Inhaltsverzeichnis

OBSECOM DATA COMPLIANCE

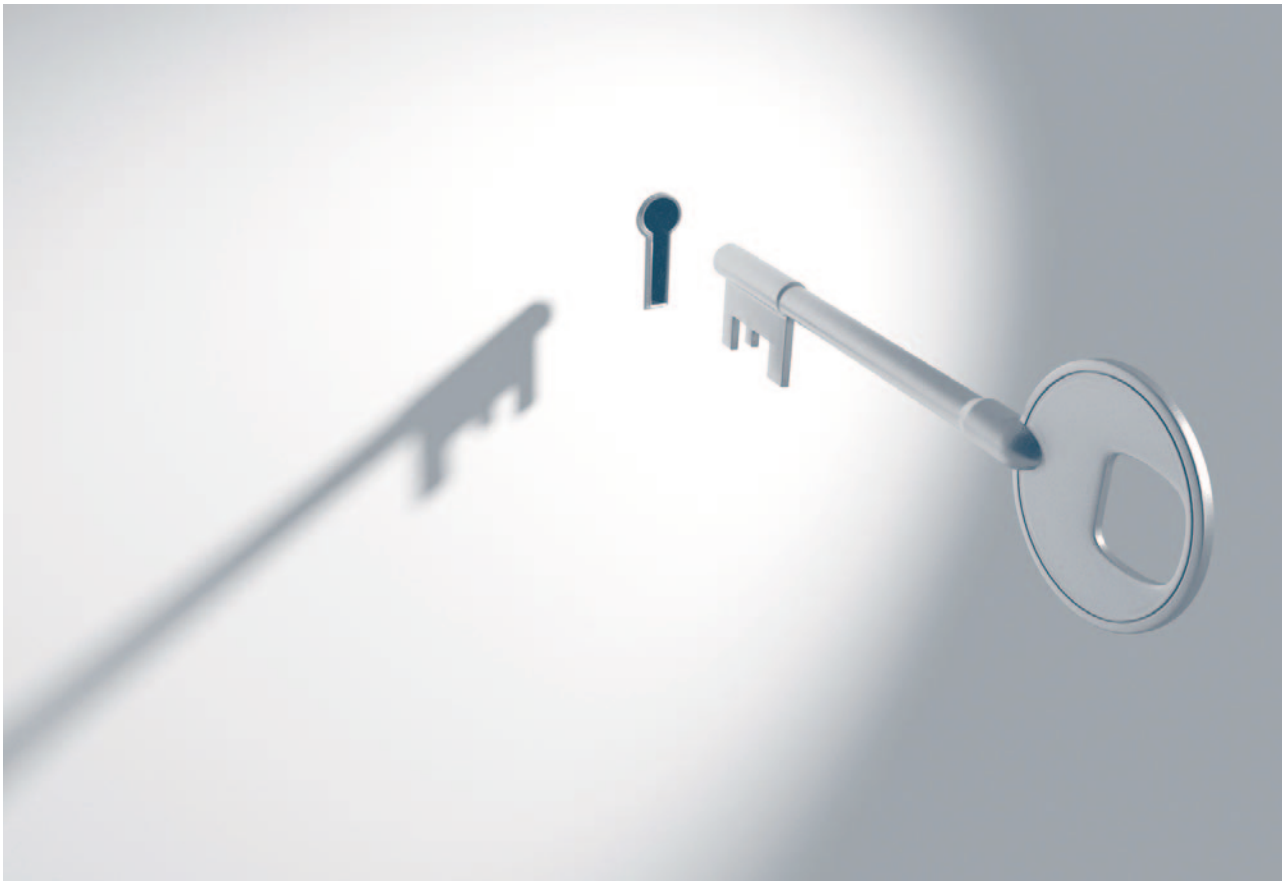

Foto by Pixabay

Der Einsatz von Corona Tracing Apps im privaten und betrieblichen Umfeld

Von Birte Frey und Judith Pfitzer

Die Installation von Tracing Apps auf den Smartphones von Bürgern soll die Gesundheitsämter bei der Nachverfolgung von Corona-Infektionsketten unterstützen. Solche Apps sollen Kontakte mit Infizierten dokumentieren, Betroffene informieren und somit zur Unterbrechung von Infektionsketten und der Pandemiebekämpfung beitragen. Dabei werden auch personenbezogene Daten der Betroffenen verarbeitet, für die die EU-Kommission bereits Leitlinien zur Gewährleistung von Datenschutzstandards vorlegte. Dieser Artikel gibt einen Überblick zum Stand der Entwicklung von Tracing-Apps und diskutiert auf welchen datenschutzrechtlichen Grundlagen solche Apps im privaten und betrieblichen Umfeld eingesetzt werden können.

Der aktuelle Stand in der Einwicklung von Tracing Apps

Tracing Apps ermitteln mittels der Signalstärke der Bluetooth Low Energy Funktechnik die Entfernung zwischen zwei Smartphones. Wird ein bestimmter Abstand für eine Mindestzeit unterschritten so tauschen beide Smartphones eindeutige IDs aus und der Kontakt wird im jeweiligen Smartphone dokumentiert. Stellt ein Benutzer in seiner Tracing App den eigenen Status auf „Corona-positiv“ um, so sendet die App über einen Server verschlüsselte Nachrichten an alle dokumentierten Kontakte. Die anderen Nutzer rufen regelmäßig die ID-Nummern der infizierten Nutzer ab und vergleichen diese mit den eigenen gespeicherten Kontakt-IDs. Erst wenn ein Nutzer positiv auf Covid-19 getestet wurde, werden die Daten zur Benachrichtigung anderer Nutzer auf einen zentralen Sever übertragen. Die Speicherung der Kontakt-IDs erfolgt dezentral auf den Smartphones und ist dabei auf 14 Tage beschränkt.

Apple und Google unterstützen die Entwicklung von Corona-Apps mit dezentraler Kontaktauswertung. Die Kontakt-IDs werden auf den Smartphones der Anwender gespeichert. Dabei spielt die Verschlüsselung auf den Smartphones eine große Rolle. „Der Schutz der Privatsphäre und die Sicherheit der Benutzer stehen dabei im Mittelpunkt dieser Entwicklung“, teilten die beiden Konzerne mit. Das Konzept sieht vor, dass Smartphones unabhängig vom konkreten verwendeten Betriebssystem nur temporär gültige Identifikationsnummern austauschen, sodass die Privatsphäre der Anwender gewahrt bleibt. Beide Firmen betonen, dass bei dem Projekt keine Benutzer identifiziert und keine Ortungsdaten verwendet würden. Google und Apple sollen dabei auch nicht erkennen können, wer krank oder wer gesund ist. In der weiteren Entwicklung arbeiten die Unternehmen daran eine Bluetooth-basierte Plattform zur Nachverfolgung von Kontakten zu ermöglichen. Diese Funktionalität soll dann direkt in das Betriebssystem, also iOS und Android, integriert werden.

In Deutschland entwickeln die Telekom und SAP im Auftrag der Bundesregierung eine Tracing-App auf Grundlage des Apple und Googles Systems. Die App soll eng mit den Gesundheitsämtern abgestimmt werden, um sicherzustellen, dass die gewarnten Nutzer telefonisch beraten werden. Ein Datum zur Veröffentlichung ist noch nicht angekündigt. Darüber hinaus sind weitere Apps auf dem Markt, die der Forschung helfen sollen, das Virus besser zu verstehen. So sendet die Corona-Datenspende App des Robert-Koch-Instituts (RKI) in Kombination mit verschiedenen

Fitnessarmbändern und Smartwatches pseudonymisiert Gesundheitsdaten der Nutzer an das RKI. Die Behörde wertet diese Daten aus um die die Ausbreitung des Coronavirus statistisch zu erfassen und die Dunkelziffer der Infizierten zu verringern. Die Corona-Datenspende ist pseudonym, da die Nutzung der App auf einer individuellen Nutzer-ID basiert, die dem Nutzer persönlich zugeordnet wird. Zwar erhält das RKI keine persönlichen Informationen, wie Namen oder Anschrift, dennoch ist die App nicht anonym.

Neben den Vorhaben für den öffentlichen Gesundheitsschutz werden auch in der Privatwirtschaft Tracing-Apps zur Kontaktverfolgung von Beschäftigten für den betrieblichen Schutz angeboten. Diese Apps sollen den Infektionsstatus der an den Arbeitsplatz zurückkehrenden Beschäftigten überwachen. Arbeitgeber wollen so das Risiko minimieren, dass durch infizierte Mitarbeiter einzelne Betriebsteile oder gar das gesamte Unternehmen wieder geschlossen werden muss. Der Anbieter PwC verspricht in der Entwicklung seiner App die Einhaltung hoher Datenschutz- und Sicherheitsstandards. Der Zugriff auf die gespeicherten Daten solle zwar zentral erfolgen, dieser sei jedoch auf wenige Personen mit Admin-Status begrenzt. Die App erkennt per GPS Geolokalisierung, dass sich ein Mitarbeiter am Firmenstandort befindet und startet sodann das Tracing über Bluetooth und WLAN. PwC setzt die App vorerst für den Eigenbedarf seiner Mitarbeiter ein. Eine Vermietung des Systems an andere Unternehmen sei jedoch geplant.

Datenschutzrechtliche Aspekte beim Einsatz von Tracing Apps

Tracing Apps verarbeiten verschiedene Arten personenbezogener Daten. Neben Kontaktdaten zur Registrierung der App und den eindeutigen Kontakt-IDs anderer Nutzer wird mit dem Infektionsstatus auch ein besonders sensibles Gesundheitsdatum nach Art. 9 EU Datenschutz-Grundverordnung (DS-GVO) verarbeitet. Selbst bei einer pseudonymisierten Datenverarbeitung ist unter Hinzunahme weiterer Daten eine Rekonstruktion des personenbezogenen Datums möglich, der Personenbezug der Daten bleibt grundsätzlich erhalten. Der Schutzbereich der DS-GVO ist somit eröffnet.

Der Datenschutz steht der Verarbeitung von Gesundheitsdaten im Rahmen einer Tracing App nicht entgegen, sondern hilft die Datenverarbeitung mit dem Recht auf informationelle Selbstbestimmung in Einklang zu bringen. Bei der Bereitstellung von Tracing Apps müssen die in Art. 5 DS-GVO festgelegten Grundsätze der Datenminimierung und Transparenz sowie die Informationspflichten befolgt werden. Es dürfen nur so viele Daten gespeichert werden wie es für die Erreichung des Zweckes, die Verhinderung weiterer Infektionsketten, erforderlich ist. Die Daten dürfen nur für diesen festgelegten Zweck verarbeitet und nur so lange gespeichert werden, wie dies erforderlich ist. Die Nutzer müssen vorab in verständlicher Weise über den Zweck der Verarbeitung, die Dauer der Speicherung und ihre Rechte als Betroffene informiert werden. Die Verarbeitung von Gesundheitsdaten steht grundsätzlich unter einem Verbot mit Erlaubnisvorbehalt. Solange die Nutzung der Tracing App nicht gesetzlich vorgeschrieben ist, kommt nach Art. 9 Abs. 2 lit. a DS-GVO nur die freiwillig erteilte Einwilligung des Betroffenen als Rechtsgrundlage in Betracht. Die Datenerfassung und Übertragung des Infektionsstatus an zentrale Server ist nur mit Zustimmung des Nutzers möglich. Voraussetzung für die Wirksamkeit der Einwilligung ist nach Art. 7 DS-GVO ihre Freiwilligkeit. Diese ist nur gegeben, wenn Betroffene aus der Nichterteilung ihrer Einwilligung keine Nachteile befürchten müssen.

Die Seiten 5 bis 12 sind in dieser Vorschau nicht enthalten.