BRANDI
RECHTSANWÄLTE

DATENSCHUTZ BEI DER NUTZUNG DER LUCA-APP

Informationen zum Datenschutz I April 2021

Einleitung

Die Ausbreitung des Corona-Virus stellt Arbeitgeber und Beschäftigte weiterhin vor große Herausforderungen. Eine Maßnahme zur besseren Eindämmung des Virus ist die Kontaktnachverfolgung, vor allem bei Publikums- und Kundenkontakt. Mit den entsprechenden Informationen können etwaige Infektionsketten nachverfolgt und potentiell infizierte Personen früher getestet werden, wodurch eine weitere Ausbreitung des Virus verhindert werden soll. Bei der dabei stattfindenden Verarbeitung personenbezogener Daten müssen die verantwortlichen Stellen aber sicherstellen, dass die datenschutzrechtlichen Vorgaben beachtet werden.

Zur Erleichterung der Kontaktnachverfolgung gibt es verschiedene softwaregestützte Lösungen. Eine der bekanntesten Angebote ist die App luca, die schon in vielen Bereichen zum Einsatz kommt. Es lohnt sich daher eine genauere Prüfung, welche datenschutzrechtlichen Besonderheiten bei dem Einsatz der luca-App und vergleichbaren Angeboten in Unternehmen beachtet werden müssen.

Funktionen der App

Nutzer von luca können durch die Registrierung in der App ihre Kontaktdaten dort hinterlegen. Wenn sie einen Ort, beispielsweise ein Unternehmen oder ein Restaurant, besuchen, an dem die App ebenfalls zum Einsatz kommt, können sie dort einen QR-Code scannen und dadurch der App mitteilen, dass sie den Ort besucht haben.

Indem Unternehmen also beispielsweise ihren Eingangsbereich oder auch einzelne Teile des Unternehmens, etwa Besprechungsräume, mit den entsprechenden QR-Codes ausstatten, haben Sie die Möglichkeit, Anwesenheiten von Mitarbeitern und Besuchern zu dokumentieren.

Gesundheitsämter können die App an ihre bestehenden Systeme anbinden. Die Daten zur Kontaktverfolgung können dadurch direkt über die App an das Gesundheitsamt übermittelt werden. Eine infizierte Person kann über die App ihre Besuchshistorie für das Gesundheitsamt freigeben. Das Gesundheitsamt erhält dadurch Informationen über die Aufenthaltsorte der Person in den letzten 14 Tagen. Es kontaktiert daraufhin die betroffenen Aufenthaltsorte und fordert sie auf, ihre zeitlich relevanten Check-ins über das luca-System an das Gesundheitsamt zu übermitteln. Die Check-ins werden von dem Gesundheitsamt entschlüsselt, wodurch es die Kontaktpersonen ermitteln und informieren kann.

Verarbeitung personenbezogener Daten

Mit der Nutzung der App geht die Verarbeitung personenbezogener Daten einher. Registriert sich ein Nutzer in der luca-App, was für die Nutzung zwingend erforderlich ist, werden Name und Kontaktdaten des Nutzers erfasst. Hierin liegt ein wesentlicher Unterschied zu der Corona-Warn-App, durch die keine Namen und Kontaktdaten erhoben werden. Bei dem Scannen eines QR-Codes mit der luca-App werden außerdem der Aufenthaltsort und die Aufenthaltsdauer des Nutzers erfasst. Über die „Geofencing-Funktion" der App kann sich ein Nutzer automatisch aus dem besuchten Ort „auschecken", wenn er den festgelegten Radius des Ortes verlässt. Diese Funktion muss allerdings aktiv von dem Nutzer eingeschaltet werden.

Durch die App können darüber hinaus weitere Informationen verarbeitet werden, wobei von dem Anbieter beispielhaft Sitzpläne, Schichtpläne, Bewohnerlisten, Einlasszeiten sowie Notizen in der Tagebuchfunktion genannt werden.

Rechtsgrundlage für die Datenverarbeitung

Der Einsatz der App in einem Unternehmen ist jedenfalls mit entsprechenden Einwilligungen der Betroffenen (Art. 6 Abs. 1 lit. a) DSGVO) möglich. In diesem Fall ist die Nutzung der App freiwillig und die betroffenen Personen können selbst darüber entscheiden, ob und welche Daten an die App und gegebenenfalls an das Gesundheitsamt übermittelt werden. Für eine wirksame Einwilligung ist es aber erforderlich, dass die Betroffenen transparent über die im Rahmen der Nutzung der App stattfindende Datenverarbeitung informiert werden. In der Pflicht ist insoweit zunächst der Anbieter der App, bei dem sich die Nutzer registrieren müssen und der die grundlegende Funktionsweise offenlegen muss. Die verantwortliche Stelle, die für die Kontaktnachverfolgung die luca-App einsetzt, kann insoweit dann auf die allgemeinen Erläuterungen verweisen. Soweit auf freiwilliger Basis die Nutzung der luca-App empfohlen wird, sollten für diejenigen, die sich gegen die Nutzung entscheiden, alternative Möglichkeiten der Kontaktdatenerfassung bereitgehalten werden. Das luca-System selbst bietet Möglichkeiten, ohne Download der App Kontaktdaten anzugeben, indem ein Kontaktformular ausgefüllt wird oder der Nutzer sich im Browser anmeldet. Wer das luca-System gar nicht nutzen möchte, sollte dann außerdem die Möglichkeit haben, seine Kontaktdaten auf ganz andere Weise, beispielsweise in Papierform, anzugeben.

Falls in einem Unternehmen überlegt wird, die luca-App für die Kontaktdatenerfassung verpflichtend einzusetzen und gegebenenfalls den Zutritt zu dem Unternehmen von der Datenerfassung über die luca-App abhängig zu machen, steht dies im Regelfall der Freiwilligkeit der Einwilligung nicht entgegen. Unternehmen steht es im Regelfall frei, zu definieren, unter welchen Voraussetzungen und Rahmenbedingungen Besuchern und Kunden ein Zutritt gewährt wird. Besucher und Kunden sind im Regelfall nicht gezwungen, die

Räumlichkeiten und Einrichtungen der verantwortlichen Stelle aufzusuchen, solange alternative Kontaktmöglichkeiten (etwa Onlinebestellungen) oder Wettbewerber verfügbar sind. Der Rückgriff auf die freiwillige Einwilligung kann aber in Konstellationen scheitern, bei denen etwa Mitarbeiter die luca-App nutzen müssen, um ihrer Arbeitsverpflichtung nachzukommen oder Kunden etwa bei Bestehen eines Kontrahierungszwangs einen Anspruch auf die angebotene Leistung haben. In diesen Fällen könnte geprüft werden, ob die verpflichtende Nutzung der luca-App und die damit einhergehende Datenverarbeitung möglicherweise auch unter dem Gesichtspunkt der Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c) DSGVO in Verbindung mit der jeweils einschlägigen Coronaschutzverordnung) gerechtfertigt sein kann.

Datensicherheit

Der Anbieter der luca-App wirbt mit besonders datenschutzfreundlichen Einstellungen der App, zum Beispiel mit Verschlüsselungstechniken, der Verifizierung von Telefonnummern und der Datenlöschung nach spätestens 30 Tagen. Die Daten seien auf ISO-27001-zertifizierten, deutschen Servern gespeichert. Positiv zu bewerten ist, dass die App grundsätzlich nicht permanent Aufenthaltsorte erfasst, sondern diese durch Scannen eines QR-Codes durch den Nutzer selbst an die App übermittelt werden.

Die Daten werden nach Angaben des Anbieters dezentral verschlüsselt und seien nur im Falle einer Infektion bei entsprechender Freigabe für das Gesundheitsamt lesbar. Der Anbieter informiert auf seiner Homepage darüber, dass nur in dem Fall, in dem die Entschlüsselung durch den Nutzer der App – bezüglich seiner Aufenthaltsorte – oder das Unternehmen – bezüglich der in dem relevanten Zeitraum bei ihm eingecheckten Kontakte – freigegeben werde, das Gesundheitsamt die Daten entsprechend entschlüsseln könne. Das Unternehmen könne die Daten zu keinem Zeitpunkt selbst entschlüsseln.

Die Angaben auf der Homepage des Anbieters sind insoweit allerdings nicht ganz eindeutig; an einer Stelle wird betont, dass nur das Gesundheitsamt die Daten entschlüsseln könne, in der Datenschutzerklärung wird jedoch beschrieben, dass der Gastgeber die Check-in-Datensätze entschlüssele und dem Gesundheitsamt zur Verfügung stelle.

In der Vergangenheit gab es außerdem Kritik an der Datensicherheit der App, beispielsweise in einer vorläufigen Analyse der Datensicherheit von luca, die von Forschern der Eidgenössischen Technischen Hochschule Lausanne und der Radboud-Universität Nijmegen am 23.03.2021 veröffentlicht wurde. Darin wird unter anderem der zentralisierte Ansatz kritisiert, der ein Missbrauchspotential durch den Betreiber des luca-Backend-Servers mit sich bringe. Kritisiert wurde in den Medien auch, dass der Quellcode der App noch nicht veröffentlicht wurde. Mittlerweile wurde aber mit der Veröffentlichung des Quellcodes begonnen; die Veröffentlichung des vollständigen Quellcodes für alle Komponenten ist aber bisher noch nicht erfolgt.

Noch vor dem Beginn der Veröffentlichung des Quellcodes hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg die luca-App aus datenschutzrechtlicher Sicht positiv bewertet und ihren Einsatz befürwortet (Pressemitteilung vom 17.02.2021). Die Aufsichtsbehörde hebt dabei besonders hervor, dass die Hoheit über die Daten durchgehend bei jedem Nutzer selbst bleibe. Die Behörde hat nach eigenen Angaben die App sowohl technisch als auch rechtlich geprüft und ist dabei zu dem Ergebnis gekommen, dass diese die hohen Datenschutz-Standards erfülle. Es gibt somit eine „offizielle" Bestätigung einer Datenschutzaufsichtsbehörde, dass die luca-App datenschutzkonform nutzbar sei.

Datenminimierung

Der Grundsatz der Datenminimierung aus der DSGVO besagt, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen (Art. 5 Abs. 1 lit. c) DSGVO). Dieser Grundsatz sollte auch bei der Angabe von Daten in der App beachtet werden. Unternehmen sollten also nur diejenigen Daten mit der App erfassen, die für die Erreichung ihres Zwecks, die Kontaktverfolgung zur Verhinderung der Ausbreitung des Corona-Virus zu ermöglichen, notwendig sind. In der Regel wird es ausreichend sein, wenn entsprechende QR-Codes im Unternehmen zur Verfügung gestellt werden und diejenigen, die die App nutzen, durch Scannen des QR-Codes angeben, dass sie sich an dem Ort aufgehalten haben.

Darüber hinausgehende Informationen wie Schichtpläne und andere detailliertere Informationen, die personenbezogene Daten enthalten, sollten nur dann über die App verarbeitet werden, wenn sie zur Kontaktverfolgung zwingend notwendig ist. Auch für diese Datenverarbeitung ist das Bestehen einer Rechtsgrundlage erforderlich; etwaige erforderliche Einwilligungen sind dafür gegebenenfalls gesondert einzuholen.

Auftragsverarbeitung

Soweit der App-Anbieter im Falle des Einsatzes der luca-App in einem Unternehmen personenbezogene Daten weisungsgebunden im Auftrag des Unternehmens verarbeitet, liegt eine Auftragsverarbeitung zwischen dem Unternehmen und dem App-Anbieter vor. Entsprechend ist der Abschluss einer Vereinbarung zur Auftragsverarbeitung erforderlich und ist auch vom Anbieter so vorgesehen.

Fazit und Ausblick

Die luca-App kann nach dem jetzigen Erkenntnisstand in Unternehmen datenschutzkonform zum Einsatz kommen, soweit die datenschutzrechtlichen Vorgaben eingehalten und Schutzmaßnahmen getroffen werden.

Die Nutzung der App in einem Unternehmen ist jedenfalls mit entsprechenden Einwilligungen der Betroffenen möglich. Die betroffenen Personen sollten dann transparent über die im Rahmen der Nutzung der App stattfindenden Datenverarbeitungen informiert werden. Für diejenigen, die die App nicht nutzen möchten, sollten alternative Möglichkeiten der Kontaktdatenerfassung bereitgehalten werden. Bei der Datenverarbeitung ist der Grundsatz der Datenminimierung zu beachten. Es sollte außerdem eine Vereinbarung zur Auftragsverarbeitung mit dem App-Anbieter geschlossen werden.

Für die Zukunft hat das Bundesgesundheitsministerium angekündigt, dass die luca-App mit der Corona-Warn-App abgestimmt werden solle. Beide Apps sollen dann die gleichen QR-Codes scannen können. Die Erweiterung der Corona-Warn-App um diese Funktion ist für April 2021 geplant. Es bleibt insoweit abzuwarten, ob mit einem weiteren Ausbau der „offiziellen" App die luca-App an Bedeutung verlieren wird.

Johanna Schmale / Dr. Sebastian Meyer

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 890
F +49 521 96535 - 113
M johanna.schmale@brandi.net

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Dr. Sebastian Meyer, LL.M.
Rechtsanwalt und Notar mit Amtssitz in Bielefeld
Fachanwalt für Informationstechnologierecht (IT-Recht)
Datenschutzauditor (TÜV)

T +49 521 96535 - 812
F +49 521 96535 - 113
M sebastian.meyer@brandi.net