datenschutz-berater.de

44. Jahrgang

DSB 07+08/2020

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

ISSN 0170-7256

dfv Mediengruppe

Simon Pentzien und Daniel Lösch

Corona-Warn-App und Personenbezug: Eine kritische Betrachtung

Lange erwartet, viel diskutiert: Die Corona-Warn-App soll ermöglichen, Infektionsketten schneller zu durchbrechen und erfährt im Allgemeinen erstaunlich viel Lob. Optimierungsbedarf gibt es trotzdem.

Einleitung

Beiträge über die Corona-Warn-App dominieren seit dem Launch weite Teile der Medienlandschaft. Die allgemeine Resonanz ist von den App-Nutzern bis hin zu Datenschutz- und IT-Experten sehr positiv. Bei einer genauen Betrachtung verwundert dies nicht: Die App bietet ein hohes Datenschutzniveau. Auch scheint der Grundsatz Privacy by Design beinahe schulmäßig umgesetzt. Der nachfolgende Beitrag erhebt nicht den Anspruch, eine allgemeine datenschutzrechtliche Bewertung der Corona-Warn-App durchzuführen. Ziel ist vielmehr, auf Konstellationen hinzuweisen, in denen scheinbar „unbemerkt" ein Personenbezug bzw. eine Personenbeziehbarkeit vorliegt. Flankierend dazu behandeln die Verfasser die datenschutzrechtliche Abgrenzung der Begriffe der Anonymisierung und Pseudonymisierung.

Architektur der Corona-Warn-App (stark vereinfachte Darstellung)

Zentral für die Funktionalität der Corona-Warn-App ist das sog. Expositionsbenachrichtigungswerkzeug (englisch: Exposition Notification Framework, kurz: ENF). Google und Apple haben das ENF entwickelt. Es ist Bestandteil der Betriebssysteme Android (ab Version 6) und iOS (ab Version 13.5) und ermöglicht Smartphones per Bluetooth Low Energy (BLE) eine energiesparende Kontaktnachverfolgung. Dadurch sind Smartphones in der Lage, wechselnde zufallsgenerierte Kennnummern zur Kontaktnachverfolgung per BLE im Hintergrund auszutauschen. Im ENF, das sich in technologischer Hinsicht außerhalb der Corona-Warn-App befindet, wird täglich ein sogenannter Tagesschlüssel (Temporary Exposure Key, kurz: TEK) als Zufallscode generiert. Alle 10 bis 20 Minuten leitet sich aus diesem Tagesschlüssel ein jeweils neuer Entfernungsschlüssel (Rolling Proximity Identifier, kurz: RPI) ab. Das Smartphone versendet den jeweils zuletzt abgeleiteten RPI per BLE alle fünf Minuten für zwei Sekunden. Zeitgleich empfängt das Smartphone die von anderen Smartphones gesendeten RPIs. Das ENF speichert diese RPIs (inklusive Metadaten wie Datum oder Dauer des Kontakts) zwei Wochen lang.

Wird ein App-Nutzer positiv auf das Coronavirus getestet, erhält er vom Arzt oder Labor einen QR-Code (vorausgesetzt die erforderliche digitale Infrastruktur ist verfügbar). Diesen QR-Code kann der App-Nutzer über die Corona-Warn-App einscannen, um schließlich sein Testergebnis abzufragen. Sofern eine Durchführung dieses Verfahrens nicht mittels QR-Codes möglich ist (etwa wegen fehlender digitaler Infrastruktur bei der Teststelle), kann der App-Nutzer mit einer Verifikations-Hotline Kontakt aufnehmen. Bei der Hotline erhält er nach Beantwortung einiger Plausibilisierungsfragen sowie Angabe seiner Telefonnummer mündlich eine teleTAN. Hierfür notiert der Hotline-Mitarbeiter die Rufnummer auf einem Zettel. Spätestens nach einer Stunde erfolgt die Vernichtung dieses Zettels samt darauf notierter Rufnummer.

Im Anschluss ist der App-Nutzer in der Lage, sein Testergebnis zu teilen. Hierzu kann er seinen eigenen Tagesschlüssel für einen Abgleich freigeben. Diesen Tagesschlüssel bezeichnet man fortan als Positivschlüssel. Hat ein App-Nutzer sein positives Testergebnis geteilt, erfolgt ein gebündelter Upload all seiner Tagesschlüssel der letzten 14 Tage.

Mehrmals täglich lädt die Corona-Warn-App die Positivschlüssel herunter und gibt diese Positivschlüssel anschließend an das ENF weiter. Dort erfolgt ein Abgleich der Positivschlüssel mit den im Kontaktprotokoll gespeicherten und aus den Positivschlüsseln abgeleiteten RPIs. Sofern eine Übereinstimmung vorliegt und damit ein Kontakt mit einem Infizierten bestätigt ist, erfolgt eine Berechnung des Ansteckungsrisikos anhand bestimmter Parameter. Anschließend wird der jeweilige App-Nutzer über die mögliche Risikobewertung informiert.

Rechtliche Grundlagen: Unterscheidung pseudonymer und anonymer Daten

Im Zuge der öffentlichen Diskussion hinsichtlich der Chancen und Risiken einer Corona-App ist ein Aspekt besonders häufig aufgefallen: Die Vernachlässigung der Differenzierung von pseudonymen und anonymen Daten. Für die datenschutzrechtliche Einordnung konkreter Verarbeitungstätigkeiten im Rahmen der Corona-Warn-App ist eine eindeutige Unterscheidung jedoch essentiell.

Pseudonyme Daten

Bei der Pseudonymisierung i. S. v. Art. 4 Nr. 5 DSGVO werden personenbezogene Daten derart verarbeitet, dass ohne Hinzuziehung zusätzlicher Informationen kein Perso-

nenbezug hergestellt werden kann. Charakteristisch ist dabei das Bestehen einer Zuordnungsregel, die den pseudonymisierten Daten ein Identifikationsmerkmal einer Person zuweist. Im Ergebnis gilt die Pseudonymisierung als Erhöhung der Datensicherheit. Der Personenbezug wird jedoch nicht aufgehoben, so dass das Datenschutzrecht vollumfänglich anwendbar bleibt.

Anonyme Daten

Anonymen Daten hingegen fehlt es an einer Zuordnungsregel. Auch unter Hinzuziehung zusätzlicher Informationen ist es bei diesen grundsätzlich ausgeschlossen, einen Personenbezug herzustellen.

Im Einzelnen: Die DSGVO enthält keine Legaldefinition, allerdings in Erwägungsgrund 26 folgende rechtliche Konturierung des Begriffs der „Anonymisierung": „Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke."

Erwägungsgrund 26 stellt damit klar, dass die Anforderungen an eine Anonymisierung höher sind als an eine Pseudonymisierung. Während es für eine Pseudonymisierung genügt, dass zur Identifikation der dahinterstehenden Person zusätzliche, aber getrennt aufbewahrte, Informationen herangezogen werden müssten, ermöglichen anonymisierte Daten grundsätzlich keinen Personenbezug mehr. Das Datenschutzrecht ist daher – und dies ist der wesentliche Unterschied – sowohl für die absolute als auch für die faktische Anonymisierung gar nicht anwendbar.

Die Unterscheidung von absoluter und faktischer Anonymisierung erfolgt folgendermaßen: Nur wenn unabhängig von möglichem Zusatzwissen Dritter eine De-Anonymisierung gänzlich ausgeschlossen ist, liegt eine absolute Anonymisierung vor. Nach dem aktuellen Stand der Technik ermöglichen dies nur wenige Methoden.

Aus Erwägungsgrund 26 ergibt sich, dass aber auch die faktische Anonymisierung als vollwertige Anonymisierung im datenschutzrechtlichen Sinne zu qualifizieren ist: „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren […]. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind."

Im Gegensatz zur absoluten Anonymisierung verlangt der Gesetzgeber bei der faktischen Anonymisierung also nicht gänzlich den Verlust des Personenbezugs. Es genügt, dass ein (böswilliger) Dritter zum Zweck der De-Anonymisierung einen unverhältnismäßig hohen Aufwand betreiben müsste und daher voraussichtlich seine Bestrebungen nicht weiterverfolgen würde. Entsprechend verlangt die Artikel-29-Datenschutzgruppe in WP 216, dass es nach einer Anonymisierung keiner Partei möglich sein darf, eine Person aus einem Datenbestand herauszugreifen, eine Verbindung zwischen zwei Datensätzen eines Datenbestands herzustellen, oder durch Inferenz personenbezogene Informationen aus einem solchen Datenbestand abzuleiten.

„Optimierungsbedarf" bei der Corona-Warn-App

Die Datenschutzfolgenabschätzung (DSFA, Version 1.0.1 v. 18. Juni 2020) des Robert Koch Instituts (RKI) zur Corona-Warn-App weist ausdrücklich auf zahlreiche Konstellationen hin, in denen bei bestimmten Verarbeitungsvorgängen ein Personenbezug vorliegt oder zumindest die Möglichkeit besteht, einen solchen herzustellen.

Gemäß der DSFA (S. 81 f.) gelte dies etwa für die Verarbeitung der Positivschlüssel durch das RKI. Aus der Perspektive des RKI handele es sich demnach bei den Positivschlüsseln um personenbezogene Daten, da diese bei der Übermittlung kurzzeitig mit der IP-Adresse der App-Nutzer verbunden würden. Wegen der Löschung der IP-Adressen aus den Server-Logfiles unmittelbar nach Beantwortung einer Anfrage bestehe der Personenbezug jedoch nur für eine „technische Sekunde". Hinzu komme der Umstand, dass das RKI selbst gar nicht über die IP-Adresse verfüge. Es bestehe also lediglich die (hypothetische) rechtliche Möglichkeit, diese von den entsprechenden Stellen heraus zu verlangen.

Unter Zugrundlegung der soeben erläuterten essentiellen Unterscheidung von anonymen und pseudonymen Daten sind weitere Konstellationen zu erkennen, in denen ein Personenbezug besteht oder hergestellt werden kann. Der Fokus der Betrachtung soll dabei auf Google und Apple sowie den App-Nutzern selbst liegen. Bewusst ausgeklammert ist der Prozess der Telefon-Hotline.

Nur sehr geringfügiger Personenkontakt

Nicht nur für das RKI besteht die jedenfalls theoretische Möglichkeit, Personenbezug hinsichtlich eines Infektionsgeschehens herzustellen. Vielmehr sind in gewissen Konstellationen sogar die App-Nutzer selbst in der Lage, andere

Nutzer eindeutig zu identifizieren, die eine Infektionsmeldung abgegeben haben.

Konkret dürfte dies der Fall sein, wenn ein Nutzer, der über den Kontakt mit einer infizierten Person informiert wurde, im relevanten Zeitraum nur sehr wenige direkte soziale Kontakte hatte und daher per Ausschlussprinzip die infizierte Person ermitteln kann.

Aus diesem Grund sollte das RKI die Behauptung, das System sei „so konzipiert, dass eine Identifizierung einzelner Nutzer durch die an der Datenverarbeitung beteiligten Stellen und andere Nutzer ausgeschlossen werden" (DSFA, S. 57) könne, korrigieren.

Herstellung eines Personenbezugs durch Apple und Google

Überdies ist nicht auszuschließen, dass Apple und Google in der Lage sind, einen Personenbezug herzustellen. Ausgangspunkt für die mögliche Herstellbarkeit eines Personenbezugs ist der Umstand, dass Apple und Google wissen, welche Nutzer sich die Corona-Warn-App aus dem App Store oder dem Google Play Store heruntergeladen haben. Dies ergibt sich etwa aus der Datenschutzerklärung von Google:

„Wir erheben Daten über die Apps, Browser und Geräte, die Sie beim Zugriff auf Google-Dienste verwenden. […] Zu den von uns erhobenen Daten zählen […] Wir erheben diese Daten, wenn ein Google-Dienst auf Ihrem Gerät unsere Server kontaktiert, beispielsweise wenn Sie eine App vom Play Store installieren […]."

Es ist naheliegend, dass auch Google oder Apple mithilfe der Positivschlüssel einen Personenbezug herstellen können – allerdings eben anders als das RKI nicht nur für eine technische Sekunde. Denkbar ist etwa, dass der Upload der gebündelten Positivschlüssel für Google oder Apple ein spezifisches Muster (z. B. aufgrund des Datenvolumens) aufweist und daher der logische Schluss, dass ein Positivschlüssel hochgeladen wurde, zwingend ist. Dadurch wäre es den beiden Unternehmen möglich, den Upload eines Positivschlüssels und damit ein positives Corona-Testergebnis mit dem konkreten App-Nutzer zu verknüpfen. Unter diesen Voraussetzungen läge keine der Voraussetzungen einer wirksamen faktischen Anonymisierung vor. Schließlich wäre es möglich, eine Person aus dem Datenbestand herauszugreifen, eine Person betreffende Datensätze miteinander zu verknüpfen und durch Inferenz Informationen aus einem solchen Datenbestand über eine Person abzuleiten.

Die lokale Datenverarbeitung auf dem Smartphone bietet Apple und Google eine weitere Gelegenheit, einen Personenbezug herzustellen. In der DSFA kommt das RKI zu dem Ergebnis, dass die nur lokal in der App und dem ENF verarbeiteten Nutzerdaten für das RKI faktisch anonym sind. Das RKI argumentiert, dass die App keine Tracing- oder Nutzungsanalyse-Funktionalitäten aufweist. Dadurch ist das RKI laut eigener Aussage nicht in der Lage, die in der Corona-Warn-App verarbeiteten Kennungen und Risikoinformationen mit einem spezifischen Nutzerprofil zu verknüpfen. (S. 81 f. der DSFA).

In Bezug auf Apple und Google hingegen sollte man dies differenziert betrachten. Hierbei ist vor allem das ENF von besonderer Bedeutung. Der genaue Ablauf der Datenverarbeitung „hinter" dem ENF liegt außerhalb des Einflussbereichs des RKI. So heißt es auch in der DSFA auf S. 112: „Es ist anzunehmen, dass Apple und Google durch eine Änderung des ENF auch zur Verknüpfung der dort verarbeiteten Tagesschlüssel und RPIs mit einer geräte- (z. B. Werbe-ID) oder nutzerspezifischen Kennung (z. B. Apple-ID oder Google-Konto) in der Lage sind." Diesbezüglich bleibt den Nutzern also vorerst nur die Möglichkeit, Apple und Google in datenschutzrechtlicher Hinsicht zu vertrauen.

Fazit

Trotz des vorhandenen Optimierungsbedarfs bleiben wir bei unseren einleitenden Worten: Die Corona-Warn-App ist in datenschutzrechtlicher Hinsicht gut umgesetzt und bietet ein sehr hohes Sicherheitsniveau. Die vorangegangenen Ausführungen zeigen allerdings auch, dass selbst bei einer professionellen Umsetzung eine durchgängige Anonymisierung i. S. d. DSGVO die Entscheidungsträger vor große Herausforderungen stellt. Dieser Umstand ist jedoch nicht zwangsläufig als Versäumnis im Rahmen der Entwicklung der Corona-Warn-App zu qualifizieren, sondern vielmehr eine Folge der weitreichenden Möglichkeiten heutiger Technologien. Keinesfalls besteht aktuell ein Grund zu der Annahme, dass in Deutschland ein Überwachungsstaat eingerichtet werden soll. Vielmehr setzt die Corona-Warn-App ein starkes Zeichen für den Datenschutz und den Technologie-Standort Deutschland.

Autoren: **Simon Pentzien (MBA) ist Rechtsanwalt und Chief Privacy Officer bei der Datenschutz hoch 4 GmbH. Er ist spezialisiert auf Datenschutzrecht und IT-Recht. Große Erfahrung hat er unter anderem bei der Verhandlung von komplexen Datenschutzverträgen und der datenschutzkonformen Implementierung von Prozessen.**

Daniel Lösch ist Volljurist und zertifizierte Fachkraft für Datenschutz (DEKRA) bei der Datenschutz hoch 4 GmbH. Er berät Unternehmen im Zusammenhang mit allen datenschutzrechtlichen Fragen bei Digitalisierungsprozessen und dem Einsatz neuer Technologien wie Virtual- und Augmented Reality, Data Analytics und Künstlicher Intelligenz.