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

FIfF e. V. – Stellungnahme

FIfF veröffentlicht Datenschutz-Folgenabschätzung (DSFA) für die Corona-App

14. April 2020 – „Es geht nicht um Privatsphäre, sondern es geht darum, eine Technik sozial beherrschbar zu machen." *Dieses Datenschutzverständnis von Wilhelm Steinmüller (1934–2013), Datenschutzpionier und langjähriges FIfF-Mitglied, möchten wir, eine Gruppe WissenschaftlerInnen und DatenschützerInnen im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V., wieder stark machen.*

Seit einigen Wochen kreist die Diskussion um die Eindämmung der Corona-Pandemie zunehmend um den Einsatz technischer Hilfsmittel. Es wird geplant, die Pandemie durch den Einsatz von Tracing-Apps für Smartphones einzudämmen. Diese Systeme sollen automatisiert die zwischenmenschlichen Kontakte aller NutzerInnen aufzeichnen und es so erlauben, die Infektionsketten des Virus schnell und effizient nachzuvollziehen, um möglicherweise exponierte Personen frühzeitig warnen und isolieren zu können.

Wir haben es angesichts der geplanten Corona-Tracing-Systeme mit einem gesellschaftlichen Großexperiment zur digitalen Verhaltenserfassung unter staatlicher Aufsicht in Europa zu tun. **Die europäische Datenschutzgrundverordnung (DSGVO) verpflichtet die BetreiberInnen umfangreicher Datenverarbeitungssysteme (zu denen auch ein Corona-Tracing-System zählen würde) zur Anfertigung einer Datenschutz-Folgenabschätzung (DSFA) im Falle eines hohen Risikos für die Grund- und Freiheitsrechte.** Hierbei handelt es sich um eine strukturierte Risikoanalyse, die mögliche grundrechtsrelevante Folgen einer Datenverarbeitung im Vorfeld identifiziert und bewertet.

Wirksamkeit und Folgen entsprechender Apps sind noch nicht absehbar und es ist davon auszugehen, dass innerhalb der EU verschiedene Varianten erprobt und evaluiert werden. Die datenschutz- und somit grundrechtsrelevanten Folgen dieses Unterfangens betreffen potenziell nicht nur Einzelpersonen, sondern die Gesellschaft als Ganze. Aus diesem Grunde ist nicht nur die Anfertigung einer DSFA angezeigt, sondern insbesondere auch ihre Veröffentlichung – und eine öffentliche Diskussion. Da bisher keine der beteiligten Stellen eine allgemein zugängliche DSFA präsentiert hat und selbst die vorgelegten *privacy impact assessments* unvollständig bleiben, **legen wir vom FIfF mit diesem Dokument eigeninitiativ eine solche Datenschutz-Folgenabschätzung als konstruktiven Diskussionsbeitrag vor.**

Zusammenfassung und Ergebnisse

1. Die in den Diskussionen vielfach betonte Freiwilligkeit der App-Nutzung ist eine Illusion. Es ist vorstellbar und wird auch bereits diskutiert, dass die Nutzung der App als Voraussetzung für die individuelle Lockerung der Ausgangsbeschränkungen gelten könnte. Das Vorzeigen der App könnte als Zugangsbarriere zu öffentlichen oder privaten Gebäuden, Räumen oder Veranstaltungen dienen. Denkbar ist, dass ArbeitgeberInnen solche Praktiken schnell adaptieren, weil sie mittels freiwillig umgesetzter Schutzmaßnahmen schneller ihre Betriebe wieder öffnen dürfen. Dieses Szenario bedeutet eine implizite Nötigung zur Nutzung der App und bedeutet erhebliche Ungleichbehandlung der Nicht-NutzerInnen. Weil nicht jede Person ein Smartphone besitzt, wäre hiermit auch eine Diskriminierung ohnehin schon benachteiligter Gruppen verbunden. Kirsten Bock vom FIfF kommentiert: „*Die Einwilligung ist nicht das richtige Regelungsinstrument für die Nutzung der Corona-App, weil deren Voraussetzungen nicht erfüllt sind. Der Gesetzgeber ist aufgerufen, das Nutzungsrisiko der App nicht auf die BürgerInnen abzuwälzen, sondern selbst die Voraussetzungen für eine freiwillige, sichere und grundrechtsverträgliche Lösung in einem Gesetz vorzugeben und die BürgerInnen so vor Grundrechtsverletzungen – auch durch Dritte – wirksam zu schützen.*" Martin Rost vom FIfF ergänzt prägnant: „*Von einer Einwilligung geht keine Schutzwirkung für Betroffene aus.*"

2. Ohne Intervenierbarkeit und enge Zweckbindung ist der Grundrechtsschutz gefährdet. So besteht ein hohes Risiko fälschlich registrierter Expositionsereignisse (falsch positiv), die zu unrecht auferlegte Selbst-Isolation oder Quarantäne zur Folge haben (zum Beispiel Kontaktmessung durch die Wand zwischen zwei Wohnungen). Um dem zu begegnen, bedarf es rechtlicher und faktischer Möglichkeiten zur effektiven Einflussnahme, etwa das Zurückrufen falscher Infektionsmeldungen, die

Löschung falsch registrierter Kontaktereignisse zu einer infizierten Person und das Anfechten von infolge der Datenverarbeitung auferlegter Beschränkungen. Eine solche Möglichkeit sieht bisher keines der vorgeschlagenen Systeme vor. „*Beim Datenschutz geht es genauso wenig um den Schutz von Daten, wie es beim Sonnenschutz um den Schutz der Sonne geht oder beim Katastrophenschutz um den Schutz von Katastrophen*“, spitzt Jörg Pohle vom FIfF zu.

3. Alle bislang erwähnten Verfahren verarbeiten personenbezogene Gesundheitsdaten. Das Verfahren besteht aus der Verarbeitung von Kontaktdaten auf den Smartphones, der Übermittlung dieser Daten auf einen Server nach der Diagnose einer Infektion und letztendlich deren Verteilung an alle anderen Smartphones zur Prüfung auf einen möglichen Kontakt mit Infizierten. Alle Daten auf einem Smartphone sind personenbezogen, nämlich bezogen auf die NutzerIn des Gerätes. Weil nur diejenigen Personen Daten übertragen, die als infiziert diagnostiziert wurden, sind die übertragenen Daten zugleich Gesundheitsdaten. Somit unterliegen diese dem Schutz der DSGVO.

4. Anonymität der NutzerInnen muss in einem Zusammenspiel rechtlicher, technischer und organisatorischer Maßnahmen erzwungen werden. Nur durch einen mehrdimensionalen Ansatz kann der Personenbezug wirksam und irreversibel von den verarbeiteten Daten abgetrennt werden, so dass danach von anonymen Daten gesprochen werden kann. Allen derzeit vorliegenden Vorschlägen fehlt es an einem solchen expliziten Trennungsvorgang. „*Wenn man sich hier nur auf technische Maßnahmen oder allein auf politische Beteuerungen verlässt, besteht ein großes Risiko der nachträglichen De-Anonymisierung*“, so Rainer Mühlhoff vom FIfF. Wir haben in dieser DSFA rechtliche, technische und organisatorische Anforderungen formuliert, deren Umsetzung in der Praxis eine wirksame und irreversible Trennung sicherstellen kann – nur unter diesen Voraussetzungen dürften die infektionsanzeigenden Daten ohne Personenbezug (iDoP) an alle Apps verbreitet werden.

Wesentliche Voraussetzung für Transparenz bezüglich der Umsetzung aller Datenschutz-Grundsätze nicht nur für Datenschutzaufsichtsbehörden, sondern gerade auch für die Betroffenen und die (Zivil-)Gesellschaft insgesamt, ist die quelloffene Entwicklung von Server und Apps nebst allen ihren Komponenten beispielsweise als freie Software. Nur so kann es gelingen, Vertrauen auch bei jenen zu erzeugen, die nicht alle informationstechnischen Details verstehen. Ergriffene Maßnahmen müssen immer aktiv prüfbar gemacht und sauber dokumentiert werden.

Abschluss

Datenschutzanalysen betrachten die gesamte Verarbeitung von Daten, nicht nur die dabei eingesetzten Apps. „*Die Grenzen der App sind nicht die Grenzen der Verarbeitung*“, erläutert Christian Ricardo Kühne vom FIfF. In der öffentlichen Diskussion und in den betrachteten App-Projekten wird Datenschutz nach wie vor auf den Schutz der Privatsphäre, also Geheimhaltung gegenüber BetreiberInnen und Dritten, und auf Aspekte der IT-Sicherheit wie Verschlüsselung reduziert. Mit dieser Verengung der Sichtweise kommen die erheblichen, gesellschaftlich wie politisch fundamentalen Risiken, die wir in dieser Folgeabschätzung aufzeigen, nicht nur nicht in den Blick – sie werden zum Teil sogar verschleiert. „*Aus dem Blickwinkel des Datenschutzes gehen die wesentlichen Risiken nicht von HackerInnen oder anderen BenutzerInnen aus, sondern von den BetreiberInnen des Datenverarbeitungssystems selbst*“, kommentiert abschließend Rainer Rehak, Vorstandsmitglied des FIfF.

Referenzen

Download der DSFA (Creative-Commons-Lizenz: Namensnennung, CC BY 4.0 Int.) unter https://www.fiff.de/dsfa-corona: Deutsch, Englisch, Spanisch (Solamente el resumen), Französisch (Seulement le résumé) in der jeweils aktuellen Fassung. Diskussion im FIfF-Github-Repositorium: https://github.com/fiff-de/dsfa-corona

Data Protection Risks of a Corona App: Full updated version of the Data Protection Impact Assessment (DPIA) now available in English

29th of April 2020 – *Doubts about usefulness of Corona App remain, even decentralised variants involve considerable risks – FIfF presents DPIA update in English at https://www.fiff.de/dsfa-corona*

The debate about the data protection-compliant design of a corona app has intensified in recent days. The app digitally supports the so called „contact tracing“ which intends to break COVID-19 infection chains by warning people who have been exposed to someone tested positive. Initially, the only goal pursued by the German government was to introduce an app with a warning functionality for those potentially infected, but in the meantime, further purposes beyond tracing are being discussed which would cause more infringements of fundamental rights. However, there are still general doubts about the effectiveness of digital contact tracing for containing the pandemic, as the discussion about false positives caused by e.g. walls, masks or varying Bluetooth signal strengths shows. The accusations that pushing such a corona app project primarily signals political actionism or that the project might accustom the general population to future tracing or tracking projects by government bodies have not yet been dispelled.

In the course of the current discussion about a ‚stay at home‘ order exit strategy, the use of a corona app has been considered strategic in other countries and is now also being considered by the German government. The German Minister of Health, Jens Spahn, has recently switched his preference from a centralized, and from a data protection point of view riskier architecture, to a decentralized model. Austria and Switzerland have already adopted the decentralized DP-3T implementation**. With the publication of a DPIA, we are pursuing the goal of informing the discussion about the far-reaching consequences of these decisions and contributing to making this app as data protection-friendly as possible.**

One of the central questions relevant to data protection is: How is the purpose limitation of the overall system secured and enforced? How can misuse, especially by the operators, be pre-

vented by technical, organizational, and legal means? It will be decisive for the success of a data protection-friendly Corona App to restrict the purpose solely to informing potentially infected persons. In our view adding other purposes such as epidemiological studies, an immunity pass function, or detailed quarantine monitoring poses disproportionate risks and infringements of fundamental rights and is therefore not justifiable.

The question of centralisation vs. decentralisation is of crucial importance for data protection due to the following circumstance: In a central architecture, an almost ‚omniscient' server coordinates all procedural activities; It collects all contact events from infected users and notifies persons at risk. In a decentralized architecture, however, the server has no access to the contact events of users. It only stores non-identifying infection indicating data. The apps themselves detect possible infection events; the necessary calculations are performed on the devices of the respective users. If a government agency were to be given blanket access to contact events of infected and non-infected persons, this would not only be a considerable violation of data protection, but also a collection of data that is simply not necessary for the purpose, i.e. a violation of the principle of data minimization. **„So far, the European Parliament, Germany, Austria, Ireland and Switzerland have spoken out in favour of a decentralised variant, whereas France still favours the centralised one. The FIfF would like to urgently point out the danger that a centralised system will be followed by extensive possibilities for subsequent use, which generates considerable potential for abuse."** warns Kirsten Bock from FIfF.

A decentralised model is clearly preferable to a centralised one, but it is also not free of serious data protection risks. Therefore, the FIfF now presents a model data protection impact assessment (DPIA) for decentralised architectures. In doing so we refer to a requirement under Art. 35 of the General Data Protection Regulation (GDPR), which is directed towards the future controller of such data processing. The purpose of this model DPIA is to demonstrate in a publicly accessible way the risks for data subjects. **„It needs to be underlined that the data protection risks also affect persons who do not use the app themselves",** says Rainer Mühlhoff, FIfF e. V. Furthermore, with this document we present recommendations for the (re)design of the app and the processing procedure as well as protective measures concerning a whole list of possible weaknesses and attacks.

„With this DPIA, we have set a new standard that others whose data processing creates high risks for fundamental rights and freedoms have to meet from now on." comments Rainer Rehak from FIfF. **„And we are also showing that DPIAs must be published as a matter of principle so that society can discuss these risks in an informed manner and exert pressure on those responsible to protect our fundamental rights when processing data,"** adds Jörg Pohle, also from FIfF.

With this DPIA, now completely available in English, we intend to enrich the pan-European discussion on data protection. Data protection, not privacy, is the guarantor for the protection of all fundamental rights in the digital age.

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 –