Corona-Warn-App auf den Diensthandy?

Viele Firmen statten Ihre Mitarbeiter mit dienstlichen Handies aus und erlauben in gewissem Umfang auch deren private Nutzung. Oft sind dieses Handies dann auch die Einzigen, die diese Mitarbeiter besitzen oder dauerhaft bei sich tragen. Es ist daher naheliegend, dass manche Mitarbeiter die Corona-Warn-App auf dem dienstlichen Gerät installieren wollen. Bei der Installation sind dabei aber einige datenschutzrechtliche Aspekte zu beachten.

Zusammenfassung:

Seit Dienstag ist die Corona-Warn-App verfügbar und viele wollen diese natürlich auch auf ihrem dienstlichen Handy installieren. Dazu haben uns erste Anfragen erreicht, wie dies datenschutzrechtlich zu bewerten sei. Eine offizielle Stellungnahme dazu ist uns derzeit nicht bekannt, jedoch sehen wir grundsätzlich keine Bedenken, wenn gewisse Randbedingungen beachtet werden.

- Die App darf nur freiwillig durch den Mitarbeiter oder auf Wunsch des Mitarbeiters installiert werden.
- Die App sollte nur auf Geräten installiert werden, die einzelnen Mitarbeitern ausschließlich und persönlich zur Verfügung gestellt wurden. Nur der Mitarbeiter selbst darf in der Lage sein die App zu bedienen. Sie darf nicht auf gemeinschaftlich genutzten Geräten installiert werden
- Andere Mitarbeiter oder Vorgesetzte dürfen nicht Einsicht in die App nehmen oder Auskunft darüber fordern.
- Vor einer Rückgabe des Mobilgerätes soll die App entweder deinstalliert werden oder der Mitarbeiter setzt die App in den Einstellungen zurück

Analyse:

Die Daten, die zwischen den Handies von verschiedenen Personen ausgetauscht werden, um Kontakte zu ermitteln, die möglicherweise das Risiko einer Ansteckung beinhaltet, sind grundsätzlich anonymisiert. In Zusammenhang mit der Zuordnung zu dem persönlich genutzten Geräte und der Möglichkeit ein Ansteckungsrisiko zu ermitteln, sind sie jedoch als Gesundheitsdaten und damit als besondere personenbezogene Daten nach Art. 9 DSGVO zu bewerten. Damit ist die Verarbeitung nur dann zulässig, wenn einer der Gründe des Art. 9 Abs. 2 a) – j) DSGVO zutrifft. Im konkreten Fall kommt nach unser Ansicht in den meisten Fällen nur Buchstabe a) in Betracht. Dies ist die ausdrückliche und freiwillige Einwilligung der Betroffenen. Ob auch die Verarbeitung z.B. durch einen Betriebsarzt nach h) in Frage kommt, hängt von den konkreten Umständen ab. Es wäre z.B. denkbar, dass ein Betriebsarzt bei einer Untersuchung Einsicht in die App nimmt, um ggf. einen Corona-Test zu empfehlen.

Bei persönlich zugeordneten Geräten, in die nur die Benutzer der Handies Einsicht nehmen kann, gehen wir davon aus, dass die Nutzer selbst als Verantwortliche für die Verarbeitung zu betrachten ist, da sie alleine über die näheren Umstände der Datenverarbeitung entscheiden. Die Corona-Warn-App lässt sich auch jederzeit durch die Nutzer deaktivieren.

Bei dem Einsatz von Mobile-Device-Management (MDM) Systemen ist ggf. zu prüfen, ob diese nicht vielleicht in irgendeiner Weise ermöglichen Einsicht in den Status der App zu nehmen. Dies würde einer Installation und Nutzung entgegenstehen. Die mittels des MDMs mögliche Löschung des Gerätes aus der Ferne, z.B. bei Verlust, sollte aber nur auf Grundlage einer Einwilligung der Nutzer erfolgen, da auch Löschen der Daten gemäß DSGVO Art. 4 Nr. 2 ein Verarbeitung darstellt. Genauso sollte die Löschung der Daten, z.B. bei Rückgabe des Gerätes, vorzugsweise durch die Nutzer erfolgen. Die App bietet dazu in den Einstellungen die Funktion „Anwendung zurücksetzen“ an. Danach sollten, so unsere Annahme, auch alle Möglichkeiten etwa anderswo gespeicherte Daten dem Benutzer zuzuordnen weitestgehend unmöglich sein.

Die Verarbeitung der an die zentralen Server übermittelten Daten erfolgt gemäß der in der App verfügbaren Datenschutzinformationen durch das Robert Koch Institut (RKI). Die Rechtsgrundlage der Verarbeitung durch das RKI ist die freiwillige Einwilligung des Nutzers. Dies betrifft auch teilweise über die Server und teilweise auf dem Endgerät durchgeführten Funktionen der Kontaktermittlung, der Risikoermittlung sowie der möglichen Eingabe eines positiven Testergebnisses. Eine andere Rechtsgrundlage als die Einwilligung der Benutzer kommt nach unser Einschätzung nicht in Betracht. Damit verbietet sich jeglicher Druck des Arbeitgebers die App zu installieren. Genauso darf die Teilnahme an Veranstaltungen oder der Zutritt zu Räumlichkeiten oder Ähnliches nicht von der Installation der App abhängig gemacht werden.

Kontakt

Falls Sie noch Fragen zu dem Thema haben freue ich mich auf Ihre Kontaktaufnahme

Dr. Stefan Krempl
089 461 3505 12
krempl@sued-it.de
Auditor ISO 27001, ISO 22301, KRITIS, Datenschutzbeauftragter