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
ten Betriebs von Schutzmaßn
sierung oder zur Anonymisie
zen und deren Wirksamkeit g
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.
Verantwortlichen weder eine ge-
er geplanten Verarbeitung noch
verlangt. Die AutorInnengruppe
n 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.

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

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 GesetzgeberIn 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:

a. Bei der Erstellung der TempIDs in der App muss sichergestellt werden, dass es keine Verkettung zwischen TempIDs gibt und geben kann. Eine konkrete TempID darf also nicht aus der zeitlich vorhergehenden oder anderen gemeinsamen Komponenten abgeleitet werden können. Die TempIDs müssen in der App so gespeichert werden, dass sich nachträglich nicht feststellen lässt, in welcher Reihenfolge sie erzeugt und gespeichert wurden.

b. Die BetreiberIn des oder der Server muss ein wirksames Trennungsverfahren einsetzen, das Gesundheits-TempIDs aus den Apps von COVID-19-infizierten Personen auf dem Server in Infektionsanzeigende Daten ohne Personenbezug (iDoP) transformiert und das rechtlich, organisatorisch und technisch abgesichert geschieht (Podlech 1976). Rechtlich muss die BetreiberIn eine unabhängige Stelle sein, die keine eigenen Interessen an den Daten haben darf und vor Pflichten zur Herausgabe von Daten geschützt ist, auch gegenüber Sicherheitsbehörden. Organisatorisch müssen die Verantwortliche strategisch und die BetreiberIn operativ eine Mixstruktur etablieren, die dafür sorgt, die funktionale Differenzierung bzw. die informationelle Gewaltenteilung innerhalb der Organisation durchzusetzen – so, wie beispielsweise Rechtsprechung und Gerichtsverwaltung zusammen und doch getrennt in der Gerichtsorganisation arbeiten. Die BetreiberIn muss ein Datenschutzmanagement etablieren, das es erlaubt, die Trennung prüfbar wirksam durchzusetzen und aufrechtzuerhalten. Technisch muss sie die Trennung so umsetzen, dass Uploads der Gesundheits-TempID nicht protokolliert werden können, weder auf dem Server noch im Netzwerk der BetreiberIn. Darüber hinaus muss der Upload der Gesundheits-TempIDs zwischen Apps und Servern Ende-zu-Ende-verschlüsselt erfolgen und durch die Nutzung vorgeschalteter Anonymisierungsproxies (z. B. Tor) gesichert werden. Im Rahmen einer Datenschutzkontrolle muss das Trennungsverfahren einer stetigen Prüfung durch die zuständige Datenschutzaufsichtsbehörde unterliegen.

Die IT-Sicherheit der genutzten IT-Komponenten in der gesamten Prozesskette, unter Einbeziehung auch der Interaktion mit ÄrztInnen und Gesundheitsämtern, muss nach BSI IT-Grundschutz oder im Rahmen von ISO-27001 zertifiziert werden. Hier sind insbesondere Aspekte der Sicherstellung der Verfügbarkeit, insbesondere der Server (-Infrastrukturen), der Authentisierung der beteiligten IT-Komponenten sowie der Vertraulichkeit der Kommunikationsbeziehungen für hohen Schutzbedarf zu beachten.

3. Flankierend zur Veröffentlichung der App muss rechtlich und faktisch sichergestellt werden, dass NutzerInnen Dritten gegenüber weder den Status der App noch die Existenz der App auf dem eigenen Gerät bekannt geben müssen. Eine Ausnahme könnte ärztliches Personal bilden, um Heimquarantäne auch bei ArbeitgeberInnen anhand von Krankschreibungen durchzusetzen. Ziel dieser Regelungen ist das Sicherstellen der Zweckbindung der Aktivitäten der App. Zugangskontrollen zu öffentlichen und privaten Gebäuden, Universitäten, Schulen, Transportmitteln, Verwaltungen, Polizeidienststellen etc., bei denen eine Einsichtnahme in die App verlangt wird, sind zu unterbinden.

4. Vor Veröffentlichung der App muss von einer unabhängigen Stelle eine umfassende Software- und Gesamtsystem-Untersuchung durchgeführt und veröffentlicht werden. Hierbei ist insbesondere auch auf die Risiken zu achten, die sich aus Interaktionen mit Betriebssystem-Komponenten ergeben und potenziell auch für Nicht-NutzerInnen der App relevant sind (siehe Angriffsszenario B5 in Kapitel 7). An der Kooperationsbereitschaft großer Plattformunternehmen (Google, Apple) oder an rechtlichen bzw. faktischen Hürden bei der Sicherstellung von Datenschutzvorgaben (siehe etwa den US-CLOUD-Act oder das PRISM-Programm der National Security Agency) könnte dieser Punkt scheitern. Sollte etwa das Risiko nicht ausgeschlossen werden können, dass Plattformen die Kontaktereignisse mitlesen und das Matching mit infizierten Personen selbst durchführen können, wäre die Einstellung des Vorhabens einer Corona-App die gebotene Konsequenz.

Das FIfF bittet um Eure Unterstützung

Viermal im Jahr geben wir die FIfF-Kommunikation heraus. Sie entsteht durch viel ehrenamtliche, unbezahlte Arbeit. Doch ihre Herstellung kostet auch Geld – Geld, das wir nur durch Eure Mitgliedsbeiträge und Spenden aufbringen können.

Auch unsere weitere politische Arbeit kostet Geld für Öffentlichkeitsarbeit, Aktionen und Organisation. Unsere jährlich stattfindende FIfF-Konferenz, der Weizenbaum-Preis, weitere Publikationen, Kommunikation im Web: Neben der tatkräftigen Mitwirkung engagierter Menschen sind wir bei unserer Arbeit auf finanzielle Unterstützung angewiesen.

Bitte unterstützt das FIfF mit einer Spende. So können wir die öffentliche Wahrnehmung für die Themen weiter verstärken, die Euch und uns wichtig sind.

Spendenkonto:
Bank für Sozialwirtschaft (BFS) Köln
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX