhalb des Geltungsbereichs der DS-GVO übermittelt?
4. **Verwendung von Daten zu eigenen Zwecken des Herstellers**
   Finden Verarbeitungen zu eigenen Zwecken des Herstellers statt?
5. **Transportverschlüsselung**
   Findet eine ausreichende Transportverschlüsselung statt und kommen nur Algorithmen zum Einsatz, die vom BSI empfohlen werden?
6. **Verschlüsselung der verarbeiteten Daten**
   Werden die Daten so verschlüsselt, dass weder die Betreiber der Plattform bzw. App noch Veranstalter bzw. Restaurants oder erfolgreiche Angreifer Daten lesen können? Erhalten nur berechtigte Stellen Daten im Klartext?

Basis der Untersuchungen sind neben eigener Analyse die vom Hersteller am 28.1.2021 zur Verfügung gestellten Dokumente „Technische Dokumentation“ (Luca_KK-280121-1434-156.pdf) und „Luca Security Concept“ (LUCA-LucaSecurityConcept-280121-1434-156.pdf), die technische Untersuchung der Verschlüsselung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) vom 10. Dezember 2020 (Az. 838-64/2020.14) und die Ergebnisse des Gespräches mit dem Hersteller Nexenio GmbH vom 29.1.2021.

Die hiesigen Untersuchungen können zeitlich bedingt keine umfassenden Sicherheits-Audits ersetzen, bilden jedoch in vertretbarer Weise die Sicherheitsstandards der App „Luca“ ab.

Zusammenfassung der technischen Prüfung

Im Gegensatz zu Kontaktlisten auf Papier kann eine solche App sowohl den Komfort für Nutzende und Veranstalter erhöhen, als auch die gebotene Datensicherheit erhöhen. Wichtig ist dazu, dass es keine zentrale Stelle gibt, die Daten alleine entschlüsseln kann. Dies reduziert signifikant die Wahrscheinlichkeit sowohl für erfolgreiche Angriffe durch Innentäter als auch von erfolgreichen Angriffen durch Schadsoftware oder sonstige externe Angreifer wie Hacker. Selbst für den Fall, dass diese Zugriff auf die Daten bekommen, sollten sie für diese nicht lesbar sein.

Bei der Untersuchung der konkreten App konnte dieses Ziel erreicht werden und es wurden keine schwerwiegenden Mängel gefunden.

Einzelne Ergebnisse der statischen App-Analyse zu potentiellen Sicherheitsproblemen sollten vom Hersteller künftig genauer betrachtet und untersucht werden. Zudem sollte die Konfiguration der Transportverschlüsselung verbessert werden.

Die Verschlüsselung der Daten der betroffenen Personen ist nach bisheriger Kenntnis sicher und gewährleistet, dass weder der Hersteller der App oder der Betreiber der Infrastruktur noch der Betreiber einer Veranstaltung bzw. eines Restaurants Zugriff auf die Daten haben kann. Dies gilt auch für (erfolgreiche) Angreifer, die Vollzugriff auf den Systemen der Beteiligten bekommen.

Um das Vertrauen der Nutzer in die App zu erhöhen, empfehlen wir, den Quellcode der App und möglichst auch der Server-Backends unter einer anerkannten Open-Source-Lizenz zu veröffentlichen.

Bei einzelnen weiteren Punkten sind weitere Verbesserungen möglich, mehr dazu im Folgenden.

Zu 1. Tracking

Bei der statischen Analyse der Android Version 1.2.5 mittels MobSF wurden keine bekannten Tracking-Bibliotheken gefunden.
Die dynamische Analyse des Datensendeverhaltens der App unter Android (1.2.5) und iOS (Version 1.3.1) hat ergeben, dass von der App aus keine Verbindungen zu Drittanbietern aufgenommen werden und kein Tracking durch Drittanbieter erfolgt.
Ein Tracking durch den Anbieter selbst konnte ebenso wenig festgestellt werden.

Allerdings wurde zum Zeitpunkt des Tests (28. und 29.1.2021) auf der „Marketing-Webseite" (https://app.luca-app.de/) Google Analytics eingesetzt. Da von dieser innerhalb der App Nutzungsbedingungen nachgeladen und eingebettet wurden, fanden entsprechende Übermittlungen statt. Im Gespräch mit dem Hersteller am 29.1.2021 wurde von diesem zugesichert Google Analytics aus der Webseite zu entfernen. Bei einem erneuten Test der Webseite am 1.3.2021 konnte dort eine Einbindung von Google Analytics nicht mehr festgestellt werden.

Zu 2. App-Sicherheit

Die Statische Analyse der Android App mittels MobSF ergab einige Auffälligkeiten. Die Code-Analyse hat vier potentielle schwerwiegende Schwachstellen identifiziert. Ob es sich hierbei um tatsächliche Bugs oder lediglich falsch-positive Meldungen handelt, ist erst durch eine manuelle Code-Verifikation feststellbar.
Die Ergebnisse wurden dem Hersteller zur Verfügung gestellt, damit dieser eine Prüfung vornehmen kann und, soweit sich der jeweilige Verdacht bestätigt, entsprechend nachbessert.

Die Entwickler nutzen zur Absicherung von Netzwerkverbindungen TLS-Cert-Pinning. Dies erschwert es Angreifern, den Datenverkehr im Klartext mitzuschneiden.

Zu 3. Drittstaatentransfer

Die App selbst kommuniziert nur mit dem host app.luca-app.de. Dieser Host hatte am 1.3. 2021 die IP-Adresse 80.158.46.50 (ASN AS6878) im Netzwerk der T-Systems International GmbH mit Sitz in Kiel. Es handelt sich um eine Adresse der Open Telekom Cloud. Der durchschnittlichen Paketlaufzeit vom LfDI-Testserver zufolge (ca. 11 ms) befindet sich der Server in Deutschland oder Europa.

Die Hosts luca-app.de (Marketing-Webseite, IP-Adresse 35.207.72.235) und www.luca-app.de (nur Umleitung auf die Marketing Webseite, IP-Adresse 35.207.105.25) gehören zur Google-Cloud. Paketlaufzeiten von 3,5 Millisekunden deuten auf einen physikalischen Standort in Deutschland hin.

E-Mails an Adressen @luca-app.de werden über den Microsoft-Server lucaapp-de01b.mail.protection.outlook.com geleitet, beim Hersteller kommt also Microsoft 365 zum Einsatz und Microsoft ist E-Mail-Diensteanbieter.

Inwieweit ein Restrisiko durch den Aufruf der Marketing-Webseite durch die App bei Anzeige von Datenschutzinformationen u.ä. sowie durch die Nutzung von Microsoft als E-Mail-Diensteanbieter bleibt und ob dieses durch technische oder vertragliche Maßnahmen ausreichend reduziert werden kann oder ein Umzug des Webservers bzw. E-Mail-Dienstes zu einem Anbieter mit Hauptsitz innerhalb des Geltungsbereichs der DS-GVO zu empfehlen ist, wäre künftig juristisch näher zu prüfen.

Zu 4. Verwendung von Daten zu eigenen Zwecken des Herstellers

Eine Verwendung von (personenbezogenen) Daten zu eigenen Zwecken des Herstellers oder Dienstebetreibers konnte im Rahmen dieser Prüfung nicht festgestellt werden. Laut Kryptografie-Konzept liegen dem Dienstebetreiber nur die Telefonnummern der Nutzenden vor, alle weiteren Daten sind für den Dienstebetreiber bzw. App-Hersteller nicht einsehbar verschlüsselt.

Zu 5. Transportverschlüsselung

Zur Absicherung der Kommunikation wird wie üblich Transport Layer Security (TLS) eingesetzt. Zur erhöhten Sicherheit vor Angriffen wird für einige (nicht alle) Verbindungen TLS-Cert-Pinning eingesetzt.
Die technische Richtlinie BSI TR-02102-2 des Bundesamts für Sicherheit in der Informationstechnik enthält Empfehlungen für Kryptografische Verfahren bei der Nutzung von TLS.
Die Empfehlungen des BSI werden teilweise umgesetzt:

Der API-Endpunkt unter https://app.luca-app.de verwendet ausschließlich TLS 1.2 (Mindestempfehlung BSI). Die Marketing-Webseite unter https:// luca-app.de

verwendet ausschließlich TLS 1.2 und 1.3. Ältere TLS- und SSL-Versionen sind bei beiden deaktiviert.

Folgende Cipher-Suiten (Kryptografische Verfahren) können dabei je nach Client auf dem wichtigen API-Endpunkt zum Einsatz kommen (in Reihenfolge der Präferenz), wobei nicht alle den Empfehlungen aus BSI TR-02102-2 entsprechen und z.B. kein PFS unterstützen:

Cipher-Suite	**Empfohlen in BSI TR-02102-2?**
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Ja
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Ja
TLS_RSA_WITH_AES_128_GCM_SHA256	NEIN
TLS_RSA_WITH_AES_256_GCM_SHA384	NEIN
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Ja
TLS_RSA_WITH_AES_128_CBC_SHA256	NEIN
TLS_RSA_WITH_AES_256_CBC_SHA256	NEIN
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Ja

Auf der Marketing-Website kommen zahlreiche weitere veraltete Cipher-Suiten zum Einsatz, wie TLS_RSA_WITH_AES_256_CBC_SHA oder TLS_RSA_WITH_CAMELLIA_128_CBC_SHA.

Der Hersteller sollte in dieser Hinsicht nacharbeiten und die BSI-Empfehlungen umsetzen.

Zu 6. Verschlüsselung der verarbeiteten Daten

Laut Eigendarstellung des Herstellers ist das Ziel, dass die Daten weder vom Betreiber einer Veranstaltung noch vom Luca-System gelesen werden können, sondern nur von den Gesundheitsämtern, um die Kontakte von Infizierten zu identifizieren und zu kontaktieren.

Nach Sichtung der zur Verfügung stehenden Unterlagen einschließlich der Analyse des TLfDI und dem Gespräch mit dem Hersteller wird dieses Ziel erreicht.

Weder Betreiber von Restaurants oder Veranstaltungen noch die Gesundheitsämter oder der App-Hersteller bzw. Dienstebetreiber haben alleine Zugriff auf die Daten.

Die von und durchgeführte Analyse der übermittelten Daten und des Datensendeverhaltens der App bestätigt, dass alle personenbezogenen Daten mit Ausnahme der Telefonnummer und der systemimmanenten IP-Adresse zusätzlich zur Transportverschlüsselung verschlüsselt übermittelt werden.

Prinzipiell bietet das System damit die Möglichkeit einer sicheren und datensparsamen Führung von Kontaktlisten in gewerblichen, sozialen und künstlerischen Stätten und bei Veranstaltungen.

Um die theoretischen Überlegungen zu untermauern und zu prüfen, ob Fehler in der konkreten Implementierung vorliegen, empfehlen wir, Sicherheits-Audits der App sowie aller Backend-Komponenten durchzuführen.

Ergebnis der technischen Prüfung: Die App „Luca" der culture4life GmbH kann als Ersatz der manuellen Führung von Corona-Kontaktlisten in Restaurants und bei Veranstaltungen datenschutzkonform verwendet werden. Durch die Verschlüsselung bietet sie in Bezug auf die Vertraulichkeit Vorteile gegenüber einer papiergestützten Verarbeitung oder mittels anderer gängiger Apps, da weder der Veranstalter noch der App- und Dienstebetreiber die Kontaktlisten einsehen kann.

III. Hinweise an die Landesregierung zur Änderung der Corona-VO

Infolge der vom App-Betreiber gewählten datenschutz-rechtlichen Konstruktion, dass er Besuchs- und Kontaktdaten im Wege der Auftragsverarbeitung für die i. S. v. § 6 CoronaVO zur Datenverarbeitung Verpflichteten (weiterhin als „Veranstalter" bezeichnet) speichert, ist nur ein geringer Eingriffe in den Text der Corona-Verordnung erforderlich, wenn die Landesregierung – was wir begrüßen würden – die Nutzung der App anstelle der Verarbeitung von Klardaten durch den Veranstalter gemäß der derzeitigen Fassung des § 6 CoronaVO zulassen will. Denn auch bei Nutzung der App erhebt und speichert der zur Datenverarbeitung Verpflichtete als Verantwortlicher im Sinne von Artikel 4 Nummer 7 DS-GVO die Besuchs- und Kontaktdaten, so dass keine Änderung bei der Bezeichnung der Person des zur Datenverarbeitung Verpflichteten vorzunehmen ist.

Allerdings geht die bisherige Fassung von § 6 CoronaVO ersichtlich davon aus, dass der zur Datenverarbeitung Verpflichtete die Kontaktdaten der Besucherinnen und Besucher in einer für ihn lesbaren Form erhebt (und speichert). Dies wird besonders augenfällig an der nach § 6 Absatz 2 CoronaVO vorzunehmenden Vollständigkeitskontrolle (die möglicherweise auch eine gewisse Plausibilitätskontrolle umfasst, da etwa bei Angabe des Namens „Donald Duck" offensichtlich eine Verweigerung der Namensnennung vorliegen dürfte und der Veranstalter den betreffenden Besucher wohl ausschließen müsste).

Um eine Nutzung der App zweifelfrei anstelle der Verarbeitung von Klardaten durch den zur Datenverarbeitung Verpflichteten zu ermöglichen, sollte daher in § 6 Corona-Verordnung (etwa in einem neuen Absatz) ergänzt werden, dass die Erhebung und Speicherung auch in einer für den zur Datenverarbeitung Verpflichteten nicht lesbaren Ende-zu-Ende-verschlüsselten Form nach dem Stand der Technik erfolgen kann, solange sichergestellt ist, dass das für den Ort des zur Datenverarbeitung verpflichtenden Ereignisses zuständige Gesundheitsamt die Daten im Falle einer Freigabe durch den zur Datenverarbeitung Verpflichteten in einer für das Gesundheitsamt lesbaren Form erhält.

Die Corona-Verordnung kann sodann – je nach politischem Gestaltungswillen – weitere Vorgaben machen. So kann sie vorgeben, dass bei dieser Art der Speicherung der Besucher in der Lage sein muss, zur Zeit des Veranstaltungsbesuchs den aktuell hinterlegten Kontaktdatenbestand anzuzeigen. Inwieweit es sinnvoll und praktikabel ist, eine Obliegenheit des zur Datenverarbeitung Verpflichteten zu normieren, die hinterlegten Daten sich einmal anzeigen zu lassen, um sie auf Vollständigkeit zu prüfen, und den Besucher im Falle der Unvollständigkeit von dem Veranstaltungsbesuch auszuschließen, wird die Landesregierung einzuschätzen haben. Eventuell könnte es sinnvoller sein, hier andere Vorgaben zu den Anforderungen an die Richtigkeitsgewähr zu machen. So könnte etwa die Anforderung normiert werden, dass in diesem Fall zumindest die Verfügungsbefugnis des Besuchers über die Telefonnummer durch die Durchführung eines SMS-TAN-Verfahren oder auf gleichwertige Art und Weise sichergestellt sein muss.

Weitere sinnvolle Ergänzungen in § 6 Corona-Verordnung wäre u. U. eine Bestimmung, dass im Falle einer digitalen Erhebung von Kontaktdaten alternativ nach Wahl der Besuchers eine nicht-digitale oder sonst barrierefreie Erfassung

(insbesondere eine solche ohne eigenes Endgerät) ermöglicht wird, um zu verhindern, dass Personen ohne Smartphone ausgeschlossen werden (vgl. § 5 Absatz 7 der Sächsischen Corona-Verordnung zum Stand 5. Februar 2021). Der Betreiber der „Luca-App" bietet z. B. auch die Nutzung eines Web-Portals ohne Registrierung an, die der Veranstalter durch Zur-Verfügung-Stellung eines entsprechenden Web-Zugangs vor Ort ermöglichen könnte.

Wegen der Vor- und Nachteile der Ausgestaltung der Corona-Verordnung im Einzelnen oder zur genauen Formulierung des Wortlauts stehen wir – wie stets bei Regelungen zum Datenschutz – der Landesregierung gerne zum Zwecke der Beratung zur Verfügung.

IV. Ergebnis

Aufgrund der gewonnenen Erkenntnisse empfehlen wir unter dem Blickwinkel des Datenschutzes der Landesregierung, die Nutzung solcher Apps in Baden-Württemberg durch entsprechende Ausstattung der Gesundheitsämter zu ermöglichen, nachdem die Corona-Verordnung des Landes entsprechend angepasst wurde.

Die geprüfte App ist aus Sicht des LfDI eine wertvolle Ergänzung der bisherigen staatlichen Schutzmaßnahmen zur Nachverfolgung von Kontakten während der Pandemie. Sie erfüllt die hohen Datenschutz-Standards der DS-GVO. Die Dokumentation der erfolgten Kontakte wird auf technisch höchstem Stand verschlüsselt und es liegt allein in der Hand des Luca-Nutzers, ob, wann und mit wem er diese sensiblen Daten teilen möchte. Die „Luca-App" kann einen sehr wertvollen Beitrag leisten, um die Gesundheitsämter bei der Nachverfolgung von Infektionsketten zu entlasten.

Stefan Brink
Landesbeauftragter für den Datenschutz und die Informationsfreiheit
Baden-Württemberg