Corona-App als Eintrittskarte?

Einleitung

Die Corona Warn-App, die vom Robert Koch Institut herausgegeben und von der Deutschen Telekom gemeinsam mit SAP entwickelt wurde, ist mittlerweile mehr als 15 Millionen Mal heruntergeladen und installiert worden. Eine der zentralen Funktionen der App ist die Risiko-Ermittlung, die darauf basiert, dass bewertet wird, in welchem Umfang Kontakt mit Personen bestanden hat, die später positiv auf Covid-19 getestet wurden. Eine sichere Bewertung bietet die Corona Warn-App jedoch nicht, da bei der Risikobewertung unter anderem nur solche Kontaktpersonen berücksichtigt werden, die ebenfalls die App nutzen und dort ihren positiven Befund angeben. Je höher die Verbreitung und Nutzung der App ist, desto aussagekräftiger ist aber natürlich die Risikobewertung der App.

Technische Gestaltung und rechtliche Wertung

Bereits bei der Konzeption der App wurden datenschutzrechtliche Aspekte berücksichtigt, wie dies durch den Grundsatz der datenschutzfreundlichen Technikgestaltung (privacy by design) gem. Art. 25 Abs. 1 DSGVO verlangt wird. Die Daten zu dem jeweiligen Nutzer der App werden ausschließlich lokal auf dem jeweiligen Gerät gespeichert, eine zentrale Datenspeicherung ist nicht vorgesehen. Es gibt auch keine eindeutige ID, die immer einem bestimmten Nutzer zugewiesen ist, sondern die verwendeten Kennungen wechseln in kurzen Intervallen. Wird über die App ein positives Testergebnis erfasst, müssen die relevanten Kennungen für den maßgeblichen Zeitraum von dem lokalen Gerät hochgeladen werden, so dass die entsprechende Übersicht mit den erfassten Werten von anderen Geräten abgeglichen werden kann, was gegebenenfalls zur Ausgabe einer Warnmeldung führt.

Empfehlung zur Nutzung der App

Sowohl aus Gründen der Risikominimierung im Unternehmen als auch im gesamtgesellschaftlichen Interesse ist es natürlich empfehlenswert, die eigenen Mitarbeiter zu ermutigen, die Corona Warn-App herunterzuladen und zu installieren. Soweit die Mitarbeiter mit dienstlichen Mobiltelefonen ausgestattet sind, kann der Arbeitgeber seinen Beitrag leisten, indem er ausdrücklich die Installation und Nutzung zulässt. Rechtlich zulässig ist es ebenfalls noch, die App standardmäßig zu installieren, wobei allerdings die Aktivierung durch den Nutzer erfolgen muss und nicht erzwungen werden darf. Unzulässig wäre eine dienstliche Verpflichtung zur Verwendung der App, selbst wenn es sich um ein Dienstgerät handelt. Die Funktionsweise der App basiert darauf, dass die App erfasst, welche anderen Geräte mit installierter App sich über einen längeren Zeitraum in der Nähe aufhalten. Die App unterscheidet dabei nicht zwischen Arbeitszeit und Freizeit, so dass die Verpflichtung zur Nutzung der App automatisch auch zu einer Erfassung von Kontakten außerhalb der Arbeitszeit führen würde, selbst wenn die Erfassung ohne unmittelbaren Personenbezug erfolgt. Im Hinblick auf die Nutzung von privaten Smartphones hat der Arbeitgeber natürlich erst recht keine Einflussmöglichkeit auf seine Mitarbeiter, die über eine reine Empfehlung hinausgehen.

Zutrittsbeschränkungen für eigene Mitarbeiter

Der Arbeitgeber hat unabhängig von seiner gesamtgesellschaftlichen Verantwortung eine Fürsorgepflicht gegenüber seinen Mitarbeitern. Bestandteil dieser Fürsorgepflicht ist es auch, angemessene Schutzmaßnahmen zur Vermeidung einer weiteren Ausbreitung von Covid-19 im Unternehmen und bei den eigenen Mitarbeitern zu treffen. Die Fürsorgepflicht kann es dabei gebieten, Mitarbeiter, bei denen die Gefahr einer Erkrankung mit Covid-19 besteht, nicht in Kontakt mit weiteren Mitarbeitern kommen zu lassen. Vor diesem Hintergrund ist es nicht abwegig, zumindest Überlegungen anzustellen, ob der Zugang zum Arbeitsplatz davon abhängig gemacht werden kann, dass der Arbeitnehmer durch Präsentation der Risikobewertung in der App nachweist, dass er voraussichtlich nicht erkrankt ist. Wie alle anderen Maßnahmen – etwa das Fiebermessen bei Betreten des Werksgeländes – ist jedoch nicht von einer besonderen Zuverlässigkeit auszugehen. Es muss also damit gerechnet werden, dass Mitarbeiter nicht an ihren Arbeitsplatz gelassen werden, obwohl von ihnen objektiv kein Risiko ausgehen würde und umgekehrt nicht jeder Fall bei einem bloßen Abstellen auf die Risikobewertung der App sicher erkannt werden kann. Diese fehlende Verlässlichkeit ist im Rahmen der datenschutzrechtlich erforderlichen Gesamtabwägung zu berücksichtigen. Auf deren anderen Seite dürften sich die Nachteile für die betroffenen Personen in Grenzen halten. Das Risiko der Stigmatisierung besteht nicht, da bei verständiger Bewertung der Maßnahmen die Zutrittsverweigerung als rein vorsorgliche Schutzmaßnahme angesehen werden muss. Weitere Nachteile für den betroffenen Mitarbeiter sind auch nicht ersichtlich, da sein Vergütungsanspruch bestehen bleibt und er gegebenenfalls auch im Home Office weiterarbeiten kann.

In datenschutzrechtlicher Hinsicht wird teilweise vertreten, dass die Auswertung schon deshalb unkritisch sei, weil die bloße Einsicht in die Anzeige der App überhaupt kein Fall der Verarbeitung personenbezogener Daten sei, wenn das Ergebnis nicht erfasst würde. Hiergegen spricht aber die Tatsache, dass als Erhebung von Daten bereits jeder Vorgang der Informationsbeschaffung zählt, und zwar unabhängig von der Absicht einer Speicherung. Der Anwendungsbereich des Datenschutzrechts ist damit eröffnet, so dass insbesondere eine Rechtsgrundlage für die Datenverarbeitung erforderlich ist. Da explizit Gesundheitsdaten als besonders geschützte Informationen abgefragt werden, muss dabei auf die relativ strengen Vorgaben von Art. 9 Abs. 2 DSGVO abgestellt werden. Hieraus lässt sich aber wohl nicht zwangsläufig ableiten, dass deswegen der Zutritt zum Werksgelände nicht von einer unbedenklichen Risikobewertung abhängig gemacht werden dürfte. Anders wäre nur die Pflicht zur aktiven Nutzung der App selbst zu bewerten. Dringend anzuraten ist es daher, immer auch alternative Möglichkeiten zur Risikobewertung vorzuhalten, etwa durch eine alternative Selbstauskunft. Auf diese Weise würden nicht schon vorab Personen ausgeschlossen, die entweder gar nicht über ein Smartphone verfügen oder auf deren Geräten die Installation der App nicht möglich ist

Vorgaben für sonstige geschäftliche Kontakte

Im Hinblick auf die Zutrittsregelungen für Geschäftskontakte, also insbesondere Kunden, Lieferanten oder Partner besteht ein größerer Ermessensspielraum des Unternehmens. Rechtsgrundlage für Zutrittsbeschränkungen ist insoweit die Ausübung des Hausrechts durch das Unternehmen, zusätzlich ist aber weiterhin eine datenschutzrechtliche Interessenabwägung erforderlich. Soweit tatsächlich beabsichtigt ist, ausschließlich Personen mit unkritischer Risikobewertung in der App auf das Werksgelände zu lassen, ist darauf zu achten, vorab die Geschäftskontakte über entsprechende Vorgaben zu informieren, da nicht mit derartigen Restriktionen gerechnet werden muss. Es sollte vermieden werden, dass Besucher unverrichteter Dinge wieder abreisen müssen. Eine in den meisten Unternehmen obligatorisch geforderte Schutzmaske mag kurzfristig noch beschafft werden können, die Installation der App ist dagegen nicht immer so einfach vor Ort möglich – zumal die App erst nach längerer Nutzung sinnvolle Ergebnisse liefern kann. Vorsicht ist schließlich in Fällen geboten, bei denen Geschäftspartner zur Leistungserbringung auf einen Zutritt zum Werksgelände angewiesen sind. Wird der Zutritt verweigert, ohne dass der Nachweis eines geringen Risikos durch Nutzung der App zuvor vertraglich vereinbart wurde, riskiert das Unternehmen durch die Zutrittsverweigerung in Annahmeverzug zu geraten und gleichwohl die Vergütung auch ohne Leistungserbringung zahlen zu müssen.

Fazit

Je höher die Verbreitung und Nutzung der App ist, desto aussagekräftiger ist die Risikobewertung der App und desto mehr kann sie einer weiteren Ausbreitung von Covid-19 entgegenwirken. Zur Risikominimierung im Unternehmen ist es deshalb empfehlenswert, die eigenen Mitarbeiter zur Installation der Corona Warn-App zu ermutigen. Eine dienstliche Verpflichtung zur Verwendung der App wäre allerdings datenschutzrechtlich unzulässig.
Sofern darüber nachgedacht wird, den Zugang zum Arbeitsplatz von der Präsentation einer unkritischen Risikobewertung der App abhängig zu machen, ist eine datenschutzrechtliche Gesamtabwägung erforderlich, die auch die fehlende Verlässlichkeit der App berücksichtigt. Es ist ratsam, immer auch alternative Möglichkeiten zur Risikobewertung vorzuhalten, etwa durch eine Selbstauskunft der Mitarbeiter.
Eine datenschutzrechtliche Interessenabwägung ist auch im Hinblick auf Zutrittsregelungen für Geschäftskontakte erforderlich. Zutrittsbeschränkungen, die auf der Risikobewertung der App basieren, sollten den Geschäftskontakten vorab kommuniziert werden..

Dr. Sebastian Meyer, LL.M.

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Dr. Sebastian Meyer, LL.M.
Rechtsanwalt
Datenschutzauditor (TÜV)

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