erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Kirsten Bock, Christian Ricardo Kühne, Rainer Mühlhoff, Měto R. Ost, Jörg Pohle, Rainer Rehak

Die Grenze der App ist nicht die Grenze der Verarbeitung

Warum eine Datenschutz-Folgenabschätzung zur *Corona-App* durch das FIfF erstellt wurde

Eine AutorInnengruppe aus FIfF-Mitgliedern hatte sich Anfang April gefunden, um Konzepte zum Contact-Tracing per App („Corona-App") *aus Datenschutzsicht zu untersuchen.*

Eigentlich kritisch gegenüber jeder Art von automatisierter Tracing-App eingestellt, nahmen sich die AutorInnen vor, Schadensbegrenzung zu betreiben. Wenn diese Apps also nicht mehr zu verhindern sind, dann sollte zumindest derjenige Typ von App stark gemacht werden, mit dem die geringste Eingriffsintensität in die Grundrechte der AnwenderInnen einherginge. Linus Neumann, einer der SprecherInnen des Chaos Computer Clubs, hatte auf seinem Blog drei Typen von Technologien für Contact-Tracing-Apps und ihren wesentlichen Eigenschaften unterschieden: GPS-Daten, Bewegungsdaten und Kontaktdaten. Besonders im asiatischen Raum wurden mitunter alle diese Daten ausgewertet, was aus Verhältnismäßigkeitsüberlegungen hierzulande ausscheidet.

Der Zweck eines Contact-Tracings soll, so bestimmte es diese AutorInnengruppe dann im Laufe ihrer Arbeit, einzig darin bestehen, Infektionsketten zu erkennen und diese zu unterbrechen. Dieser Funktionsumfang konnte mit den Typ-3-Daten, also *Kontaktdaten* am ehesten umgesetzt werden. Insbesondere fasste Neumann ein dezentrales Verfahren zusammen, welches im *WirVsVirus*-Hackathon entwickelt worden war. Zudem hatte eine internationale EntwicklerInnengruppe unter der Projektbezeichnung DP-3T angefangen, ein dezentrale Typ-3-App technisch zu spezifizieren und diese Überlegungen über Github öffentlich zugänglich zu machen.

Ein Clou der dezentralen Typ-3-App besteht in der Abstandsmessung von Personen per Bluetooth zwischen deren Smartphones durch wechselnde temporäre Kennungen. Wenn Menschen einander zu nahe kommen und zu lange interagieren, besteht ein hohes Infektionsrisiko. Die zweite architektonisch nicht minder bedeutsame Eigenschaft dieses Konzepts besteht darin, dass riskante Begegnungen mit positiv getestet infizierten Personen in der Vergangenheit auf den Smartphones der App-NutzerInnen – nicht auf einem zentralen Server – ermittelt werden. Es obliegt dann den Personen selber, nach einer Warnung durch die App sich in Quarantäne oder Behandlung zu begeben. Der Abgleich von Bluetooth-Kennungen möglicherweise riskanter Kontaktereignisse soll über einen Server geschehen, auch wenn dieser im dezentralen Modell nur eine gemeinsame „Dateiablage" darstellt. Insofern hat die als „dezentral" bezeichnete Architektur mit einem solchen Server – real wären es wohl eine ganze Reihe an geografisch verteilten Servern –

auch ein zentrales Element, nur dass dieser Server außer dem Zwischenspeichern von Daten, die keinen Personenbezug mehr aufweisen, keine weitere Funktion innehat. Insbesondere kann er keine „sozialen Graphen" errechnen wie etwa bei den zentralen Konzepten. Allerdings müssen dafür einige Schutzmaßnahmen angewendet werden, insbesondere bei der Interaktion der Smartphones mit dem zentralen Server. Die AutorInnengruppe war davon überzeugt, dass das Konzept Typ-3 grundsätzlich datenschutzfreundlich funktionieren könnte.

Während der anhaltenden konzeptionellen Arbeiten der AutorInnengruppe am Untersuchungskonzept gab das Robert-Koch-Institut die Wearable-App heraus. Diese App war zwar als *Corona-App* bezeichnet worden, verfolgte aber einen anderen Zweck. Sie sollte der medizinischen Vermessung von Körpern dienen, aber nicht wirkungsvoll Infektionsketten unterbrechen. Das Üble an dieser App ist, dass Menschen hochauflösend ihre Körperfunktionen messen sollen und dann zu einer „Datenspende" ihrer Gesundheitsdaten aufgefordert werden, wobei das RKI die Daten dann nicht direkt vom Smartphone, sondern über die Anbieter der Fitness-Tracker bezieht. Die AutorInnengruppe war in Sorge, dass nun in schneller Folge weitere Apps mit beliebigen, hochzweifelhaften Zwecken auf windigen Rechtsgrundlagen folgen würden.

Die AutorInnengruppe entschied sich daher, das Typ-3-Konzept in Form einer Datenschutz-Folgenabschätzung (DSFA) zu untersuchen, wie sie die Datenschutz-Grundverordnung (DSGVO) in Artikel 35 der verantwortlichen BetreiberIn einer solcher Technik auferlegt. Bei einer DSFA handelt es sich um eine strukturierte Risikoanalyse, die mögliche grundrechtsrelevante Folgen einer Datenverarbeitung im Vorfeld identifiziert. Es werden darin Maßnahmen beschrieben, mit denen diese Risiken adressiert werden oder es wird dargestellt, dass und warum es Schutzmaßnahmen im konkreten Fall nicht gibt oder geben kann. Mit dieser Entscheidung für die Methodik wurden notwendig insbesondere auch die Rechtsgrundlagen für die Nutzung einer Corona-App in den Blick gestellt.

Mit der Entscheidung zur Durchführung einer DSFA zeigte sich umgehend die nächste Schwäche der App des Robert-Koch-Instituts: Wie kann es möglich sein, dass ein Totalmonitoring menschlicher Körperfunktionen zur Praxis wird, ohne dass die Risiken bei der Nutzung dieser App in einer DSFA, so wie es die DSGVO verlangt, offengelegt werden? Eine DSFA durchzuführen ist in jedem Falle obligatorisch, auch (gerade!) wenn Menschen sich freiwillig einer Totalüberwachung aussetzen. Zumal es hieß, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) an der Entwicklung der App beteiligt worden war. Auf Twitter beteuerte der BfDI, dass eine DSFA für diese App vorläge. Diese DSFA wurde bislang nicht veröffentlicht und es wurden keine Aussagen über Prüfmethode und Prüftiefe gemacht.

Die Entscheidung für eine Muster-DSFA nach DSGVO weitete insofern den Blick und generierte unabweisbar einen ganzen Strauß an hochrelevanten Fragestellungen:

- Was genau ist der **Untersuchungsgegenstand**? Aus Datenschutzsicht ist die gesamte Verarbeitungstätigkeit in den Blick zu nehmen, in der eine App und der Betrieb eines zentralen Servers zum Einsatz kommen würden. Die DSGVO verlangt, bei einer Verarbeitungstätigkeit dabei insgesamt mindestens 14 Subprozesse zu unterscheiden, vom Prozess des Erhebens von Daten bis zu deren Löschung (Artikel 4 Absatz 2 DSGVO). Alle Darstellungen zur Corona-App fokussierten bislang technisch auf der Idee mit der Bluetooth-Abstandsmessung, niemand thematisierte bis dahin den anderen, nicht minder schützenswerten Teil des Workflows auf der Serverseite, mit einem Zu-Ende-Denken der gesamten Prozessstruktur, inkl. des Automatisierens von Kommunikationswegen zwischen Ämtern, ÄrztInnen und Betroffenen.

- Welche Instanz ist **verantwortlich für den Betrieb der gesamten Verarbeitungstätigkeit**, inklusive des korrekten Funktionierens der App und der Kommunikationswege? Wer muss entsprechend als datenschutzrechtlich Verantwortliche für die Anfertigung auch der DSFA verantwortlich sein und die Verarbeitung so einrichten, dass sie den Zweck der Infektionskettenunterbrechung – und nichts anderes! – erfüllt und dafür jede Menge an Schutzmaßnahmen installiert werden, bis hin zur Spezifikation, Dokumentation und Offenlegung des Quellkodes, abgeleitet aus dem Transparenzanspruch in Artikel 5 DSGVO.

- Welche **Rechtsgrundlage** muss geschaffen werden und gelten, damit eine solche App tatsächlich rechtskonform eingesetzt werden kann? Wie sind die Betroffenenrechte bzgl. Auskunft oder Korrektur und Widerspruch umgesetzt? Wie muss das System betrieben werden, auch für solche Fälle, in denen fälschlich Daten hochgeladen wurden und diese zurückgerufen werden müssen?

- Wer gilt als **Hauptangreifer** auf die Betroffenen? Es sind nicht die anderen Betroffenen, mit denen in der Vergangenheit Kontakt bestand. Aus Datenschutzsicht ist der Hauptangreifer des Verfahrens immer derjenige, der das Verfahren betreibt, denn dieser ist maximal mächtig und in der Regel auch daran interessiert, um über den Zweck hinaus weitere Daten zu erheben oder diese Daten auch noch für andere Zwecke zu verarbeiten. Und wenn er nachlässig die Daten verarbeiten (lässt), dann können wiederum Unbefugte Zugriff auf diese Daten nehmen. Und weiterhin besteht grundsätzlich für jede App-Konzeption das Problem, wie Betroffene vor den Aktivitäten von Apple und Google zu schützen sind, die das Betriebssystem stellen, mit dem einerseits die Bluetooth-Signale und temporären Kennungen (tempIDs) erzeugt werden und die die Schnittstelle zur App bilden? Die App steuert die gesamte Technik inklusive des Uploads und Downloads von tempIDs. Apple und Google sind technisch in der Lage, aber nicht befugt, Zugriff auf die tempIDs zu nehmen. In der DSFA wird ein Angriff untersucht, der zeigt, wie in diesem Verfahren die Daten auch unbeteiligter Android-NutzerInnen gespeichert werden.

- Welche **Modellierung der Risiken** wird gewählt? Die Risikomodellierung aus Datenschutzsicht besteht darin, dass die Verarbeitung nicht (hinreichend) die Grundsätze des Artikel 5 DSGVO erfüllt. Eine Risikomodellierung nimmt diese Grundsätze auf und entwickelt an diesen entlang eine Heuristik. Und weil Datenschutz permanent sicherzustellen ist, muss seitens der Verantwortlichen ein Datenschutz-

Management betrieben werden, mit dem kontinuierlich Störungen und Fehlfunktionen entdeckt, geprüft und wirksam behoben werden.

- Welche **Angriffe** zum vorsätzlichen Unterlaufen des Systems oder zur (Zer-) Störung der Funktionalität sind denkbar und wahrscheinlich?

- Mit welchen **Schutzmaßnahmen** lassen sich die identifizierten Risiken so verringern, dass die Anforderungen der DSGVO hinreichend erfüllt sind und ein verantwortbarer, beherrschbarer Betrieb des Verfahrens aufgenommen werden kann? Denn das Ergebnis einer DSFA besteht in einem **DSFA-Bericht** an die Verantwortliche, die diese Empfehlungen bzgl. der Gestaltung des Verfahrens und des kontrollierten Betriebs von Schutzmaßnahmen, etwa zur Pseudonymisierung oder zur Anonymisierung von Daten, dann umsetzen und deren Wirksamkeit gem. Art. 35 nachweisen muss. Wenn der Betrieb trotz Schutzmaßnahmen weiterhin zu hohe Risiken birgt beziehungsweise ein zu geringes Schutzniveau für die Betroffenen aufweist, kann die Verantwortliche Kontakt zur zuständigen Datenschutz-Aufsichtsbehörde nehmen und dort um eine Empfehlung bitten. Dabei kann sich herausstellen, dass eine geplante Datenverarbeitung grundsätzlich nicht betrieben werden kann.

Sowohl bei der Bestimmung und Modellierung der Risiken in Bezug auf die erzeugten Daten, die beteiligten IT-Systeme und die Prozesse als auch beim Bestimmen wirksamer Schutzmaßnahmen griff die AutorInnengruppe auf das Standard-Datenschutzmodell-V2a (SDM) zurück. Neben dem SDM, das die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) seit 2018 zur Nutzung empfehlen, wurden unter anderen insbesondere das DSK-Kurzpapier Nr. 5 zur systematischen Durchführung der DSFA und das Working Paper Nr. 248 der Artikel-29-Arbeitsgruppe zur Analyse der Risikohöhe diese Verfahrens („Schwellwert-Analyse“) herangezogen.

Auf diese Weise strebte die AutorInnengruppe an, in möglichst vorbildlicher Weise sowohl den technischen, als auch den rechtlichen und methodischen Maßstab dafür auszuweisen, wie die Funktionen und die daraus sich ergebenden Datenschutz-Risiken einer Tracing-App für Betroffene in Zukunft zu analysieren, zu bestimmen und gegebenenfalls zu verringern sind.

Eine DSFA nach Artikel 35 DSGVO hat allerdings zwei Schwächen. Sie ist keine wissenschaftliche Technikfolgenabschätzung. Das bedeutet, dass sie von der Verantwortlichen weder eine gesellschaftliche Kontextierung der geplanten Verarbeitung noch eine Veröffentlichung der DSFA verlangt. Die AutorInnengruppe ist jedoch der Ansicht, dass ein Contact-Tracing-Verfahren mit einem derart hohen Risiko für die Grundrechte und mit der enormen Tragweite der Akzeptanz einer Überwachungs-App für die Gesellschaft insgesamt, grundsätzlich in den gesellschaftlichen Kontext gestellt werden sollte. Eine Überwachungs-App und überhaupt alle derartig eingriffsintensiven Systeme müssen mit ihren Risiken und deren Bearbeitung durch die verantwortliche Organisation einem öffentlichen Diskurs unterstehen, weswegen die dazugehörigen DSFAen grundsätzlich veröffentlicht werden sollten.

Referenz

Datenschutz-Folgenabschätzung (DSFA) für die Corona-App,
https://www.fiff.de/presse/dsfa-corona

FIfF e. V.

Empfehlungen für die Verantwortlichen

zur Gestaltung der Verarbeitung und Umsetzung der identifizierten Schutzmaßnahmen

Diese DSFA-Projektgruppe empfiehlt der Verantwortlichen für das Verfahren, mit dem riskante Kontakte mit COVID-19-infizierten Personen unter Zurhilfenahme einer Smartphone-App identifiziert werden sollen, die Gestaltung der Verarbeitung und das Treffen von Schutzmaßnahmen wie folgt anzugehen, um die Anforderungen der DSGVO umzusetzen:

1. Es müssen geeignete Rechtsgrundlagen geschaffen und Verantwortlichkeiten geklärt werden. Die Verarbeitung als „freiwillig“ auszuweisen und auf der Grundlage von Einwilligungen umzusetzen, genügt den datenschutzrechtlichen Anforderungen nicht, insbesondere weil Zweifel an der Freiwilligkeit und Informiertheit bestehen. Stattdessen müssen gesetzliche Grundlagen geschaffen werden, die diese Anforderungen, insbesondere zur Zweckbindung, zur Anonymisierung, zum Löschkonzept und zum Datenschutzmanagement, umsetzen. Dabei ist nicht allein auf die technischen Spezifikationen einer App zu achten, sondern es ist das gesamte Verfahren einschließlich der Schnittstellen, zum Beispiel Einbindung in das geplante elektronische Meldeverfahren, zu berücksichtigen. Ebenso sind unerwünschte technische und soziale Nebenwirkungen, die Einfluss auf die Grundrechtsausübung nehmen und sich damit auch mittelbar auf die Akzeptanz des Verfahrens auswirken, zu berücksichtigen. So muss sichergestellt werden, dass Dritte keine Einsicht in die App und ihre Anzeigen auf den Smartphones von Betroffenen nehmen können. Die Gesetzgeber*In muss eine Verordnung nach § 14 Absatz 8 IfSG erlassen, die technische Anforderungen datenschutzkonform konkretisiert.

2. An zwei Stellen der gesamten Prozesskette ist der Personenbezug besonders heikel; nämlich im Kontext der Erstellung und Speicherung der TempIDs sowie im Kontext des Uploads der Gesundheits-TempIDs von CV-infizierten Personen und ihrer Speicherung auf dem Server. Diese neuralgischen Stellen müssen wie folgt gestaltet werden: