Datenschutz-Folgenabschätzung für die Corona-App

Kirsten Bock
kirsten.bock@fiff.de

Christian Ricardo Kühne
demian@fiff.de

Rainer Mühlhoff
rainer.muehlhoff@fiff.de

Měto R. Ost
meto.ost@fiff.de

Jörg Pohle
joerg.pohle@fiff.de

Rainer Rehak
rainer.rehak@fiff.de

Version 1.1 – 14. April 2020

Forum InformatikerInnen für Frieden und
gesellschaftliche Verantwortung (FIfF) e. V.

Kontakt: dsfa-corona@fiff.de

https://www.fiff.de/dsfa-corona

https://www.fiff.de/dsfa-corona

© 2020 Die Autorïnnen

Version 1.0 erschienen am 14. April 2020.

Dokument verfügbar unter:
https://www.fiff.de/dsfa-corona

Erschienen unter der Creative Commons
Lizenz – Namensnennung (CC BY 4.0 Intl.).

Inhaltsverzeichnis

Zusammenfassung und Ergebnisse

Seit der Ausbreitung des SARS-CoV-2-Virus auch in Europa Anfang 2020 lässt eine technische Vision unsere öffentlichen und politischen Debatten nicht mehr los: Die Pandemie könnte möglicherweise durch den Einsatz von Tracing-Apps für Smartphones eingedämmt werden. Dieses System würde automatisiert die zwischenmenschlichen Kontakte aller Nutzerïnnen aufzeichnen und es so erlauben, die Infektionsketten des Virus schnell und effizient nachzuvollziehen, um möglicherweise exponierte Personen frühzeitig isolieren zu können.

Staaten wie Singapur, Südkorea und Israel haben für diese Vorgehensweise teils radikale Vorbilder geliefert, die aus Sicht europäischer Rechtssysteme mit unverhältnismäßigen Grundrechtseingriffen verbunden sind. In Reaktion darauf haben sich europäische Initiativen gebildet, insbesondere das *Pan-European Privacy Preserving Proximity Tracing* (PEPP-PT)-Konsortium, die das Konzept einer Corona-Tracing-App aufgreifen und bereits im Namen mit einer Verpflichtung auf Datenschutz – oder zumindest auf »privacy«, was nicht dasselbe ist, – verbinden. So werden aktuell Tracing-Systeme konzipiert, die im Verhältnis zu den Maßnahmen bestimmter außereuropäischer Länder *vergleichsweise* datenschutzfreundlicher sind. Ein begleitender Mediendiskurs vermittelt seit Wochen konsequent das Bild: Corona-Apps *made in Europe* versprechen, die »Privatsphäre« aller Nutzerïnnen zu wahren und mit der EU-Datenschutzgrundverordnung (DSGVO) konform zu sein.

Datenschutzfreundlichkeit jedoch ist keine Ja/Nein-Frage, sondern eine komplexe Erwägung, die einer präzisen und detaillierten Diskussion bedarf. Die DSGVO selbst verpflichtet die Betreiberïnnen umfangreicher Datenverarbeitungssysteme (zu denen auch ein Corona-Tracing-System zählen würde, siehe Abschnitt 6) 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.

Wir haben es angesichts der geplanten Corona-Tracing-Systeme mit einem gesellschaftlichen Großexperiment zur digitalen Verhaltenserfassung unter staatlicher Aufsicht in Europa zu tun. 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 sind, legen wir – eine Gruppe Wissenschaftlerïnnen und Datenschützerïnnen im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. – mit diesem Dokument eigeninitiativ eine solche Datenschutz-Folgenabschätzung als konstruktiven Beitrag vor.

Überblick über das Verfahren

Wir beziehen uns in dieser DSFA auf die primär diskutierten Frameworks und Konzeptentwürfe für eine europäische Corona-Tracing-App, die auf Nahfeldsensortechnik mittels Bluetooth Low Energy (BTLE) beruhen. Dazu zählen insbesondere PEPP-PT, DP-3T, sowie ein allgemeines, vom CCC-Mitglied Linus Neumann vorgelegtes Konzept (siehe Neumann 2020). Unter diesen Projekten stellt PEPP-PT ein Rahmenkonzept dar, also keine konkrete App, sondern eine Spezifikation für ein solches Datenverarbeitungssystem. Innerhalb dieses Rahmens sind verschiedene Implementierungen, also konkrete Systeme/Apps, die das Framework umsetzen, denkbar; das DP-3T-Projekt ist dafür ein konkreter Vorschlag unter mehreren. Das PEPP-PT-Framework lässt prinzipiell zu, dass jede europäische Nation ihre eigene Implementierung entwickelt. Das Framework bietet also Gestaltungsspielraum, während es zugleich eine grenzüberschreitende Interoperabilität gewährleisten möchte.

In dieser Situation ist es ein zentrales Ergebnis unserer Untersuchung, dass alle betrachteten Frameworks – und insbesondere gilt dies für PEPP-PT – **wichtige technische Merkmale und Verfahrenseigenschaften offen lassen, die mit wesentlichen datenschutzrelevanten Folgen verbunden sind.** Es lassen sich grob mindestens drei Systemarchitekturen unterscheiden, die alle mit dem PEPP-PT-Framework kompatibel wären (vgl. Kapitel 1):

a) Eine **zentralisierte Architektur**: Anonymität der Nutzerïnnen und Geheimhaltung der Kontaktereignisse wird hier nur nach außen, also gegenüber anderen Nutzerïnnen und externen Akteurïnnen, angestrebt; die Betreiberïnnen und beteiligten Behörden können alle Nutzerïnnen identifizieren und mit den aufgezeichneten Kontakthistorien in Zusammenhang bringen.

b) Eine **teilweise dezentralisierte Architektur**, die zugleich **epidemiologische Forschung** erlaubt (DP-3T): Nutzerïnnen und Kontaktereignisse bleiben nur gegenüber anderen Nutzerïnnen und Dritten geheim, während der Server infizierte Nutzerïnnen de-anonymisieren kann. Das System verfügt über eine Datenspendefunktion, durch die Nutzerïnnen ihre Kontakthistorien für epidemiologische Untersuchungen zugänglich machen können – in diesen Fällen werden Kontaktereignisse infizierter Nutzerïnnen auch für Betreiberïnnen und Behörden nachvollziehbar.

c) Ein **gänzlich dezentralisierte Architektur** (vgl. Neumann 2020): Gegenüber anderen Nutzerïnnen und Dritten bleiben Nutzerïnnen anonym und Kontaktereignisse geheim. Betreiberïnnen und Behörden können infizierte Nutzerïnnen deanonymisieren, nicht jedoch ihre Kontakthistorien. Epidemiologische Untersuchungen werden nicht unterstützt.

Betreiberïnnen und Behörden können ...	Variante a	Variante b	Variante c
... alle Nutzerïnnen de-anonymisieren	ja	nein	nein
... infizierte Nutzerïnnen de-anonymisieren	ja	ja	ja
... alle Kontakte nachvollziehen	ja	teilweise	nein

Unsere **DSFA bezieht sich schwerpunktmäßig auf die datenschutzfreundlichste Variante c,** teilweise gehen wir auf technische Details von Variante b ein.

Im Ergebnis zeigt sich erstens, dass **selbst die dezentrale Implementierung zahlreiche gravierende Schwachstellen** (siehe Kapitel 7) **und Risiken** birgt, denen begegnet werden muss. Zweitens zeigt ein Vergleich der zentralen und dezentralen Varianten, den wir an relevanten Stellen ziehen, dass **wesentliche Datenschutz-Konsequenzen mit der Entscheidung zwischen Zentralität und Dezentralität verbunden sind.** Eine beliebige PEPP-PT-Implementierung als datenschutzfreundlich zu bezeichnen, ist deshalb pauschal nicht zutreffend.

Die wichtigsten Erkenntnisse, Risiken und Lösungsansätze

Wir führen hier vorab eine Auswahl der wichtigsten Erkenntnisse, Risiken und Lösungsansätze an:

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 Arbeitgeberïnnen 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 führt zu einer erheblichen Ungleichbehandlung der Nicht-Nutzerïnnen. Weil nicht jede Person ein Smartphone besitzt, wäre hiermit auch eine Diskriminierung ohnehin schon benachteiligter Gruppen verbunden.

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.

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 Nutzerïn 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 Nutzerïnnen muss in einem Zusammenspiel rechtlicher, technischer und organisatorischer Maßnahmen erzwungen werden.** Nur durch einen mehrdimensionalen Ansatz kann der Personenbezug wirk-

> sam 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. 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.

Für eine umfassende Darstellung der Risiken und Schwachstellen verweisen wir auf Kapitel 7, für die notwendigen Schutzmaßnahmen auf Kapitel 8.

Die Perspektive des Datenschutzes geht grundsätzlich davon aus, dass **die wesentlichen Risiken der Datenverarbeitung von den Betreiberïnnen eines Datenverarbeitungssystems ausgehen.** In solchen Fällen ist es dringend erforderlich, dass die Barriere zur einer missbräuchlichen Verarbeitung, die den Datenverarbeitungszweck übersteigt, in einer wirksamen Kombination von rechtlichen, technischen und organisatorischen Maßnahmen besteht – und nicht bloß in öffentlich geäußerten Versprechungen der Betreiberïnnen, den Datenschutz zu beachten. Ergriffene Maßnahmen müssen aktiv prüfbar gemacht und sauber dokumentiert werden.

Die quelloffene Entwicklung von Server und Apps nebst allen ihren Komponenten – beispielsweise als freie Software – ist eine wesentliche Voraussetzung, damit es **Transparenz bezüglich der Umsetzung der Datenschutz-Grundsätze** nicht nur für Datenschutzaufsichtsbehörden, sondern gerade auch für die Betroffenen und die (Zivil-)Gesellschaft insgesamt gibt. Nur so kann es gelingen, Vertrauen auch bei jenen zu erzeugen, die nicht alle informationstechnischen Details verstehen.

Auch von Dritten können Risiken für Grundrechte ausgehen. Dabei ist nicht in erster Linie an Hackerïnnen, sondern an **kommerzielle Akteurïnnen,** etwa große Plattformbetreiberïnnen, und staatliche Stellen zu denken. Diese profitieren gegebenenfalls von einem erhöhten Aufkommen an Tracking-Daten, die sie selbst auswerten können, weil Bluetooth für die Corona-App immer eingeschaltet sein muss, oder durch umfassende Zugriffmöglichkeiten auf Daten, die bei privaten Akteurïnnen gespeichert sind.

Datenschutzanalysen betrachten die gesamte Verarbeitung von Daten, nicht nur die dabei eingesetzten Apps.

In der öffentlichen Diskussion und in den betrachteten App-Projekten wird Datenschutz nach wie vor auf den Schutz der Privatsphäre, also Geheimhaltung gegenüber Betreiberïnnen 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.

Kapitel 1

Einleitung

Gemäß Art. 35 der Datenschutz-Grundverordung (DSGVO) muss eine Verantwortliche einer Datenverarbeitung eine Datenschutz-Folgenabschätzung (DSFA) dann vorlegen, wenn von der geplanten Datenverarbeitung ein (voraussichtlich) hohes Risiko für die Rechte und Freiheiten der davon betroffenen Personen ausgeht.

Für die hiermit vorliegende DSFA steht noch nicht fest, welche Organisation für die Gestaltung und den Betrieb einer Verarbeitung mit Hilfe einer Tracing-App, wenn sie denn realisiert wird, verantwortlich sein wird. Ebensowenig ist die rechtliche und die funktionale Ausgestaltung der Datenverarbeitung festgelegt. *Die vorliegende DSFA wird deshalb für eine Datenverarbeitung mit Hilfe einer Tracing-App vorgelegt, die im Urteil der Autorïnnen den Zweck funktional vollumfänglich erfüllt und dabei im geringst möglichen Umfang in die Rechte und Freiheiten von Personen eingreifen würde.* Für diesen Zweck werden die möglichen Auswirkungen im Hinblick auf die Relevanz der identifizierten Risiken (Validität), die Wirksamkeit der Maßnahmen und deren Belastbarkeit (Reliabilität) antizipiert.

Grundsätzlich gilt, dass mit einer dokumentierten Durchführung einer DSFA eine Verantwortliche ihre Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) zur Einhaltung der datenschutzrechtlichen Anforderungen erfüllt.

1.1 Ziele und Zwecke dieses Textes

Ziel des vorliegenden Textes ist die Erstellung einer DSFA nach Art. 35 DSGVO für die Verarbeitung von Kontaktdaten mithilfe einer Smartphone-App, die mit Nahfeldsensortechnik wie Bluetooth Low Energy Beacon Kontaktereignisse aufzeichnet, der Übertragung von Daten aus der App auf einen oder mehrere Server im Fall der Infektion der App-Nutzerïn, der Bereitstellung dieser Daten an alle Nutzerïnnen zum Zweck ihrer Information über mögliche Kontakte zu SARS-CoV-2-Infizierten. Die Anforderungen des Art. 35 DSGVO werden erfüllt, wenn der Verantwortlichen ein DSFA-Bericht mit Empfehlungen vorgelegt wird, erstens, und zweitens auch die empfohlenen Maßnahmen implementiert sind und der Nachweis der Wirksamkeit der getroffenen Maßnahmen erbracht ist.

Für die vorliegende DSFA unterscheiden wir folgende Typen von Smartphone-Apps nach den verarbeiteten Datenarten:

- **Typ 1:** Verarbeitung von Standortdaten (GPS-, Mobilfunkmetadaten)
- **Typ 2:** Verarbeitung von Bewegungsdaten (aggregierte GPS-, Mobilfunkmetadaten)
- **Typ 3:** Verarbeitung von Kontaktdaten (Nahfeldsensoren, zum Beispiel Bluetooth)

- **Typ 3 »zentral«:** Server bekommt alle Kontaktereignisse der Infizierten (inklusive der Informationen über IDs der Gefährdeten), Server informiert Gefährdete. (Beispiele: TraceTogether, PEPP-PT-Auslegung.)
- **Typ 3 »dezental + epidemiologisch«:** Server bekommt die (mathematisch zusammenhängenden) TempIDs der Infizierten und User können weitere Informationen zu Forschungszwecken freigeben, Smartphone errechnet Risiko lokal und informiert User lokal. (Beispiele: DP-3T, PEPP-PT-Auslegung.)
- **Typ 3 »rein dezentral«:** Server bekommt die (mathematisch nicht zusammenhängenden) IDs der Infizierten, Smartphone errechnet Risiko lokal und informiert User lokal. (Beispiel: Vorschlag von Linus Neumann, vgl. Neumann 2020.)

Die vorliegende DSFA betrachtet primär die Verarbeitungstätigkeit (VT) von Daten entsprechend Typ 3 im Rahmen des gesamten Verfahrens und bezieht sich aus Schärfungsgründen nur auf einen einzigen Zweck: Informieren von infektionsgefährdeten Personen. Die betrachtete VT bezieht sich daher auf Typ 3 »rein dezentral«, angereichert durch technische Details des DP-3T-Projektes, insofern sie sich auf diesen Zweck richten. Die von den Apps der Nutzerïnnen generierten und über Bluetooth verschickten temporären Identifier (*TempIDS*), die im Falle einer COVID-19-Diagnose zu *Gesundheits-TempIDs* werden, werden von der CV-infizierten Person an den Server oder die Server geschickt, wo sie in einem rechtlich, organisatorisch und technisch abgesicherten Trennungsverfahren anonymisiert werden. Anschließend können diese *infektionsanzeigenden Daten ohne Personenbezug* (iDoP)von allen App-Nutzerïnnen heruntergeladen werden. Die Personen sind dadurch in die Lage versetzt, anhand der eigenen, in ihrer App gespeicherten TempIDs und den *Kontaktdaten* (»fremden« TempIDs inkl. Zeitdauer und Signalstärkenprofil) mögliche Expositionsereignisse zu berechnen.

Es ist nicht das Ziel, mit Hilfe dieser DSFA eine App nach Typ 3 zu spezifizieren beziehungsweise zu realisieren, sondern ausschließlich die Risiken und Schutzmaßnahmen zu identifizieren, die sich anhand der Kriterien gemäß der DSGVO ergeben.

Es ist nicht das Ziel, ein »Privacy Impact Assessment« durchzuführen, das sich auf die Betrachtung der Auswirkungen auf die Privatsphäre beschränkt, sondern es werden die Auswirkungen auf alle Grundrechte und Grundfreiheiten natürlicher Personen betrachtet.

Es ist nicht das Ziel, ein »Surveillance Impact Assessment« durchzuführen, das nur die Auswirkungen von Verarbeitungsformen betrachtet, die als Überwachung bezeichnet werden können, sondern es werden alle Verarbeitungen personenbezogener Daten betrachtet.

Dieser Text will für den Fall einer Implementation dieses grundrechteschonenden Verfahrens wesentliche formale, strukturelle und inhaltliche Vorarbeiten leisten.

Ganz wesentlich für eine DSFA nach der DSGVO ist, dass nicht eine hervorstechende Technik, in diesem Falle die »Corona-App«, in den Fokus gestellt wird. Im Fokus der DSFA steht stattdessen das Verfahren insgesamt, das aus mehreren personenbezogenen Verarbeitungstätigkeiten besteht, in denen selbst wieder Vorgänge oder Vorgangsreihen stattfinden oder vorgenommen werden – teilweise technikgestützt. Die Betrachtung muss also über die Nutzung der App hinausgehen, denn Grenze der App ist nicht die Grenze der Verarbeitung. Wesentliches Definitionsmerkmal für ein Verfahren beziehungsweise für eine Verarbeitung ist der ausgewiesene Zweck (Hoffmann 1991).

Die Risikomodellierung im Datenschutz muss entschieden an dem Risiko aus der Perspektive des von der Verarbeitung Betroffenen ansetzen. Hier besteht das Risiko darin, dass die Verarbeitung zur Gänze nicht hinreichend grundrechteschonend gestaltet wurde und betrieben wird. Es ist unzureichend, ausschließlich oder insbesondere die Risiken einer nicht-hinreichenden IT-Sicherheit oder das Risiko finanzieller Schäden in den analytischen Blick zu nehmen (Rost 2018, Bieker, Bremert und Hansen 2018).

Als methodologische Grundlage zur Transformation von normativen Anforderungen in funktionale Anforderungen dient das Standard-Datenschutzmodell (SDM) in der Fassung V2.0a, das von der 98. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder im November 2019 beschlossen und vom IT-Planungsrat allen öffentlichen Verantwortlichen zur Nutzung empfohlen wurde (DSK SDM2.0a).

1.2 Zielgruppe des Textes

Die vorliegende DSFA wendet sich an

- politische Entscheiderïnnen im Bund und in den Ländern,
- Datenschutzaufsichtsbehörden des Bundes und der Länder,
- technische und juristische Expertïnnen,
- mögliche Herstellerïnnen und Betreiberïnnen sowie
- alle sonstigen Stakeholder.

1.3 Mitglieder der Projektgruppe

Ass. jur. Kirsten Bock studierte Rechtswissenschaften in Kiel und Guildford/UK mit Schwerpunkt Rechtsphilosophie und Rechtslogik, arbeitet im aufsichtsbehördlichen Bereich und ist Mitglied in Arbeitsgruppen des europäischen Datenschutzausschusses (EDSA). Sie forscht zu ethischen und gesellschaftlichen Grundsatzfragen des Datenschutzes, der Zertifizierung und dem Standard-Datenschutzmodell (SDM). Sie ist Mitglied des FIfF.

Dipl.-Inf. Christian Ricardo Kühne studierte Philosophie, Informatik und Soziologie; zurzeit forscht er als freier Akademiker im Bereich der Commons-Theorie und Kritischen Informatik über emanzipatorische Informations- und Kommunikationstechnologien. Nebenbei arbeitet er im GNUnet-Projekt an einem alternativen Internet-Stack mit. Er ist Mitglied des FIfF.

Dr. Rainer Mühlhoff studierte Mathematik, Informatik und theoretische Physik; promovierte in Philosophie. Er forscht zu Datenschutz im Kontext anonymer Massendaten, ethischen Fragen der Künstlichen Intelligenz und Sozialtheorie der digitalen Gesellschaft. Er arbeitet am Excellence Cluster *Science of Intelligence* an der Technischen Universität Berlin, ist Mitbegründer des *Berlin Ethics Lab for Responsible AI and Responsible Human-Computer Interaction* und Mitglied des FIfF.

Dr. Jörg Pohle studierte Informatik, Rechts- und Politikwissenschaften und promovierte in Informatik zur Geschichte und Theorie des Datenschutzes und Folgerungen

für die Technikgestaltung. Er forscht zu Technikanalyse und -gestaltung, Rechtsinformatik sowie Digitalisierung und Soziologischer Theorie. Er ist Leiter des Forschungsprogramms »Daten, Akteure, Infrastrukturen« am Alexander von Humboldt Institut für Internet und Gesellschaft in Berlin und Mitglied des FIfF.

Dipl.-Inf. Rainer Rehak studierte Informatik und Philosophie in Berlin, Hongkong und Peking. Er promoviert am Weizenbaum-Institut für die vernetzte Gesellschaft zu systemischer IT-Sicherheit. Er lehrt und forscht zu Datenschutz und Datensicherheit, staatlichem Hacking sowie Technikzuschreibungen. Er ist aktiv bei Amnesty International, als technischer Sachverständiger, etwa für Parlamente oder das Bundesverfassungsgericht und er ist Mitglied im Vorstand des FIfF.

Bei Fragen, Kritik, Ergänzungen oder Anregungen wenden Sie sich gern an die Autorïnnen via `dsfa-corona@fiff.de`.

1.4 Dokumente der methodologischen und inhaltlichen Grundlage zur Durchführung einer DSFA

Zur methodischen Durchführung dieser DSFA gem. Art. 35 DSGVO wurde insbesondere auf die folgenden Dokumente zurückgegriffen:

- Article 29 Data Protection Working Party (2013). *Opinion 03/2013 on purpose limitation*. Working Paper WP 203
- Article 29 Data Protection Working Party (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is »likely to result in a high risk« for the purposes of Regulation 2016/679, as last revised and adopted on 4 October 2017*. Working Paper WP 248
- Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2018a) [DSK KP5]. *Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO*. Kurzpapier Nr. 5
- Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2018c) [DSK KP18]. *Risiko für die Rechte und Freiheiten natürlicher Personen*. Kurzpapier Nr. 18
- Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2019) [DSK SDM2.0a]. *Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele*. Version 2.0a
- European Data Protection Board (2019b). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. Adopted on 13 November 2019
- European Union (2016) [GDPR]. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, 1–88*

– Michael Friedewald u. a. (2017). *Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz*. White Paper. Version 3. Forum Privatheit

Wir bedanken uns insbesondere bei Martin Rost für fruchtbare Anregungen, kritisches Feedback und erhellende Diskussionen, darüber hinaus bei Malte Engeler, Julian Hölzel, Niklas Rakowski und Lena Ulbricht für den wertvollen Austausch.

Kapitel 2

Kontextierung der Verarbeitung

Die Datenverarbeitung, die die vorliegende DSFA adressiert, stehen im Zusammenhang mit der weltweiten Corona-Pandemie, die Ende 2019 in Wuhan, Volksrepublik China, begann und sich seitdem über die ganze Welt ausgebreitet hat. Nach dem ersten Auftreten von Infektionen in Europa Ende Januar 2020 – zuerst in Frankreich am 24. Januar, vier Tage später in Deutschland – dauerte es bis Mitte März – etwa 40 Tage –, bis in Deutschland umfassende Maßnahmen ergriffen wurden, sowohl Vorbereitungs- wie Eindämmungsmaßnahmen. Am 22. März 2020 einigten sich Bund und Länder auf ein »umfassendes Kontaktverbot«, die Bundesländer Bayern, Berlin, Brandenburg, das Saarland, Sachsen und Sachsen-Anhalt darüber hinaus umfassende Ausgangsbeschränkungen. Mit dem Stand 7. April 2020 sollen die Maßnahmen bis mindestens 19. April 2020 aufrechterhalten werden.

In der Öffentlichkeit werden derzeit technikgestützte Verarbeitungstätigkeiten diskutiert, die es erlauben sollen, 1) die Ausbreitung der Pandemie nachzuvollziehen, um Vorhersagen über die weitere Ausbreitung treffen zu können, 2) die Pandemie zu stoppen und zumindest zu steuern, 3) potenziell Infizierte über ihre mögliche Infektion zu informieren sowie 4) das Kontaktverbot, die Ausgangsbeschränkungen und/oder individuelle Quarantäneauflagen zu überwachen und durchzusetzen, um von allgemeinen Maßnahmen, wie generellen Ausgangsbeschränkungen, zu risiko- und zielgruppenspezifischen Maßnahmen übergehen zu können, um damit die Auswirkungen von Infektionsschutzmaßnahmen insbesondere auf die Wirtschaft zu minimieren.[1]

2.1 Technikgestützte Verfahren weltweit

Inzwischen wurden eine ganze Reihe an technikgestützten Verarbeitungen in einer Vielzahl von Ländern eingeführt, darunter in der Volksrepublik China, Südkorea, Singapur, Israel und Österreich.[2]

Die Volksrepublik China verpflichtete ab Mitte Februar 2020 Bürger*innen zur Installation und Nutzung einer App auf dem Smartphone, mit der die Bewegung überwacht werden kann, um die Quarantänemaßnahmen durchzusetzen und Kontaktpersonen zu identifizieren. Die App übermittelt Bewegungsdaten an den oder die Server, auf denen (mögliche) Kontakte zu Infizierten identifiziert werden, im Anschluss werden die Besitzer*innen der Smartphones mit Farbcodes darüber informiert, wie sie sich zu verhalten haben – von mehr oder weniger Bewegungsfreiheit bis zu mehrwöchiger Zwangsisolation. Die App zeigt den Status bezüglich einer Corona-Infektion an, sie muss bei Polizei-

[1] Eine umfangreiche Kontextierung einer Verarbeitungstätigkeit ist kein obligatorischer Bestandteil einer DSFA nach Art. 35 DSGVO. Wir diskutieren andere Formen von Verarbeitungstätigkeiten mit gleichen, ähnlichen oder benachbarten Zwecken deshalb, um darzulegen, dass es eine Lösung für einen engen legitimen Zweck auch mit weniger intensiven Eingriffen in die Grundrechte der Bürgerinnen und Bürger gibt.

[2] Eine fortlaufend aktualisierte Übersicht findet sich unter GDPRhub-Liste.

und anderen Kontrollen vorgezeigt werden.

Südkorea verwendet Telefon- und Kreditkartendaten von Infizierten zur Nachverfolgung ihrer früheren Bewegungen, um mögliche Kontaktpersonen zu identifizieren. Personen, bei denen festgestellt wird, dass sie sich in der Nähe von infizierten Personen aufgehalten haben, erhalten telefonische Benachrichtigungen mit Informationen über ihre früheren Bewegungen. Darüber hinaus werden die Bewegungsdaten von Infizierten veröffentlicht, was nach Angaben der Regierung anonymisiert erfolgen soll, jedoch wurden bereits viele Betroffene re-identifiziert, es kam zu Fällen sozialer Stigmatisierung (Kim 2020).

Singapurs Government Technology Agency startete am 20. März die Verbreitung der Smartphone-App »TraceTogether«, die der Unterstützung von Kontaktverfolgungsmaßnahmen des Gesundheitsministeriums dient. Mit Hilfe einer App werden die Nutzenden bei einem zentralen Server identifiziert, anschließend wird ein zentral vergebenes Pseudonym an die App gesandt, das dann im täglichen Gebrauch per Bluetooth mit in der Nähe befindlichen Geräten ausgetauscht wird. Auch diese Daten werden an den Server geschickt. Im Falle der Infektion einer Person, werden die Kontakte ermittelt und die entsprechenden Personen informiert, um diese in Quarantäne zu schicken. Diese Quarantäne wird durch Überwachung der infizierten Personen anhand der GPS-Daten ihrer Smartphones durchgesetzt; die Infizierten müssen mithilfe von spontan abgefragten Fotos ihrer Wohnumgebung nachweisen, dass sie sich tatsächlich in ihrer Wohnung aufhalten.

In Österreich wurde am 25. März 2020 die App »Stopp Corona« vom Österreichischen Roten Kreuz veröffentlicht. Auf der Basis von eindeutigen Nutzerkennungen erlaubt es die App, dass Daten zwischen einander nahen Smartphones ausgetauscht werden, die dann als Kontakte gespeichert werden. Im Falle einer Infektion sollen sich die Nutzerïnnen über die App beim Verantwortlichen, dem Roten Kreuz, melden, die dann diejenigen Kontaktpersonen über die App verständigen, mit denen sie in den vergangenen 3 Kalendertagen in Kontakt waren. Diese Meldung löst die Sammlung weiterer Daten, darunter der Mobilfunknummer der Infizierten, aus. Das Österreichische Rote Kreuz tritt explizit als Verantwortlicher im Sinne der DSGVO auf, Entwicklung und Betrieb liegen in den Händen von Accenture, die Dienste werden in der Microsoft Azure Cloud gehostet und für die Benachrichtigungen wird Googles Firebase Cloud Messaging verwendet.[3]

Israels Regierung hat am 18. März 2020 unter Umgehung des israelischen Parlaments der Knesset beschlossen, die Mobiltelefone von bestätigten und verdächtigen COVID-19-Patientïnnen vom Inlandsgeheimdienst Schin Bet und der Polizei überwachen zu lassen. Alle Mobilfunkdaten werden seit Jahren verdeckt gesammelt, vorgeblich zu Zwecken der Terrorismusbekämpfung, und werden jetzt für die Pandemiebekämpfung verwendet (Halbfinger, Kershner und Bergman 2020). Diese Vorkehrungen dienen dem Zweck, die umfassenden Quarantänemaßnahmen durchzusetzen, sowohl gegenüber den bestätigt Infizierten wie gegenüber den der Infektion Verdächtigten sowie all denjenigen, mit denen Infizierte innerhalb der letzten 14 Tage vor deren Diagnose Kontakt hatten. Dabei werden nicht nur die Standort- und Bewegungsdaten, sondern auch Finanztransaktionsdaten zentral ausgewertet (Landau, Kubovich und Breiner 2020).

[3] Die Informationen finden sich in der FAQ unter Österreichisches Rotes Kreuz 2020b sowie in der Datenschutzerklärung, Österreichisches Rotes Kreuz 2020a.

2.2 Technikgestützte Verfahren in Deutschland und Europa

Nachfolgend sollen fünf Corona-(Contact-)Tracing-Systeme, die sich in verschiedenen Stadien der Entwicklung befinden, kurz vorgestellt werden, weil es vor allem diese Entwicklungen sind, die einen großen Einfluss auf die Situation in Deutschland haben oder haben werden: die europäischen Projekte Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) und Decentralized Privacy-Preserving Proximity Tracing (DP-3T), die Corona-Datenspende-App des Robert-Koch-Instituts (RKI) sowie ein Vorschlag von Linus Neumann für eine Kontaktdaten-App. Die EU-Kommission plant zusammen mit den Mitgliedsstaaten und dem Europäischen Datenschutzausschuss (EDSA) bis zum 15. April 2020 ein Konzept zu entwickeln, mit dem sich Coronavirus-Infektionen, unter Rückgriff auf Apps, verfolgen lassen. Außerdem haben Apple und Google am 10. April 2020 eine Kooperation zur Entwicklung einer Contact-Tracing-Plattform verkündet.

Das Projekt Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), das als gemeinnützige Organisation in der Schweiz erst noch gegründet werden soll, beabsichtigt technische Mechanismen und Standards vorzulegen, die »fully protect privacy while taking advantage of the possibilities of digital technology to maximize the speed and real-time capability of national pandemic responses« (Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) 2020). Das Projekt verspricht die Durchsetzung von Datenschutz, unter anderem durch die Anonymisierung von Daten, unter Beachtung der DSGVO sowie den Anforderungen der IT-Sicherheit. Mit einer App versehene Smartphones senden temporär gültige, »anonyme« Identifikatoren (IDs) aus, die von anderen Smartphones empfangen und gespeichert werden. Das Projekt verspricht, dass die Kontakthistorie von niemandem eingesehen werden kann, auch nicht von den Smartphone-Nutzerïnnen. Ältere Ereignisse in der Historie wären gelöscht, sobald sie epidemiologisch unwichtig werden. Wenn Nutzerinnen oder Nutzer der App als infiziert ermittelt wurden, werden sie kontaktiert, damit sie die Benachrichtigung ihrer Kontakte anstoßen können. Zugesichert wird, dass dabei die »anonymen« Kontakt-IDs aus der Kontakthistorie zum Server übermittelt werden. Apps laden sich regelmäßig Updates vom Server, dazu gehören die IDs der Kontakte von Infizierten, und ihre Nutzerïnnen erfahren darüber, dass sie mit Infizierten in Kontakt standen. Jede App, die nach diesem Standard entwickelt wird. muss sich von dem PEPP-PT-Konsortium zertifizieren lassen (Schulzki-Haddouti 2020).

Das Projekt Decentralized Privacy-Preserving Proximity Tracing (DP-3T) beabsichtigt, PEPP-PT in einer – nach eigenen Angaben – dezentralen Form technisch umzusetzen. Dennoch benötigt auch dieses System einen zentralen Server, der ausschließlich die erforderlichen Daten speichere und dem deshalb nicht vertraut werden müsse, weil »it does not maintain any secrets« (DP-3T-FAQ). In erster Linie versuchen die Entwicklerinnen und Entwickler, die Geheimhaltung der Daten zu garantieren, wobei sie »Geheimhaltung von Daten« als zentralen Anknüpfungspunkt für Datenschutzverletzungen identifizieren.[4] Dazu werden »as much sensitive data on users devices as possible« gespeichert DP-3T Project 2020b. Auf der Basis der lokal vorliegenden Daten sowie der Daten von Infizierten, d.h. deren (mathematisch zusammenhängende) IDs, die regelmäßig vom Server aktualisiert werden, wird ein Risiko-Score ermittelt, der die Wahrscheinlichkeit einer Infektion wiedergeben soll (Troncoso u. a. 2020). Darüber hinaus erlaubt die App das Übermitteln von »anonymen« Daten über alle Kontakter-

[4] Das folgt aus der Tatsache, dass alle beschriebenen Risiken so formuliert sind, dass sie nur dann eintreten können, wenn die Daten bekannt werden.

eignisse, die die Nutzerïn mit allen als infiziert bekannten Personen hatte, für Zwecke der epidemiologischen Forschung (Troncoso u. a. 2020).

Die »Corona-Datenspende«-App des Robert-Koch-Instituts (RKI) wird als Angebot beworben, die »öffentlichen Stellen bei der Bewältigung der schwersten gesellschaftlichen Krise seit 100 Jahren zu unterstützen« (Apple App Store 2020) und werden nach eigenen Angaben »ausschließlich für wissenschaftliche Zwecke verwendet« (Robert Koch-Institut 2020a). Sie dient weder den Infizierten noch den Nichtinfizierten, sondern allein dem RKI. Sie soll es dem RKI ermöglichen, Personen automatisiert überwachen zu können, die Symptome aufweisen, wie sie auch typisch für eine Infektion mit dem Corona-Virus sind, bis auf die Ebene der Postleitzahl nachzuvollziehen und die Verbreitung der Infektion auf der Webseite des RKI tagesaktuell als Karte visuell darzustellen. Die Nutzung der App setzt die Erstellung eines Pseudonyms der Nutzerïn voraus. Die weitere Datenerhebung erfolgt zum Teil durch manuelle Eingabe, zum anderen Teil durch Sensoren wie Wearables oder Fitnesstrackern, die am Körper getragen werden und mit der App verbunden sind. Eine Teilmenge der sensorischen Daten werden anonymisiert, indem beispielsweise das Gewicht auf eine Gewichtsklasse abgebildet wird.

Der Vorschlag von Linus Neumann für eine Kontaktdaten-App (Neumann 2020) knüpft an Einreichungen zum Hackathon »Wir vs. Virus« an und verfolgt ausschließlich das Ziel, eine Person, bei der eine Infektion festgestellt wird, in die Lage zu versetzen, ihre Kontakte der letzten 14 Tage darüber zu informieren. Neumann erklärt, dass sämtliche Daten ausschließlich »dezentral« und »anonym« vorgehalten werden sollen. Dazu werden lokal in kurzen Abständen anonyme IDs erzeugt, die über Bluetooth Low Energy Beacon vom Smartphone ausgesandt werden, die dann von anderen Smartphones empfangen werden können und, wenn der Abstand gering genug ist, diese speichert. Im Falle einer Infektion sendet das Smartphone die eigenen anonymen IDs an einen zentralen Server, der diese dann für den Abruf durch andere Smartphones bereithält, die dann lokal feststellen können, ob sie mit Infizierten Kontakt hatten.

Das Contact-Tracing-System-Kooperationsprojekt von Apple und Google (Google, Inc. 2020) hat große Ähnlichkeiten mit DP-3T, ist auch dezentral aufgebaut, und es werden nur die eigenen temporären IDs an den Server übertragen, falls eine Infektion diagnostiziert wurde. Es ist geplant, in zwei Stufen erst eine API und dann eine umfassende, in die eigenen Betriebssysteme jeweils eingebaute, Bluetooth-basierte Contact-Tracing-Plattform zu entwickeln. Über die API ist es möglich, die eigenen temporären IDs, die im Infektionsfall etwa vom Gesundheitsamt signiert sein können, zum Server hochzuladen bzw. die vom Server heruntergeladenen mit den selbst gesehenen IDs abzugleichen, um das Risiko einer Exposition zu bestimmen. Es soll nicht möglich sein, die selbst gesehenen temporären IDs zu extrahieren.

2.3 Akteure und Akteurskonstellationen

Der gesellschaftliche Kontext, in dem die hier adressierten Datenverarbeitungsverfahren durchgeführt werden, ist von einer großen Zahl von Akteurïnnen geprägt, die vor dem Hintergrund der Verhältnisse, in denen sie zueinander stehen, und der strategischen und taktischen Interessen, die sie verfolgen, in verschiedener Weise Einfluss auf die Verarbeitung nehmen können und nehmen.

Die EU-Kommission versucht derzeit, die Kontrolle über die Bedingungen für Gestaltung und Einsatz von Datenverarbeitungsverfahren zu verschiedenen Zwecken im Bereich der Corona-Pandemie-Bekämpfung an sich zu ziehen. Sie hat dazu am 9. April

2020 Empfehlungen für »a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data« (European Commission 2020) vorgelegt, denen am 15. April 2020 ein »pan-European approach for COVID-19 mobile applications« sowie »Commission guidance on privacy and data protection« folgen sollen.

Bundes- und Landesregierungen und -parlamente können ihre eigenen und die partikularen Interessen einzelner Akteure als allgemeine Interessen setzen und als bindendes Recht setzen. Die Bundesregierung fährt nach derzeitigem Stand mehrgleisig: Gesundheitsminister Jens Spahn (CDU) wollte noch vor kurzem das Infektionsschutzgesetz novellieren, um die Gesundheitsbehörden zu ermächtigen, die möglichen Kontakte mit Infizierten mithilfe von Mobilfunkdaten, die TK-Anbieter den Behörden zur Verfügung stellen sollten, zu ermitteln. Nach großer öffentlicher Kritik wurde der Versuch abgebrochen, wenn auch nicht aufgegeben (Rudl 2020). Inzwischen unterstützt die Bundesregierung massiv die »Corona-Datenspende«-App des RKI.

Die größte und differenzierteste Gruppe von Akteuren stellen die von der Datenverarbeitung Betroffenen dar. Im Hinblick auf in dieser DSFA betrachtete die Datenverarbeitung und ihre Auswirkungen sind folgende Betroffenengruppen aus grundrechtlicher Perspektive besonders zu betrachten:

- infizierte Betroffene,
- nicht infizierte Betroffene,
- Betroffene, die einem faktischen Zwang zur Nutzung einer entsprechenden App ausgesetzt sind, etwa über ihre Arbeitgeber oder aufgrund von Gruppendruck,
- Betroffene, die kein oder kein kompatibles Smartphone besitzen. Hierbei handelt es sich typischerweise um Kinder, um geistig Behinderte sowie tendenziell um Personen in höherem Lebensalter;
- Dritte, die ein unmittelbares Interesse an der Identifikation Infizierter sowie an integren Prognosen bzgl. der Ausbreitung des Corona-Virus haben.

Verantwortliche ist eine Rolle im Anwendungsbereich der DSGVO. Verantwortlicher ist, wer »allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet« (Art. 4 Nr. 7 DSGVO).

Unter den Akteurïnnen im technischen Feld befinden sich Herstellerïnnen, Betreiberïnnen und Dienstleisterïnnen unterschiedlicher Art. Diese können im Sinne der DSGVO als Verantwortliche, Auftragsdatenverarbeiterïnnen oder Dritte auftreten.

Herstellerïn können formale Organisationen, d.h. juristische Person oder Behörde, oder Personengruppen sein, die jeweils Mitglieder haben, die direkt an der Entwicklung mitarbeiten, vor allem als Entwicklerïnnen.

Betreiberïn des oder der Server sind grundsätzlich formale Organisationen.

Dienstleisterïn treten an unterschiedlichen Stellen auf, sei es als Betreiberïn der Rechenzentren, in denen die Server stehen, bzw. der Clouds, auf denen der Server als Dienst läuft, als Internet-Service-Provider, die für den Datentransport zu den Servern und zwischen ihnen sorgen, sowie Mobilfunk-Provider, die für den Datentransport zu den Smartphones sorgen. Daneben gibt es Dienstleisterïn, die grundlegende Systemfunktionen bereitstellen, darunter die Herstellerïnnen der Smartphones sowie der Smartphone-Betriebssysteme, vor allem Google, Apple und Microsoft, die zugleich

auch die zentralen App-Stores betreiben, die Anbieterïnnen von verbreiteten Frameworks oder von Integrationstools, die auch von staatlichen Stellen eingesetzt werden, wie Palantir (Lewis, Conn und Pegg 2020). Mobilfunk-Provider wie die Deutsche Telekom haben freiwillig und ohne gesetzliche Verpflichtung Mobilfunkmetadaten ihrer Nutzerïnnen »anonymisiert« und an das RKI übermittelt.

Sicherheits- und Ordnungsbehörden, insbesondere Polizeien, verfügen über umfassende Befugnisse sowohl zur Durchsetzung der zur Pandemieeindämmung getroffenen Maßnahmen, einschließlich der Ausgangsbeschränkungen, wie auch zum Zugriff auf bei staatlichen und privaten Akteurïnnen vorhandene Daten, personenbezogene wie anonyme, sowie informationstechnische Systeme. Darüber hinaus werden diesen Behörden solche Daten auch übermittelt, selbst nachdem zuständige Datenschutzaufsichtsbehörden die Rechtswidrigkeit der Übermittlung festgestellt und deren Einstellung angeordnet hat (Laufer 2020).

Datenschutzaufsichtsbehörden sind unabhängige Behörden für die Überwachung der Anwendung der DSGVO, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden. Ihre primäre Aufgabe besteht in der Überwachung und Durchsetzung der Anwendung der DSGVO. Zur Erfüllung ihrer Aufgaben verfügt sie über die notwendigen Befugnisse, etwa zur Durchführung von Untersuchungen in Form von Datenschutzüberprüfungen oder zur Verhängung von Verarbeitungsbeschränkungen und -verboten sowie Geldbußen.

Gesundheitsbehörden, Polizeien im materiellen Sinne, die dem Bunde oder den Ländern unterstehen, haben vor allem im Anwendungsbereich des Infektionsschutzgesetzes (IfSG) umfassende Befugnisse mit weitgehenden Eingriffsrechten in Grundrechte.

Das Robert-Koch-Institut (RKI) ist eine selbstständige deutsche Bundesoberbehörde unter anderem für Infektionskrankheiten, die direkt dem Bundesministerium für Gesundheit unterstellt ist. Im Gegenstandsbereich der vorliegenden DSFA besteht seine Aufgabe in der Erkennung, Verhütung und Bekämpfung der Corona-Pandemie, damit zusammenhängen epidemiologischen Untersuchungen und der Berichterstattung gegenüber der Bundesregierung und der Öffentlichkeit.

Öffentliche und private Krankenkassen sowie Versicherungen erheben, speichern, verarbeiten und verwenden große Mengen personenbezogene Daten, darunter besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, von Versicherten und ihren Angehörigen. Es gibt eine große Zahl gesetzlicher Regelungen, die Kassen und Versicherungen zur Übermittlung von personenbezogenen, aber auch von anonymisierten Daten verpflichten.

Gesundheitseinrichtungen, Krankenhäuser, Ärztïnnen und Apotheken erheben, speichern, verarbeiten und verwenden große Mengen personenbezogene Daten, darunter besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, von Patientïnnen. Es gibt eine große Zahl gesetzlicher Regelungen, die diese Stellen zur Übermittlung von personenbezogenen, aber auch von anonymisierten Daten verpflichten, darunter nach dem IfSG Daten über Infizierte und Infektionen an Gesundheitsbehörden.

Pflegeeinrichtungen erheben, speichern, verarbeiten und verwenden nicht nur große Mengen personenbezogene Daten, darunter besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, von Pflegebedürftigen und ihren Angehörigen, sie üben in der stationären Pflege auch ein großes Maß an Kontrolle über den Tagesablauf von zu pflegenden Personen aus. Das gilt, wenn auch in geringerem Maße, auch für die ambulante Pflege. Auch sie sind gesetzlich zu einer Vielzahl von Übermittlungen von personenbezogenen, aber auch von anonymisierten Daten verpflichtet.

Öffentliche Forschungseinrichtungen unterstehen, von Ausnahmen abgesehen, der

Hoheit der Länder, erfüllen die ihnen nach einschlägigen Bundes- und Landesgesetzen übertragenen Aufgaben und sichern die Freiheit der Forschung ihrer Mitglieder. In den letzten Jahrzehnten sind die öffentlichen Forschungseinrichtungen, nicht zuletzt aufgrund von Mittelkürzungen bzw. die von den Einrichtungen zu verkraftenden Kostensteigerungen nicht umfassend tragenden Mittelerhöhungen, zunehmend auf die Einwerbung von Drittmitteln bei öffentlichen und privaten Mittelgebern angewiesen, einschließlich Auftragsforschung. Private Forschungseinrichtungen müssen über die einzelnen Forschungsprojekte hinaus auch ihre Institutionskosten über eigene oder Drittmittel tragen. Alle Forschungseinrichtungen stehen unter zunehmendem Evaluations- und Bewertungsdruck einerseits und Zeitdruck im Hinblick auf Veröffentlichungen andererseits, gleiches gilt für ihre Mitglieder. Darüber hinaus stehen die Einrichtungen grundsätzlich in Konkurrenz zueinander um Personal und Geld.

Betreiberïnnen kommerzieller Bluetooth-Trackinginfrastrukturen, zum Beispiel in Geschäftsräumen, Malls oder an Werbetafeln im Straßenland, tracken Geräte, die über Bluetooth erreichbar sind, und deren Adressdaten, um an die Geräte personalisierte Werbung auszuspielen.

Arbeitgeberïnnen, Vermieterïnnen und andere Stellen, die Hausrechte innehaben, kontrollieren Zugang zu und Nutzung von Einrichtungen, Gebäuden, Objekten oder Flächen, seien es der Arbeitsplatz, das Mietobjekt, Geschäftsräume, öffentliche Verkehrsmittel oder Kultureinrichtungen. Sie können den Zugang und die Nutzung ermöglichen oder erzwingen, erschweren oder verhindern.

2.4 Interessen und Interessenkonstellationen

Die unterschiedlichen Akteurïnnen im Kontext des betrachteten Verfahrens verfolgen je eigene, jeweils überlappende oder disjunkte, gemeinsame oder konträre, strategische oder taktische Interessen, die das Verfahren positiv oder negativ beeinflussen können, die selbst wieder vom Verfahren positiv oder negativ beeinflusst werden, und die Akteurïnnen als Angreiferïnnen im Verständnis des Datenschutzes plausibilisieren oder eher unwahrscheinlich machen können.

Das Hauptinteresse der Betroffenen, die die App nutzen, besteht darin, dass ihnen die App ermöglichen soll festzustellen, ob sie mit Infizierten (länger und näher) in Kontakt gekommen sind und damit ein, einen angemessenen Schwellwert überschreitendes, Risiko besteht, dass sie sich selbst infiziert haben. Darüber hinaus besteht aus Sicht der Betroffenen ein Interesse, dass die App es ihnen ermöglicht, gegenüber Dritten nachzuweisen, dass sie einem hohen Risiko ausgesetzt waren und daher möglicherweise infiziert sind, um medizinisch auf eine Corona-Infektion getestet zu werden. Gleichzeitig besteht ein Interesse der Betroffenen, zur Verhinderung möglicher Diskriminierungen und Stigmatisierungen erfolgreich abstreiten zu können, dass sie einem hohen Risiko ausgesetzt waren, etwa wenn die Diskriminierungen und Stigmatisierungen ausschließlich aufgrund des Risikos, dem die Betroffenen ausgesetzt waren, und nicht auf der Basis einer medizinischen Diagnose stattfinden. Auch haben die Betroffenen ein Interesse, dass ihnen die Verarbeitungstätigkeit und/oder die App ermöglicht nachzuweisen, dass sie infiziert waren, jedoch nicht mehr infiziert – und damit (wahrscheinlich) immun – sind.

Da von der Verarbeitung der Daten auch Personen betroffen sind, die die App nicht nutzen wollen oder nicht nutzen können, etwa weil sie kein oder kein kompatibles Smartphone besitzen, haben diese Personen ein Interesse, dass das Verfahren so gestaltet ist, dass es soweit als möglich auch ohne die Verwendung einer App auskommt

und dabei gleiche oder vergleichbare Funktionalität bietet.

Das Hauptinteresse der staatlichen Stellen, darunter der Europäischen Kommission, von Bundes- und Landesregierungen sowie Sicherheits- und Gesundheitsbehörden, besteht darin, die Corona-Pandemie zu stoppen bzw. zumindest zu kontrollieren und zu steuern. Darüber hinaus haben diese Stellen ein Interesse, die Ausbreitung der Pandemie nachvollziehen zu können, um auf dieser Basis Vorhersagen über die weitere Ausbreitung treffen und entsprechend angemessene Maßnahmen treffen zu können. Ein drittes Interesse der staatlichen Stellen liegt in der Ersetzung von allgemeinen Ausgangsbeschränkungen durch zielgruppen- und risikospezifische Regelungen, für die es notwendig ist festzustellen, wer (wahrscheinlich) infiziert ist, etwa weil sie mit Infizierten (länger und näher) in Kontakt gekommen sind, ggfls. auch, diese Personen über ihre Exposition zu informieren. Darüber hinaus besteht auf Seiten des Staates das Interesse, die Einhaltung der Maßnahmen überprüfen und sicherstellen zu können, seien es Ausgangsbeschränkungen, Kontaktverbote oder Quarantäneauflagen. Und nicht zuletzt gibt es das sich in öffentlichen Verlautbarungen politischer Entscheidungsträgerïnnen, in Gesetzesverschärfungen, zuletzt auch in Verstößen gegen Übermittlungsuntersagungsanordnungen (Krempl 2020) deutlich zeigende Interesse des Staates an einem Ausbau von Überwachungsinfrastrukturen, einschließlich der dafür notwendigen gesetzlichen Grundlagen, auch für zukünftige, noch nicht festgelegte Zwecke, einer Verstetigung existierender Überwachungsmaßnahmen sowie ihrer zunehmenden Ausdehnung auf immer weitere Zwecke. Das mangelnde Interesse des Staates an einem effektiven Grundrechtsschutz zeigt sich nicht zuletzt darin, dass weder die EU-Kommission oder die Bundes- oder Landesregierungen noch die Europäische, die Bundes- oder die Landesgesetzgeberïnnen im Zusammenhang mit dem Erlassen von Rechtsgrundlagen für die Verarbeitung personenbezogener Daten jemals eine DSFA nach Art. 35 Abs. 10 DSGVO durchgeführt haben, obwohl die DSGVO bereits vor vier Jahren verabschiedet wurde. Dies unterblieb selbst in den Fällen, in denen ganz offensichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bestand.

Datenschutzaufsichtsbehörden leiden notorisch an Ressourcenmangel, sowohl personell als auch bei den sachlichen Ressourcen als auch in Bezug auf insbesondere technische Kompetenzen ihrer Mitarbeiterïnnen. Sie haben insofern ein Interesse an effizienten Prüfverfahren. Bei einem hohen Risiko einer Verarbeitung erwarten Sie deshalb das Vorliegen einer substantiell-aussagekräftigen DSFA, in denen alle aus der DSGVO heraus bestimmten, relevanten Anforderungen methodisch nachvollziehbar versammelt und sowohl funktional als auch normativ prüffähig vorgelegt und beurteilt werden können.

Die öffentliche wie private Forschung verfolgt das Interesse, die Ausbreitung der Corona-Pandemie nachvollziehen zu können, um Vorhersagen über die weitere Ausbreitung treffen zu können, aber auch für allgemeine Erkenntnisse über Pandemien, die Wirkung staatlicher Maßnahmen auf deren Ausbreitung und Eindämmung, das Verhalten von Personen in solchen Pandemien, einschließlich ihrer Bewegungen, und weitere Phänomene in diesem Bereich.

Herstellerïnnen der Corona-App – oder generell: von weiteren Corona-Apps, insbesondere wenn diese als Open-Source-Software veröffentlicht werden – haben ein Interesse am Verkauf der App oder an der Nutzung der App, wobei zusätzliche »Komfortfunktionen« und Funktionen mit anderen Zwecke, unter Umständen auf der Grundlage einer zusätzlichen Einwilligung, angeboten werden, die den Datenschutz der Nutzenden unterlaufen könnten.

Betreiberïnnen und Dienstleisterïnnen haben als ökonomische Akteure ein Interesse, ihre Dienste zu möglichst geringen Kosten für einen möglichst hohen Preis anbieten zu

können. Soweit sie begründet damit rechnen können, von den Aufsichtsbehörden nicht oder nicht umfassend geprüft zu werden, haben sie ein Interesse, besonders an den nicht prüfbaren oder praktisch nicht oder selten geprüften Teilen ihrer Dienstleistung zu sparen. Anstelle von Maßnahmen, die einer möglichen Weiter- oder Zweitverwendung von Systemen und personenbezogenen Daten im Wege stehen, werden sie sich eher auf Maßnahmen konzentrieren, die primär der Sicherung der Verarbeitung dienen, die sich aber gegenüber Außenstehenden als Datenschutzmaßnahmen verkaufen lassen, etwa Datenschutzerklärungen oder die Sicherheitsmaßnahmen nach Art. 32 DSGVO. Betreiberïnnen und Dienstleisterïnnen haben ein Interesse an einer vom Staat durchgesetzten Verstetigung der Verarbeitungstätigkeiten, weil sie in diesem Fall begründet damit rechnen können, dass sie als diejenigen, die ihre Dienstleistung schon in der Phase erbracht haben, die als befristet geplant war, auch zum Weiterbetrieb ausgewählt werden, wenn die Verarbeitungstätigkeiten auf Dauer gestellt werden.[5] Dazu gehören insbesondere Dienstleisterïnnen, die grundlegende Systemkomponenten oder -funktionen oder verbreitete Schnittstellen zu anderen entweder vom Staat oder von Privaten genutzten Systemen oder Plattformen betreiben, kontrollieren und bereitstellen, wie etwa Google, Apple, Facebook, Amazon oder Microsoft, aber auch Herstellerïnnen oder Betreiberïnnen von Drittsystemen, die auf solchen Systemen aufsetzen, solche Schnittstellen nutzen oder die in der Verarbeitungstätigkeit verarbeiteten personenbezogenen Daten weiterverarbeiten wollen, wie etwa Palantir.

Arbeitgeberïnnen, Vermieterïnnen und Inhaberïnnen von Hausrechten haben ein Interesse, an der Verarbeitungstätigkeit als Empfängerïnnen beteiligt zu sein, um auf der Basis der dabei erlangten Informationen über den Zugang oder Nichtzugang zu Gebäuden, Geschäftsräumen oder anderen Einrichtungen entscheiden zu können, sei es aus Gründen einer möglichst umfassenden Minimierung von Infektionsrisiken für Mitarbeiterïnnen, Kundïnnen oder Gäste, sei es aus Gründen der Personalverwaltung, -kontrolle und -steuerung, um damit Risiken auf die Betroffenen zu externalisieren.

Dritte, seien es Individuen, Gruppen oder staatliche oder private Organisationen, haben eine Vielzahl unterschiedlicher Interessen. Für die hier untersuchte Verarbeitungstätigkeit sind insbesondere die folgenden Interessen relevant:

- das Interesse an der Aufdeckung der Identität von Infizierten, ob aus persönlichen, ökonomischen oder staatlichen Gründen,
- das Interesse an nicht-validen Daten in Bezug auf die Ausbreitung der Pandemie, sei es zu hohe oder zu niedrige Fallzahlen zu erzeugen,
- das Interesse an einer Störung der Verarbeitungstätigkeit, ob aus Freude am »Hacken«, aus Freude an der Zerstörung oder mit dem Ziel der Unterminierung von Vertrauen in die Fähigkeit des Staates oder der Verantwortlichen, eine solche Verarbeitungstätigkeit erfolgreich, sicher und datenschutzkonform betreiben zu können,
- das Interesse, bestimmte Eigenschaften der Verarbeitungstätigkeit, etwa das für die stetige Aussendung von TempIDs notwendige dauerhafte Einschalten von Bluetooth, den Upload von Gesundheits-TempIDs oder den Download von infektionsanzeigenden Daten ohne Personenbezug (iDoP), für eigene Zwecke auszunutzen, etwa zum Angriff auf die Smartphones mit eingeschaltetem Bluetooth oder auf beteiligte Server.

[5] Vgl. die von Apple und Google am 10. April 2020 verkündete Kooperation (Google, Inc. 2020).

Kapitel 3

Use Cases

Der Gestaltung des Datenverarbeitungsverfahrens, in der die Corona-App eingebunden ist, liegen grundsätzlich verschiedene Annahmen über typische Gebrauchsweisen der App durch die Nutzerïnnen und des Gesamtsystems durch die Betreiberïnnen zugrunde. Im Folgenden rekonstruieren wir diese Annahmen als Use Cases. Ihre Aufschlüsselung hilft, die leitenden Vorstellungen hinter verschiedenen Gestaltungsmerkmalen sowohl der App als auch des Servers und der Verarbeitungstätigkeit insgesamt nachvollziehen und überprüfen zu können.

3.1 Das Verfahren

(1.1) Das Verfahren, in das die App eingebettet ist, erlaubt und ermöglicht Interventionen im Fehlerfall.

(1.2) Das Verfahren ermöglicht die Widerrufung von invaliden, fehlerhaften oder fälschlich übertragenen Gesundheits-TempIDs bzw. den entsprechenden infektionsanzeigenden Daten ohne Personenbezug (iDoP), etwa wenn sich die Diagnose der Infektion als inkorrekt herausstellt.

3.2 Rechtsgrundlagen / Rechtstreue

(2.1) Es gibt gültige, verfassungskonforme und grundrechtsschonende Rechtsgrundlagen für die Verarbeitungstätigkeit gem. der Definition in Art. 4 Abs. 2 DSGVO, die zudem die Verantwortlichkeit und Zuständigkeiten regeln.

(2.2) Es gibt entsprechende Rechtsgrundlagen für die Herstellung, die Bereitstellung und den Betrieb des oder der Server, mit denen die Apps kommunizieren, und die zum Empfang von Gesundheits-TempIDs von infizierten Personen, zu deren Anonymisierung und zur Verteilung der infektionsanzeigenden Daten ohne Personenbezug (iDoP) dienen.

(2.3) Es gibt entsprechende Rechtsgrundlagen für die Herstellung, die Bereitstellung und die Wartung der App.

(2.4) Die Betroffenenrechte (Art. 12 bis 22 DSGVO) werden berücksichtigt.

(2.5) Die Verantwortliche und die Auftragsdatenverarbeiterïnnen im Sinne der DSGVO verhalten sich jederzeit rechtstreu.

(2.6) Die Verantwortliche, die Zuständigen und die Auftragsdatenverarbeiterïnnen stellen die Rechtstreue ihrer Mitarbeiterïnnen sicher.

3.3 Betrieb der Technik

(3.1) Der oder die Server – sowie die von diesen genutzten technischen Infrastrukturen – werden auf dem Stand der Technik sicher (vertraulich, integer und verfügbar) und datenschutzkonform (transparent, nichtverkettbar und intervenierbar) aufgesetzt und betrieben.

(3.2) Die App wird mit Methoden auf dem »Stand der Technik« entwickelt und sicher (vertraulich, integer und verfügbar) und datenschutzkonform (transparent, nichtverkettbar und intervenierbar) implementiert.

(3.3) Der oder die Server sind jederzeit verfügbar.

3.4 Smartphone

(4.1) Die Person besitzt ein Smartphone. Sie lädt die App aus einer sicherer Quelle herunter, etwa der Webseite des Betreibers oder dem App-Store des Betriebssystemherstellers ihres Smartphones, und installiert die App nach den Vorgaben der Installationsanleitung. Nach der Installation ist die App funktionsfähig.

(4.2) Die Person trägt das Smartphone zu jeder Zeit bei sich, wenn sie sich in der Nähe anderer Personen befindet. Dies gilt auch innerhalb des familiären Umfelds.

3.5 App

(5.1) Die App sendet regelmäßig, etwa alle 5, 15 oder 30 Minuten, wechselnde IDs (»TempIDs«) per Bluetooth Low Energy Beacon aus (»TempID-Token«) und empfängt die TempIDs anderer Smartphone-Apps aus der Umgebung. Der Gültigkeitszeitraum der TempIDs wird von der Herstellerïn nach Maßgabe der datenschutzrechtlich Verantwortlichen vorgegeben. Die Messung ergibt ausschließlich valide Daten, die korrekt in der App gespeichert werden.

(5.2) Die App kontaktiert regelmäßig den oder die Server und lädt Updates mit den infektionsanzeigenden Daten ohne Personenbezug (iDoP) herunter. Diese Daten werden durch Anonymisierung von Gesundheits-TempIDs, die von als infiziert diagnostizierten Personen an den oder die Server übermittelt wurden, auf dem Server erzeugt. Die heruntergeladenen Daten sind korrekt und valide, sie werden fehlerfrei übertragen und korrekt in der App gespeichert. Die Kommunikation mit dem oder den Servern ist vertraulich und abstreitbar gegenüber Dritten. Die Kommunikation mit dem oder den Servern ist nicht verkettbar mit anderen Kommunikationen mit dem oder den Servern.

(5.3) Die App bestimmt auf der Basis lokaler Berechnungen unter Verwendung der in der App gespeicherten Kontaktdaten, das heißt aufgrund von Kontaktereignissen gespeicherte fremde TempIDs, der Zeitdauer und des Signalstärkenprofils, sowie der vom Server oder von den Servern empfangenen infektionsanzeigenden Daten ohne Personenbezug (iDoP), ob es zu einer Exposition gekommen ist. Das Berechnungsverfahren, nach dem auf der Basis von Kontaktereignissen die Exposition berechnet wird, wird nach Vorgaben der zuständigen Gesundheitsbehörden durchgeführt und produziert valide Expositionsrisiken. Das Berechnungsverfahren ist transparent und öffentlich, und in der App fehlerfrei implementiert.

(5.4) Den Warnmeldungen können weitere Informationen, etwa über weitere Informationsquellen, oder Handlungsanweisungen beigegeben werden. Die Handlungsanweisungen sind per Gesetz bestimmt, öffentlich und transparent, und korrekt in der App implementiert.

(5.5) Die von der App erzeugten TempIDs werden nach Ablauf der von den Gesundheitsbehörden vorgegeben Fristen in der App gelöscht.

(5.6) Die in der App gespeicherten fremden TempIDs von Kontaktereignissen werden nach Ablauf der von den Gesundheitsbehörden vorgegeben Fristen in der App gelöscht.

(5.7) Die widerrufenen infektionsanzeigenden Daten ohne Personenbezug (iDoP) werden in der App sofort nach dem Update gelöscht.

(5.8) Sobald ein positiver Match errechnet wurde, und somit der Zweck der App erfüllt wurde, werden alle TempIDs bzw. die TempID-History in der App gelöscht. Es wird ein Hinweis gegeben, dass die App deinstalliert werden kann.

(5.9) Die Übertragung der Gesundheits-TempIDs von App auf den oder die Server werden in der App integer protokolliert. Das Übertragungsprotokoll ist sowohl nachweisbar wie abstreitbar gegenüber Dritten.

(5.10) Die TempIDs, die in der App verwendet werden, werden nach einem dem Stand der Technik entsprechenden Verfahren so generiert, dass sie weltweit eindeutig sind.

(5.10) Die App ist jederzeit bei der Herstellerïn, Verantwortlichen und in den App-Stores zum Herunterladen verfügbar.

(5.11) Die App ist nach der Installation auf dem Smartphone jederzeit verfügbar.

(5.12) Die TempIDs sind jederzeit verfügbar, sowohl in der App wie auf dem oder den Servern.

3.6 Person

(6.1) Wenn bei der Person eine CV-Infektion diagnostiziert wurde, übermittelt sie unter Verwendung der App die TempIDs, die die App innerhalb der letzten Tage erzeugt und ausgesendet hat, als Gesundheits-TempIDs an den oder die Server. Die Anzahl der Tage vor dem Zeitpunkt der Diagnose, für die die Gesundheits-TempIDs ausgesendet werden, bestimmt die Herstellerïn nach Vorgaben der zuständigen Gesundheitsbehörden. Die Vorgabe der Anzahl der Tage ist öffentlich und transparent, und sie ist korrekt in der App implementiert. Die Übermittlung der Gesundheits-TempIDs an den Server muss aktiv von der Person ausgelöst werden.

(6.2) Nach einer Infektion begibt sich die betroffene Person in (Heim-)Quarantäne und deaktiviert die App, um False Negatives zu verhindern.

(6.3) Solange bei einer Person keine Infektion diagnostiziert wurde, übermittelt weder sie noch die App Daten an den oder die Server.

(6.4) Wenn das Expositionsrisiko einen oder mehrere vorgegebene Schwellwerte überschreitet, werden der Nutzerïn jeweils Warnmeldungen zur Exposition angezeigt. Der oder die Schwellwerte werden von den Gesundheitsbehörden vorgegeben. Die Nutzerïn kann unter Umständen auch zusätzlich einen weiteren, eigenen Schwellwert angeben. Die vorgegeben Schwellwerte sind transparent und öffentlich. Alle Schwellwerte sind in der App korrekt hinterlegt.

(6.5) Die App erlaubt es der Nutzerïn, eine eigene Exposition, die eine Infektion nicht indiziert, gegenüber Dritten wirksam abstreiten zu können, etwa um damit das Risiko von Diskriminierungen oder Stigmatisierungen verringern zu können.

Kapitel 4

Beschreibung der Verarbeitungstätigkeit

Die Beschreibung einer Verarbeitungstätigkeit zur Durchführung einer DSFA muss die Verantwortliche erstellen. Da bislang nur Entwürfe für eine Verarbeitung mit Hilfe einer Tracing-App vorliegen und angesichts der bislang unklaren politischen und rechtlichen Situation, ist nicht damit zu rechnen, dass eine hinreichend belastbare Beschreibung der Verarbeitungstätigkeit von der verantwortlichen Stelle vorgelegt wird. Dieses Dokument bezieht sich deshalb auf eine spezifizierte Verarbeitung, die sich prinzipiell an den Entwürfen von DP-3T und Linus Neumann orientiert, und im Kapitel 3 »Use Cases« unter Ausweis rechtlicher und funktionaler Annahmen hochauflösend dargestellt ist.

Eine Beschreibung der Verarbeitung muss Aussagen darüber treffen, welche funktionalen, sicherheitstechnischen und datenschutzfreundlichen Eigenschaften angestrebt werden oder was bereits umgesetzt wurde; also bspw. welche konkreten Schutzmaßnahmen im Detail geplant oder umgesetzt wurden. Das ist in diesem, auf Entwürfen basierenden Falle nicht in hinreichender Weise möglich. Stattdessen können hier nur die zu treffenden Schutzmaßnahmen benannt werden. In den tieferliegenden technischen Beschreibungsschichten werden vielfach weitere, technisch detailliertere Möglichkeiten diskutiert.

Die Verantwortliche ist gemäß Art. 35 DSGVO verpflichtet, die Wirksamkeit ihrer Maßnahmen vor Inbetriebnahme der Verarbeitung nachzuweisen. Die Verarbeitung der Daten muss dabei dauerhaft überprüfbar sein (vgl. Art. 32 Abs. 1 lit. d DSGVO). Daraus folgt, dass für den Betrieb ein Datenschutzmanagement (DSM) vorhanden sein muss, mit dem die Anforderungen der DSGVO nicht nur kontrolliert, geprüft und beurteilt, sondern auch in den beteiligten Organisationen wirksam durchgesetzt werden. Die Prüfbarkeit einer Verarbeitung ist keine passive Eigenschaft, sondern muss während der Gestaltungsphase der Verarbeitungstätigkeit aktiv hergestellt werden (Seidel 1984, S. 191). Eine wesentliche Voraussetzung zur Umsetzung der Prüfbarkeit der mit Bezug zur Verarbeitung beteiligten Tätigkeiten von Personen und Aktivitäten von IT-Systemen ist deren Protokollierung. Im diesem Falle einer Verarbeitung mit hohem Risiko (vgl. Kapitel 6) ist eine revisionsfeste, d.h. integre, Protokollierung nötig, insbesondere an den Stellen der Verarbeitung, an denen Personenbezug besteht bzw. der Personenbezug aufgehoben werden soll. Das bedeutet, dass mindestens die folgenden Aspekte Bestandteile einer Beschreibung der Verarbeitungstätigkeit sein müssen:

1. Art, Umfang und Umstände der Verarbeitungstätigkeit (vgl. Kapitel 4.1).
2. Allgemeinverständliche Beschreibung des Zwecks und der Funktionalität der Verarbeitungstätigkeit, mit der dieser Zweck erreicht werden soll (vgl. Kapitel 4.2).
3. Beschreibung der Annahmen, warum der Zweck legitim ist (vgl. Kapitel 4.3).
4. Beschreibung von absehbaren »benachbarten« Zwecken (vgl. Kapitel 4.4).

5. Ausweis der dabei verwendeten Kategorien personenbezogener Daten (vgl. Kapitel 4.5).
6. Analyse der einzelnen Verarbeitungstätigkeiten (vgl. Kapitel 4.6).
7. Benennung der Maßnahmen, mit denen speziell die Bindung des Zwecks sichergestellt und überprüfbar gemacht wird (vgl. Kapitel 4.7).
8. Benennung von Schutzmaßnahmen, die insbes. gemäß Art. 5 DSGVO (Grundsätze), Art. 25 (Datenschutz by Design) und Art. 32 DSGVO (Sicherheit) gefordert sind (vgl. Kapitel 4.8).
9. Benennung weiterer Anforderungen der DSGVO (wie Rechtsgrundlage, Datenschutzbeauftragter, Datenschutzmanagement) (vgl. Kapitel 4.9).
10. Benennung der Verantwortlichen (vgl. Kapitel 4.10).

Nachfolgend werden diese Aspekte behandelt.

4.1 Art, Umfang und Umstände

Diese Art der Datenverarbeitung ist zumindest in der Hinsicht neu, als dass ein epidemiologisches Problem durch ein Verfahren gelöst werden soll, welches auf einen breiten Einsatz vernetzter informationstechnischer Systeme, der Kooperation vieler Personen und der Verwendung von Daten mit hohem Schutzbedarf (medizinische Daten) angewiesen ist. Zwar sind die einzelnen technischen Komponenten, die für die Unterstützung des Verfahrens geplant sind, an und für sich Stand der Technik, jedoch in ihrer Kombination neuartig und es liegen keine Erfahrungen bezüglicher ihrer Nutzung vor.

Die Datenverarbeitung ist in jedem Fall umfangreich, da in ihr personenbezogene Informationen einer sehr großen Anzahl von Personen in der Größenordnung ganzer Staaten, Kontinente oder gar des ganzen Planeten verarbeitet werden.

Die Umstände dieser Datenverarbeitung sind, wenn nicht einzigartig in ihrem Auftreten, so doch außergewöhnlich. Im Regelfall existieren zu den meisten Datenverarbeitungstätigkeiten Vorgänger und Variationen, die in anderen Organisationen eingeführt, betrieben und wieder außer Betrieb genommen worden. Dies ist hier nicht der Fall.

4.2 Zweck der Verarbeitung

Der übergeordnete Zweck der Verarbeitung personenbezogener Daten ist die Steuerung bzw. Eindämmung der globalen Corona-Pandemie, woraus das Auffinden und Unterbrechen von Infektionsketten abgeleitet wird. Dieser Zweck beinhaltet konkret das schnelle Informieren potentiell infizierter Personen. Um diesen Zweck zu erreichen, soll Betroffenen ein verlässlicher Indikator zur Verfügung gestellt werden, wenn sie zuvor mit SARS-CoV-2-Infizierten epidemiologisch relevant in Berührung gekommen sind. Daraufhin sollen sich die Gewarnten in Heimquarantäne begeben und so die Infektionskette unterbrechen. Die Inkubationszeit von COVID-19 beträgt bis zu zwei Wochen und infizierte Personen sind schon infektiös, bevor sich möglicherweise Krankheitssymptome zeigen. Dadurch ist die Aufzeichnung einer Kontakthistorie notwendig, um rückwirkend die Kontakte zu identifizieren. Die Dauer der Kontakthistorie wird als Parameter durch die Gesundheitsbehörden vorgegeben.

Das Verfahren umfasst folgende Verarbeitungstätigkeiten:

a) App-seitige Verarbeitung von Kontaktereignissen

Im besten Falle wird auf allen Smartphones von Bürgerïnnen eine App installiert (Corona-App, CA), die in regelmäßigen Abständen mittels Bluetooth-Technologie (Bluetooth Low Energy Beacon) eine zufällige Zeichenfolge – ein sogenanntes temporäres Identifikationsmerkmal (TempID) – aussendet – als TempID-Token. Diese TempID ändert sich regelmäßig innerhalb eines Tages, bspw. alle 5, 10, 15 oder 30 Minuten. Empfängt das Smartphone A mit einer installierten App von einem Smartphone B (ebenfalls mit App) ein Signal einer bestimmten Stärke, wird daraus der Abstand der Smartphones zueinander geschätzt. Je stärker das Signal zwischen den Smartphones, desto geringer ist der Abstand zwischen den Personen. Ist der Abstand zwischen den Personen gering genug, entpacken beide Apps das jeweils andere TempID-Token und speichern die entpackte, fremde TempID ab.

Die so gesendeten eigenen und empfangenen fremden TempIDs werden in der eigenen App für eine begrenzte Dauer gespeichert und sind für diese Dauer personenbezogen. Sind sind personenbezogen, weil sie auf einem Smartphone (in der App) gespeichert sind, das einer Person zugeordnet ist. Da die ausgesendeten TempIDs sich über die Zeit ändern, können Nutzerïnnen einander in alltäglichen Situationen nicht dauerhaft verfolgen (tracken).

b) Autorisierung des Uploads, Anonymisierung, Zwischenspeicherung und Verbreitung des positiven Infektionsstatus

Angenommen Smartphone-Benutzerïn A wird später als infiziert diagnostiziert. In diesem Falle erhält sie eine TAN, ob von einer Ärztïn oder einer Behörde, mit der sie den Upload der TempIDs, die mit der Diagnose zu Gesundheits-TempIDs wurden, auf den CA-Server authentisieren kann. Nach dem Upload wird rechtlich, organisatorisch und technisch wirksam anonymisiert, und die infektionsanzeigenden Daten ohne Personenbezug (iDoP) werden auf dem Server als zentralem Zwischenspeicher gespeichert. Anschließend werden sie über Updates an alle genutzten Apps verteilt.

c) Dezentrale Kontaktnachverfolgung

Alle anderen Smartphone-Benutzerïnnen laden regelmäßig die veröffentlichten infektionsanzeigenden Daten ohne Personenbezug (iDoP) in ihre App herunter. Diese TempIDs sind ohne Aussage über die Verbindung zu einer identifizierten oder identifizierbaren natürlichen Person (Article 29 Data Protection Working Party 2007). Sie haben zugleich nur einen Informationswert für all diejenigen Personen, die mit den infizierten Personen innerhalb eines bestimmten Risikoraums Kontakt hatten.

Der Abgleich der auf dem Server veröffentlichten infektionsanzeigenden Daten ohne Personenbezug (iDoP) mit den lokal auf den Smartphones gespeicherten TempIDs ermöglicht die Feststellung, ob dieser Benutzer in einem bestimmten Zeitraum Kontakt mit einer vermutlich infektiösen Person hatte. Aus den Daten lässt sich jedoch nicht ableiten, ob der Kontakt über längere Zeit mit einer einzigen infizierten Person bestand oder ob es eher kurze Kontaktereignisse mit vielen verschiedenen Personen waren. Solche Details können aus den Daten nicht rekonstruiert werden. Anhand einer einprogrammierten Berechnungsvorschrift wird aus den Kontaktereignissen ein Risiko-Score berechnet.

Auf dem zentralen Server befinden sich keine Daten darüber, welche Personen infiziert sind, wo sie sich wann aufgehalten haben, oder welche Personen sie wo getroffen haben.

Es muss der Prozess noch ausgestaltet werden, mit dem eine ausschließlich einmal und nur von der als positiv getesteten Person nutzbaren TAN auf Seiten der diganostizierenden Ärztïnnen erzeugt und an diese Person übermittelt werden kann. Eine besondere Rolle kann eine TAN spielen, die zu ersten Hälfte unter Anwesenden – also Patentïn und Ärztïn – augetauscht, während der andere Teil der TAN per Telefon nach dem Ergebnis der Laboruntersuchung der Patientïn mitgeteilt wird. Mit der Eingabe der beiden TAN-Teile wird der Upload auf den Server inittiert, damit die Gesundheits-TempIDs auf den CA-Server hochgeladen werden. Wenn der Upload während des Telefonats iniitiert wird, kann die Ärztïn die Gültigkeit der TAN nach dem Ende des Telefonats außer Funktion setzen, andernfalls muss die Patientin die Ärztin nach dem Upload erneut anrufen, damit diese die TAN außer Funktion setzt.

Sobald ein positiver Match festgestellt wird, also Infektionsgefahr besteht, können alle TempIDs in der App gelöscht werden bzw. kann die App deinstalliert werden. Hierbei ist noch der Zeitraum zu berücksichtigen, der beansprucht werden muss, um bereits hochgeladene infektionsanzeigenden Daten ohne Personenbezug (iDoP) auf dem CA-Server, bspw. für den Falle einer doch nicht vorhandenen Infektion, löschen zu lassen.

4.3 Legitimität des Zwecks

Die Unterbrechung von Infektionsketten durch Warnung möglicherweise Infizierter mit Hinweis auf Quarantäneempfehlung sind bei einer hochansteckenden und im schlimmsten Falle tödlich verlaufenden Krankheit nicht nur legitim, sondern geboten.

Die dafür genutzte Verarbeitungstätigkeit und die dabei verwendeten Techniken wie bspw. eine App mit Server, müssen den Anforderungen des Datenschutzes und der IT-Sicherheit genügen. Besonders grundrechtsintensive Verarbeitungstätigkeiten sind dabei in der Nachweispflicht, dass sie den möglichst eng begrenzt ausgewiesenen Zweck erfüllen und es keine mildere, grundrechtsschonendere Variante gibt (vgl. Kapitel 5.4).

4.4 Abgrenzung von »benachbarten« Zwecken

In den Diskussionen um die Corona-App (CA) werden unterschiedliche Erwartungen an die Funktionen einer solchen App gestellt. In der Regel gilt die Aufmerksamkeit dabei allein der CA und nicht der Verarbeitungstätigkeit als Ganze, von der die Nutzung der CA nur ein Teil ist.

Andere Zwecke als den oben genannten zu verfolgen bedeutet, dass es sich um andere Verarbeitungstätigkeiten handelt, die eine andere Schwellwert- und Datenschutz-Folgenabschätzung (DSFA) als die hier vorgelegte durchlaufen müssen, die wiederum andere Risiken und andere Schutzmaßnahmen zutage fördern können. Die vorliegende DSFA beschränkt sich ausschließlich auf eine Verarbeitung zum oben ausgewiesenen Zweck der Identifikation und Unterbrechung von möglichen Infektionsketten durch Informierung potenziell CV-infizierter Personen.

Andere Zwecke – und damit andere Funktionen der CA – wären zum Beispiel (a) die Nachverfolgung der epidemiologischen Verbreitung des CV, (b) das Warnen vor CV-infizierten Inhaberïnnen von Smartphones in spontanen Begegnungen, (c) die Überwachung von CV-infizierten Personen, (d) die Erstellung von Prognosen für die epidemiologischen Verbreitung, (e) die Behandlung von CV-infizierten Personen, die ein Smartphone besitzen.

I. Nachverfolgung der epidemiologischen Verbreitung des CV

Aus epidemiologischer Sicht ist es wünschenswert und legitim, eine geographische Verbreitung des CV nachvollziehen zu können. Diese Funktionalität wird bislang durch Meldungen der Gesundheitsämter gewährleistet.

Mit der CA-Typ3 dezentral wäre eine vermutlich ausreichend auflösende Lokalisierung des CV in dem Fall möglich, wenn es nicht nur einen einzigen zentralen Server sondern viele geographisch verteilte Server gäbe und Infizierte angehalten wären, sich beim nächstgelegenen Server, etwa dem des zuständigen Gesundheitsamts, zu melden. Ansonsten ließe sich mit einer Verarbeitungstätigkeit auf Basis von CA-Typ3 dezentral nur die Tatsache gemeldeter Fälle bzw. deren Zu- oder Abnahme feststellen, sofern infizierte Personen mit CA-Typ3 dezentral verpflichtet sind, ihre Gesundheits-TempIDs hochzuladen. Dies wäre ein Nebenzweck, den eine CA-Typ3 dezentral erfüllen könnte, und der, wenn er zum Bestandteil der Zweckbestimmung gemacht würde, eine Erweiterung der DSFA zur Identifikation weiterer Risiken nach sich zöge.

II. Warnen vor CV-infizierten Inhaberïnnen von Smartphones während einer Begegnung

Aus unmittelbarer Sicht der Betroffenen wäre es wünschenswert und grundsätzlich legitim, wenn Inhaber einer CA sich bei alltäglichen spontanen Begegnungen automatisiert gegenseitig mit Hilfe einer App über ihren Status bezüglich einer CV-Infektion informierten. Dieser Zweck zieht jedoch eine Verarbeitung nach sich, die intensiv mit personenbezogenen Daten arbeitet.

Der Nutzen einer solchen App zur Verhinderung von Kontakten mit CV-Infizierten hingegen wäre gering, da zu erwarten ist, dass die identifizierten CV-Infizierten sich nicht mehr in der Öffentlichkeit aufhalten werden oder aber ihre Infektion bewusst verschleiern wollen.

Der Nutzen einer solchen App bei auch getestet nicht-festgestellt infizierten Personen wäre ebenfalls gering, weil die Inkubationszeit variabel ist, zwischen wenigen bis zu 14 Tagen, und eine Infektionsgefahr auch bei Ausbleiben von Symptomen besteht.

Der Nutzen einer App, mit der getestet-immunisierte Personen per Bluetooth Ihren Status melden, könnte erwogen werden, liegt aber nicht im Gegenstandsbereich dieser DSFA. Dieser Zweck ist auch nicht als Nebenzweck der CA-Typ3 dezentral umsetzbar.

III. Überwachung von CV-Infizierten

Eine der am häufigsten formulierten Anforderungen an eine CA besteht darin, CV-infizierte Personen oder mögliche Kandidatïnnen per App überwachen zu können.

In dieser Vorstellung hätte eine App die Funktion einer elektronischen Fußfessel. CV-infizierte Personen wären verpflichtet, jede Bewegung außerhalb ihres Quarantäne-Quartiers – oder innerhalb eines Krankenhauses – nur unter Mitnahme ihres Smartphones durchzuführen. Es muss dann eine Instanz geben, die solche Bewegungen überwacht und bei riskanten Begegnungen gegebenenfalls Alarm auslöst, entweder in einer Meldestelle oder unmittelbar bei anderen Smartphone-Nutzerïnnen. Alternativ müssten riskante Begegnungen protokolliert werden mit dem Zweck, CV-infizierten Personen im Nachhinein nachweisen zu können, dass diese sich nicht an Auflagen gehalten haben.

In der am 7. April 2020 vom RKI veröffentlichten »Corona-Datenspende«-App wird die Funktion der Überwachung der Gesundheitsdaten von Personen durch die Kopplung einer Smartphone-App mit Fitnesstrackern realisiert, so dass zusammen mit der

Lokalisierung der Nutzerïnnen anhand von Postleitzahlen eine auch örtlich spezifizierte Vollüberwachung der Körperfunktionen von Nutzerïnnen stattfindet. Doch auch ein solches Einsatzszenario verfolgt einen gänzlich anderen Zweck und stellt eine gänzlich andere Verarbeitungstätigkeit dar. Dieser Zweck wäre ebenfalls nicht als Nebenzweck mit einer CA-Typ3 dezentral zu realisieren und zöge einen sehr viel intensiveren Grundrechtseingriff nach sich.

IV. Erstellung von Prognosen für die epidemiologischen Verbreitung

Der Zweck der Erstellung von Prognosen für die epidemologische Verbreitung geht einen Schritt weiter als der in (a) beschriebene. Wissenschaftliche Prognosen versuchen statistische Aussagen über die zukünftige Situation zu machen, um beispielsweise die Wirkung von bestimmten Maßnahmen oder den baldigen Ressourcenbedarf (Krankenhausbetten, Medikamente) abschätzen zu können. Auch dieser Zweck erscheint legitim im Sinne der Vorsorge- und Versorgungsplanung.

Zur Umsetzung dieses Zwecks wären voraussichtlich Daten von bereits als infiziert diagnostizierten Personen und deren ungefähre geographische Position notwendig, um einschränkende Maßnahmen und zusätzliche Ressourcenaufwände möglichst minimal und regional begrenzt zu halten. Für die Erstellung von Prognosen müssten diese Daten zentral gespeichert und methodisch kontrolliert ausgewertet werden.

In der am 7. April 2020 vom RKI veröffentlichten App wird diese Funktion durch eine Smartphone-App realisiert, die anhand einer von der Nutzerïn eingegebenen Postleitzahl die Lokalisierung von Personen realisiert (Robert Koch-Institut 2020b). Als Zweck wird ausgewiesen:

> »Das zur Verfügung stellen der Daten meines Fitnessarmbands unterstützt das Robert Koch-Institut (im Folgenden ›RKI‹) dabei, eine bessere Vorhersage des bundesweiten Erkrankungsverlaufs mit COVID-19 und damit eine verbesserte Steuerung von Eindämmungsmaßnahmen gegen die Corona-Pandemie zu ermöglichen. Die Vorhersagen sollen tagesaktuell auf Postleitzahlen- bzw. Kreisebene getroffen und in anonymisierter Form der Öffentlichkeit zur Verfügung gestellt werden. Auf Basis wissenschaftlicher Modelle berechnet die App anhand meiner personenbezogenen Daten täglich die Wahrscheinlichkeit des Vorliegens einer grippeähnlichen Erkrankung, wie Covid-19. Bereits die Auswertung des Ruhepulses, der Schlafdauer und des Aktivitätslevels sind ausreichend für eine Erkennung von entsprechenden Symptomen. Meine individuellen Daten werden mit den Daten aller anderen App-Nutzer zusammengeführt und national / regional ausgewertet (im Folgenden ›Zweck‹).« (Robert Koch-Institut 2020b)

Damit kann die epidemiologische Verbreitung vorhergesagt werden, indem Körperfunktionen von Personen überwacht werden, deren Adressdaten für das RKI zugänglich sind.

In jüngerer Zeit sind solche Vorhaben mit Techniken aus dem Bereich »Big Data« und sogenannter »Künstlicher Intelligenz« unterstützt worden. Die Risiken, die von einer IT-gestützten statistischen Analyse diesen Umfangs ausgehen, bei der ganze Populationen ausgewertet werden, sind zuletzt bei dem Cambridge-Analytica-Fall zu Tage getreten. In diesem Fall wurden die Daten von Millionen von Facebook-Nutzerïnnen für die Zwecke der Manipulation demokratischer Wahlen verwendet. Je größer die zentral verwaltete Datenmenge, desto größer sind die Begehrlichkeiten und Missbrauchsrisiken.

Zwar könnte dieser Zweck ergänzend zu (a) aufgenommen werden, er hätte aber aufgrund der zentralisierten Speicherung und der zusätzlichen statistischen Auswertung neue schwerwiegende Folgen und Risiken für Einzelne, Gruppen und die Gesellschaft und würde daher eine eigenständige DSFA benötigen.

V. Behandlung von CV-infizierten Inhaberïnnen von Smartphones

Die EU-Kommission hat am 8. April 2020 eine Empfehlung für einen europaweiten einheitlichen Standard vorgelegt. In Erwägungsgrund 13 weist sie unter anderem die Behandlung von CV-Erkrankten mit Hilfe von medizinischen Geräten als legitimen Zweck aus (European Commission 2020). Darunter könnte auch die CA fallen.

Dieser Zweck ist unspezifisch und kann die Möglichkeiten umfassen, den COVID-19-Erkrankten über die CA lediglich Empfehlungen zur Selbstbehandlung zu geben, einen text-, audio- oder videogestützten Kommunikationskanal zwischen Ärztïnnen und Patientïnnen zu etablieren oder den COVID-19-Erkrankten Zwangsmaßnahmen durch eine Behörde aufzuerlegen.

Hier fehlt es an einer genauen Zweckbestimmung und Verfahrensbeschreibung, auf deren Grundlage eine eigenständige DSFA durchgeführt werden kann.

4.5 Verwendete Kategorien personenbezogener Daten

Nachfolgend werden die verwendeten Kategorien personenbezogener Daten beschrieben, die Empfängerïnnen dieser Daten sowie gegebenenfalls eine Übermittlung an ein Drittland oder an eine internationale Organisation.

Die Übermittlung an ein Drittland ist im Kontext von Cloud-Computing nicht ausgeschlossen. Die Cloud-Dienste großer Anbieter können sich außerhalb der EU befinden.

Auch die Übermittlung an internationale Organisationen könnten im Rahmen einer transnationalen Kooperation zur Pandemie-Bekämpfung stattfinden.

Temporärer pseudonymer Identifikator (TempID) Der temporäre pseudonyme Identifikator (TempID) bildet in dem Informationsmodell die zeitlich eng begrenzte Existenz einer CA-Benutzerïn ab, in dessen Nähe sich Infektionen abspielen können. An sich enthält dieses TempID keine Informationen über Ort, Zeit oder Person, sie ist aber personenbezogen, soweit sie sich auf dem Smartphone einer Person befindet, der aussendenden oder der empfangenden. Diese Information wird in regelmäßigen Intervallen geändert, bspw. alle 5, 10, 15 oder 30 Minuten. Empfängerïnnen dieser Information sind andere CA-Benutzerïnnen in Bluetooth-Reichweite.

Entfernung Die Entfernung ist der geschätzte Abstand zwischen zwei in physischer Reichweite befindlichen Smartphones. Dieser wird sensorisch mittels der Bluetooth-Signalstärke der empfangenen TempIDs ermittelt. Der konstruierte Zusammenhang zwischen Signalstärke und Entfernung beruht jedoch auf unterschiedlichen Annahmen über die physische und technische Situation. Eine Annahme ist zum Beispiel, dass der Standort des Smartphones mit dem Standort der CA-Benutzerïn im dreidimensionalen Raum identisch ist. Eine andere ist, dass im Kontaktfeld keine Raum trennenden Elemente vorhanden sind (zum Beispiel Glaswände).

Dieses Datum wird zusammen mit einer empfangenen fremden TempID abgespeichert.

Zeitdauer Die Zeitdauer bezieht sich auf die registrierte Anzahl identischer TempIDs in Abhängigkeit von der Zeit. Dieses Datum wird zusammen mit der empfangenen fremden TempID auf dem Smartphone der CA-Benutzerïn gespeichert.

Infektionsstatus Der Infektionsstatus hat mehrere CV-Zustände: {nicht infiziert, exponiert, infiziert, immun}. Der erste Zustand ist der Standardzustand. Der zweite Zustand ergibt sich aus Kontaktereignissen mit infizierten Personen. Der dritte und vierte Zustand hängen von einer ärztlichen Diagnose ab.

Im Falle des Infektionsstatus »infiziert« wird diese Information durch die Übermittlung der Gesundheits-TempID an den Server mitgeteilt. Nach der Anonymisierung befinden sich nur infektionsanzeigende Daten ohne Personenbezug (iDoP) auf dem Server.

Risiko-Score Gibt es beim Abgleich der sensorisch empfangenen TempIDs mit den vom Server erhaltenen infektionsanzeigende Daten ohne Personenbezug (iDoP) Übereinstimmungen, so wird anhand von Dauer und Entfernungsprofil der Kontaktereignisse unter Zuhilfenahme der statistischen Berechnungsvorschrift ein individueller Risiko-Score berechnet. Ist dieser Wert oberhalb eines festgelegten Grenzwerts, wird die Benachrichtigung der Nutzerïn ausgelöst.

IP-Adressen Die IP-Adresse ist für die Kommunikation im Internet (Routing, Adressierung) notwendig. Empfängerïnnen dieser Daten sind aufgrund der Internet-Architektur in erster Linie die Server-Betreiberïnnen und in zweiter Linie die Internet-Provider.

In drei Anwendungsfällen wird die IP-Adresse mindestens benötigt: (a) Beim Abruf einer App aus einer Installationsquelle im Internet, (b) beim Abruf von infektionsanzeigenden Daten ohne Personenbezug (iDoP) vom Server und (c) beim Melden der eigenen Gesundheits-TempIDs beim Server, wenn eine Infektion bei der Benutzerïn diagnostiziert wurde.

Zeitangabe Die Zeitangabe bezeichnet das Datum des Kontaktes. Dieses Datum wird zusammen mit der empfangenen fremden TempID auf dem Smartphone der CA-Benutzerïn gespeichert.

TAN Die TAN wird von der Verantwortlichen oder einer vertrauenswürdigen Dritten erzeugt und von der behandelnden Ärztïn an eine als infiziert diagnostizierte Person übermittelt. Diese TAN regelt die Zugriffskontrolle auf dem Server und erlaubt es der Person, und nur ihr, ihre Gesundheits-TempIDs an den Server zu übermitteln.

4.6 Analyse der einzelnen Verarbeitungstätigkeiten

In diesem Abschnitt werden die Verarbeitungstätigkeiten nacheinander in sogenannte Vorgänge gemäß Art. 4 Nr.2 DSGVO aufgeschlüsselt, die von der Verantwortlichen fair und beherrschbar gestaltet sein müssen. Einige dieser Vorgänge sind IT-gestützt und werden in Rahmen der Analyse eingehender betrachtet. Einen schematischen Überblick bietet die Abbildung 4.1.

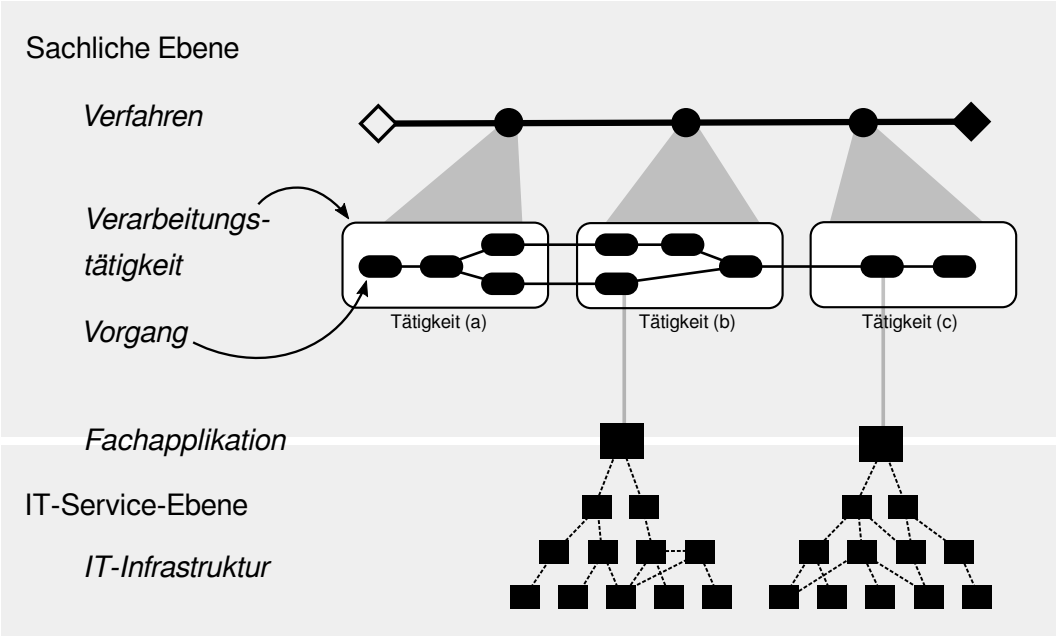

Abbildung 4.1: Verfahrensstruktur

Im ersten Schritt werden für jede Verarbeitungstätigkeit die folgenden drei Analyseebenen betrachtet:

1. **Sach- oder Zweckebene,**
2. **Fach(applikations)ebene,**
3. **IT-Service-Ebene.**

Im zweiten Schritt werden auf allen Ebenen die für die Verarbeitungstätigkeit materiell benötigten betrieblichen Komponenten beschrieben, nämlich:

- die darin verarbeiteten personenbezogenen **Daten** und ggf. technischen, organisatorischen und personellen **Rollen,**
- die beteiligten technischen **Systeme, Dienste** und damit verbundenen Betriebs**prozesse,**
- die vorhandenen **Kommunikationsbeziehungen** und dafür verwendeten **Schnittstellen.**

Die erste (sachliche) Ebene ist in allgemeiner Weise bereits in Abschnitt 4.2 beschrieben worden und wird hier nun mit Blick auf die darin stattfindenden Vorgänge beziehungsweise Vorgangsreihen untersucht.

Verarbeitungstätigkeit »App-seitige Verarbeitung von Kontaktereignissen«

Sachliche Ebene:

Nr.	Vorgang	Rollen	Daten
0	Installation und Inbetriebnahme der CA	CA-Benutzerïn	Nutzungsdaten, Gerätedaten
1	Lokales Generieren eigener TempIDs		TempIDs
2	Speichern eigener TempIDs		TempIDs
3	Übermittlung eigener TempIDs		TempIDs
4	Empfangen fremder TempID-Token über BTLE		fremde TempID-Token
5	Speichern von Kontaktereignissen		fremde TempIDs, Entfernung, Zeitdauer, Zeitangabe

Fachapplikationsebene:

Nr.	Vorgang	Fachapplikation(en)
1	Lokales Generieren eigener TempIDs	CA
2	Speichern eigener TempIDs	CA
3	Übermittlung eigener TempIDs	CA
4	Empfangen fremder TempID-Token über BTLE	CA
5	Speichern von Kontaktereignissen	CA

IT-Services-Ebene:

Nr.	Fachapplikation	IT-Systeme / Dienste	Prozesse	Rolle
1	CA	Smartphone, BTLE-Dienst	Life-Cycle-Pflege	CA-Benutzerïn

Kommunikationsbeziehungen und Schnittstellen:

Nr.	Quelle	Ziel	Schnittstelle	Zweck
1	CA1	CA2	Bluetooth	Übermittlung von TempID-Token von CA1
2	CA2	CA1	Bluetooth	Übermittlung von TempID-Token von CA2

Verarbeitungstätigkeit »Autorisierung des Uploads, Anonymisierung, Zwischenspeicherung und Verbreitung des positiven Infektionsstatus«

Sachliche Ebene:

Nr.	Vorgang	Rollen	Daten
1	Ärztliche Untersuchung (Proben-Entnahme)	Ärztïn, CA-Benutzerïn	TAN
2	Erhebung des Infektionsstatus (Testvorgang)	med. Personal	
3	Autorisierung des zugeordneten TANs und Übermittlung an CA-Benutzerïn	Ärztïn, CA-Benutzerïn	TAN
4	Autorisierte Übermittlung der Gesundheits-TempIDs der CA-Benutzerïn an den Server	CA-Benutzerïn	TAN, Gesundheits-TempIDs
5	Anonymisierung der Gesundheits-TempIDs auf dem Server	Betreiberïn	Gesundheits-TempIDs, infektionsanzeigende Daten ohne Personenbezug (iDoP)
6	Speicherung der iDoP auf dem Server	Betreiberïn	iDoP
7	Löschen der iDoP auf dem Server 14 Tage nach dem epidemiologisch festgelegtem Zeitpunkt	Betreiberïn	iDoP

Fachapplikationsebene:

Nr.	Vorgang	Fachapplikation(en)
1	Ärztliche Untersuchung (Proben-Entnahme)	TAN-Verwaltung
2	Erhebung des Infektionsstatus (Testvorgang)	*unbekannt*
3	Autorisierung des zugeordneten TANs und Übermittlung an CA-Benutzerïn	TAN-Verwaltung
4	Autorisierte Übermittlung der Gesundheits-TempID an den Server	CA
5	Anonymisierung der Gesundheits-TempIDs auf dem Server	CA-Server
6	Speicherung der infektionsanzeigende Daten ohne Personenbezug (iDoP auf dem Server	CA-Server
7	Löschen der iDoP auf dem Server 14 Tage nach dem epidemiologisch festgelegtem Zeitpunkt	CA-Server

IT-Service-Ebene:

Nr.	Fachapplikation	IT-Systeme / Dienste	Prozesse	Rollen
1	TAN-Verwaltung	*unbekannt*	*unbekannt*	Ärztïn
2	CA	Smartphone, Internet	Life-Cycle-Pflege	CA-Benutzerïn
3	CA-Server, Datenbank-Server, Server-OS, HW	RZ, Internet	Server-Administration, RZ-Betrieb	Server-Admin

Kommunikationsbeziehungen und Schnittstellen:

Nr.	Quelle	Ziel	Schnittstelle	Zweck
1	CA	CA-Server	TCP/UDP	Übermittlung der Gesundheits-TempIDs
2	CA-Server	CA	TCP/UDP	Abruf der Liste von infektionsanzeigenden Daten ohne Personenbezug (iDoP)

Verarbeitungstätigkeit »Dezentrale Kontaktnachverfolgung«

Sachliche Ebene:

Nr.	Vorgang	Rollen	Daten
1	Abfragen der Liste der infektionsanzeigenden Daten ohne Personenbezug (iDoP) vom Server durch andere CA-Benutzerïnnen		Liste von iDoP
2	Abgleichen der infektionsanzeigenden Daten ohne Personenbezug (iDoP) mit den über Bluetooth empfangenen TempIDs auf dem Smartphone		Listen von TempIDs und iDoPs, Matches
3	Verwenden der Matches für die Berechnung des Infektionsrisikos und der Darstellung von Verhaltensempfehlungen nichts tun, in Quarantäne begeben, testen lassen		Matches
4	Verwendung der Handlungsempfehlungen, um ggf. ärztliches Personal oder das Gesundheitsamt zu kontaktieren	CA-Benutzerïn	Dokumente, Text, Bild, Interaktiv

Fachapplikationsebene:

Nr.	Vorgang	Fachapplikation(en)
1	Abfragen der Liste der infektionsanzeigenden Daten ohne Personenbezug (iDoP) vom Server durch andere CA-Benutzerïnnen	CA, CA-Server
2	Abgleichen der infektionsanzeigenden Daten ohne Personenbezug (iDoP) mit den über Bluetooth empfangenen TempIDs auf dem Smartphone	CA
3	Verwenden der Matches für die Berechnung des Infektionsrisikos und der Darstellung von Verhaltensempfehlungen nichts tun, in Quarantäne begeben, testen lassen	CA
4	Verwendung der Handlungsempfehlungen, um ggf. ärztliches Personal oder das Gesundheitsamt zu kontaktieren	CA

IT-Service-Ebene:

Nr.	Fachapplikation	IT-Systeme / Dienste	Prozesse	Rollen
1	CA	Smartphone, Internet	Life-Cycle-Management	CA-Benutzerïn
4	CA-Server	Datenbank-Server, RZ, Internet	Server-Administration	Server-Admin

Kommunikationsebenen und Schnittstellen:

Nr.	Quelle	Ziel	Schnittstelle	Zweck
1	CA-Server	CA	TCP/UDP	Übermittlung der infektionsanzeigenden Daten ohne Personenbezug (iDoP) an die CA zum lokalen Abgleich

4.7 Benennung von Maßnahmen zur Sicherstellung der Zweckbindung

Wesentliche Maßnahmen zur Sicherstellung der Zweckbindung für einen ausgewiesenen Zweck besteht im Allgemeinen darin, pseudonymisierte und anonymisierte Daten, bei denen der Personenbezug so weit wie möglich aufgehoben oder unter Bedingungen gestellt ist, zu verwenden und Datenbestände, Kommunikationsbeziehungen und Teilprozesse jeweils voneinander zu trennen.

Für das vorliegende Verfahren bedeutet das, dass die TempIDs nicht-sprechend, sondern im Idealfall weltweit eindeutige Zufallszahlen sind. Sie sollen ohne bedingte Kontextierungen keine unmittelbare Aussagen über Personen, Orte, Zeiten, soziale Umstände möglich machen.

Um die Zweckbindung auf dem Smartphone durchzusetzen ist es erforderlich, die App in einem Container zu betreiben, der vor Zugriffen durch andere Apps oder durch das Betriebsystem schützt und dessen Schnittstelle zu den TempID-Token sowie zum Download der infektionanzeigenden Daten ohne Personenbezug (iDoP) und Upload der Gesundheits-TempID zum Server einem besonderen Schutz (Authentisierung, Verschlüsselung) sowie Kontrolle bzgl. der Protokollierung unterliegen müssen der Ereignisse an diesen Schnittstellen.

Ein ganz wesentlicher Personenbezug besteht in dieser Verarbeitungstätigkeit zu dem Zeitpunkt, an dem von der Ärztïn eine TAN übermittelt wird, mit dem der Upload der Gesundheit-TempIDs auf den Server autorisiert wird. Die von der Ärztïn erzeugte Verknüpfung von TAN und Person ist streng vertraulich und muss durch geeignete Sicherheitsmaßnahmen, wie Zutritts-, Zugangs- und Zugriffskontrollen, Berechtigungsmanagement, durch Backups, Verschlüsselung, Integritätssicherungen, Löschen und Protokollierung, inklusive einem reifen Datenschutzmanagement geschützt werden.

Eine weitere Maßnahme hinsichtlich der Zweckbindung und damit der Nichtverkettung ist die automatische Löschung nach Ablauf der Anzahl an Tagen, die die zuständige Gesundheitsbehörde als maximale Infektiosität ermittelt hat.

4.8 Benennung weiterer geplanter Schutzmaßnahmen

Alle Verarbeitungstätigkeiten müssen den Anforderungen der DSGVO genügen, wie sie in konzentrierter Form der Art. 5 DSGVO mit den Grundsätzen fordert. Hinzukommen insbesondere die Anforderungen aus Art. 25 DSGVO zum Datenschutz durch Technikgestaltung und aus Art. 32 DSGVO bezüglich der Sicherheit und Belastbarkeit (besser: Resilienz Gonscherowski, Hansen und Rost 2018) der Verarbeitung.

Die nachfolgenden Schutzmaßnahmen wurden den Design-Vorschlägen – vor allem den Entwurfsdokumenten des DP-3T-Projektes (DP-3T Project 2020a) – zum beschriebenen Verfahrenszweck entnommen und nach den Standard-Datenschutz-Schutzzielen geordnet (DSK SDM2.0a). Die Schwachstellen und Sicherheitslücken, die eine Gefährdung oder Verletzung der Schutzziele nach sich ziehen, werden in Abschnitt 7 beschrieben. Das Schutzziel der Nicht-Verkettbarkeit wurde bereits in Abschnitt 4.7 adressiert.

a) App-seitige Verarbeitung von Kontaktereignissen

Diese Verarbeitungstätigkeit wird technisch unterstützt durch die Nutzung eines Smartphones und die darauf installierte CA.

Für das Smartphone sind keine zusätzlichen technischen oder organisatorischen Maßnahmen zur operativen Sicherheit vorgesehen als die allgemeinen Empfehlungen zum Gebrauch von Smartphones.

Vertraulichkeit – Die Kontakthistorie ist durch die verschlüsselte Speicherung auf dem Smartphone vor nicht autorisierten Zugriffen gesichert.

Verfügbarkeit – Die App muss nicht freigeschaltet oder anders persönlich aktiviert werden, sodass auch mehrere Smartphones parallel verwendet werden können.

Integrität
Keine.

Intervenierbarkeit – Die Teilnahme kann jederzeit beendet werden durch das Deinstallieren der CA, das Abschalten des Bluetooth-Modules oder des Smartphones.

Transparenz – Dieser Verfahrensschritt und die Funktion der CA wird in der Verfahrensdokumentation beschrieben.

– Die Betroffene wird durch eine Datenschutzerklärung in der App über das Verfahren der Datenverarbeitung informiert. Spezifikation, Dokumentation und Quellcode der CA liegen offen vor, die CA ist also prüfbar.

Nicht-Verkettbarkeit – Siehe Abschnitt 4.7.

b) Autorisierung des Uploads, Anonymisierung, Zwischenspeicherung und Verbreitung des positiven Infektionsstatus

Vertraulichkeit – Die Datenübertragung zwischen Server und CA ist durch die Nutzung eines verschlüsselten und integritätssicheren Kanals gegenüber nichtautorisierten Zugriffen geschützt.

– Es werden TempIDs als Pseudonyme verwendet,[1] die eine unmittelbare Identifizierung von infizierten Personen aus Sicht des Server-Betreiberïn erschweren.

– Die von der Ärztïn erzeugte Verknüpfung von TAN und Person ist streng vertraulich zu halten.

– Der Server legt keine Protokolle (IP-Adresse o.ä.) der Uploadvorgänge an.

Integrität – Die Datenübertragung zwischen Server und CA ist durch die Nutzung eines verschlüsselten und integritätssicheren Kanals gegenüber nichtautorisierten Zugriffen geschützt.

– Freigabe der Datenübertragung via TAN, die von Ärztïnnen nur nach Positivtest vergeben wird.

Verfügbarkeit keine.

Intervenierbarkeit – CA-Benutzerïnnen stoßen das Mitteilen des Infektionsstatus selbstständig an. Freigabe der Datenübertragung explizit nur nach TAN-Eingabe, was zusätzlich die Relevanzwahrnehnmung steigert.

[1] Im DP-3T-Whitepaper etwa wird fälschlicherweise von anonymen IDs gesprochen.

Transparenz – Dieser Verfahrensschritt und die Funktion des Serves wird in der Verfahrensdokumentation beschrieben. Spezifikation, Dokumentation und Quellcode der App und des Servers liegen offen vor, CA und Server sind also prüfbar.

Nicht-Verkettbarkeit – Siehe Abschnitt 4.7.

c) Dezentrale Kontaktnachverfolgung

Vertraulichkeit – Die Datenübertragung zwischen Server und CA ist durch die Nutzung eines verschlüsselten und integritätssicheren Kanals gegenüber nichtautorisierten Zugriffen geschützt.

Integrität – Die Datenübertragung zwischen Server und CA ist durch die Nutzung eines verschlüsselten und integritätssicheren Kanals gegenüber nicht autorisierten Zugriffen geschützt.

Verfügbarkeit – Die Liste der infektionsanzeigenden Daten ohne Personenbezug (iDoP) ist aufgrund der zentralen Speicherung auf einem Server durch das erneute Herunterladen wiederherstellbar.

Intervenierbarkeit – Die Datenübertragung verlangt eine aktive Internetverbindung, diese kann deaktiviert oder aber nur der App keinen Zugriff auf das Internet gewährt werden.

Transparenz – Dieser Verfahrensschritt und die Funktion des Serves wird in der Verfahrensdokumentation beschrieben. Spezifikation, Dokumentation und Quellcode des Servers liegen offen vor, der Server ist also prüfbar.

Nicht-Verkettbarkeit – Siehe Abschnitt 4.7.

4.9 Benennung weiterer Anforderungen der DSGVO

Es muss ein Verfahren zur regelmäßigen Überprüfung der Verarbeitungstätigkeit nach Art. 32 Abs. 1 lit. d DSGVO implementiert sein. Das bedeutet konkret, dass ein Datenschutz- und IT-Sicherheitsmanagement implementiert werden muss, mit dem die Verantwortliche Schutz- und Kontrollmaßnahmen um- und durchsetzt. Die bei hohen Risiken obligatorisch zu bestellende Datenschutzbeauftragte ist wiederum aufgefordert, die Arbeit des exekutiven Datenschutzmanagements im Kontext eines umfassenden Qualitätsmanagement des Betriebs einer Verarbeitung zu beaufsichtigen im Hinblick darauf, dass das IT- und Datenschutzmanagement Mängel erkennt und diese wirksam behebt Rost und Welke 2020. Die IT-Sicherheit aller beteiligtenhttps://www.overleaf.com/project/5e92ec019289ed0001965966 IT-Komponenten muss gesichert sein. Zur Sicherung der Verfügbarkeit müssen zumindest die zentralen Komponenten redundant ausgelegt sein und Backups angefertigt werden. Die Authentizität der beteiligten Server, Clients und Dienste muss durch Rückgriff auf Zertifikate einer Public-Key-Infrastruktur sichergestellt sein. Alle Kommunikationsverbindungen müssen Ende-zu-Ende verschlüsselt sein, damit Dritte nicht erkennen können, ob personenbezogene Daten übertragen. Die Betroffenenrechte auf Information und Auskünfte, auf Berücksichtigung von Korrekturen und Löschungen (vgl. Art. 12–22) müssen durch die Verantwortliche bzw. die eingesetzten technischen Komponenten wirksam umgesetzt werden. Der Upload der Gesundheits-TempIDs im Falle der Infektion muss durch die Betroffene selbst und aktiv ausgelöst werden können.

4.10 Benennung der Verantwortlichen

Die Verantwortliche muss ihre Kontaktdaten sowie die der Vertreterin sowie der Datenschutzbeauftragten angeben.

Kapitel 5

Rechtsgrundlagen und Verantwortlichkeit

Das Kapitel dient der Beschreibung der vorhandenen und zu schaffenden Rechtsgrundlagen für das Verfahren und die Verarbeitungstätigkeiten sowie der Festlegung der Verantwortlichkeiten für diese Verarbeitungstätigkeiten.

5.1 Rechtmäßigkeit der Verarbeitung

In Umsetzung des Art. 8 der Charta der Grundrechte der Europäischen Union stellt die DSGVO Bedingungen zum Schutz der Rechte und Freiheiten natürlicher Personen auf, die eine Verarbeitung personenbezogener Daten ermöglichen. Dies gilt auch für die Verarbeitung von personenbezogenen Daten im Rahmen von Maßnahmen, die zur Eingrenzung und Bekämpfung von COVID-19 erfolgen, insbesondere dem Einsatz einer App.

Jede Verarbeitung personenbezogener Daten stellt zunächst einen Eingriff in die Rechte und Freiheiten der davon betroffenen Personen dar und ist daher zu rechtfertigen. Voraussetzung für die Rechtfertigung von Eingriffen ist die Einhaltung der Vorgaben der DSGVO, der ePrivacy Directive (ePrivacyRL) und der darauf beruhenden mitgliedstaatlichen Regelungen, in Deutschland dem BDSG 2018 und dem sektorspezifischem Recht. Ihre einzelnen Anforderungen sind dabei in Form der Grundsätze der Verarbeitung in Art. 5 DSGVO festgehalten. Dazu zählen u.a. die Rechtmäßigkeit, die Erforderlichkeit und die Verhältnismäßigkeit der Verarbeitung sowie die Richtigkeit der Daten und der Grundsatz der Datenminimierung. Die Einhaltung der Grundsätze für die Verarbeitung obliegt der Verantwortlichen. Sie ist es auch, die ihre Verarbeitung zum Nachweis der Rechtmäßigkeit auf eine Rechtsgrundlage stützen können muss und angemessene Maßnahmen zum Schutz der Betroffenen zu treffen hat.

5.1.1 Personenbezogene Daten

Voraussetzung für den sachlichen Anwendungsbereich der DSGVO und damit für alle Rechtsgrundlagen ist die Verarbeitung personenbezogener Daten.

Art. 4 Nr. 1 DSGVO definiert personenbezogene Daten als

> »alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ›betroffene Person‹) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;«

Bei Bewegungs- und Standortdaten (Typen 1 und 2, siehe Kapitel 1.1), die für ein Endgerät ermittelt werden, handelt es sich um Standortdaten, die über die Telefonnummer, die IP- oder MAC-Adresse des Endgerätes, bzw. allgemeiner deren Netzwerk- und Hardwareadresse, durch den Provider einer natürlichen Person zugeordnet werden können.

Kontaktdaten werden von der DSGVO nicht explizit definiert. Kontaktdaten werden durch einen Abgleich von TempIDs ermittelt. Sie werden ebenfalls auf dem Smartphone einer Person generiert und weisen , solange sie auf dem Smartphone gespeichert sind, Personenbezug auf.

Bei Telekommunikationsdaten handelt es sich um Stamm- und Verbindungsdaten die beim Provider natürlichen Personen zugeordnet werden können und damit in der Regel um personenbezogene Daten.

5.1.2 Gesundheitsdaten

Unabhängig von der Rechtsgrundlage für die Verarbeitung personenbezogener Daten, erfordert die Verarbeitung der personenbezogener Daten der in Art. 9 Abs. 1 DSGVO aufgezählten besonderen Kategorien auch eine (weitere) besondere Rechtfertigung. Grundsätzlich ist deren Verarbeitung untersagt, es sei denn eine der in Abs. 2 aufgezählten Ausnahmen trifft zu.

Krankheitsdaten sind eine besondere Kategorie personenbezogener Daten nach Art. 9 Abs. 1 DSGVO, die eine Aussage über den negativen Gesundheitszustand einer Person treffen.

Bei der im Falle einer positiv Testung auf COVID-19 von der zuständigen Gesundheitsbehörde oder -einrichtung an die Betroffene übermittelten TAN handelt es sich um ein Gesundheitsdatum, ebenso wie bei den Gesundheits-TempIDs von positiv diagnostizierten Personen, die eine TAN erhalten haben.

Wenn Gesundheitsdaten an den oder die Server übermittelt werden, und die Betreiberïn ein wirksames Trennungsverfahren (siehe Kapitel 8.3) umsetzt, handelt es sich bei dem Output des Verfahrens um infektionsanzeigende Daten ohne Personenbezug (iDoP).

5.1.3 Verarbeitung

Der Begriff der Verarbeitung[1] wird in Art. 4 Nr. 2 DSGVO durch Beispiele beschrieben. Danach meint Verarbeitung

> »jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;«

Art. 4 Nr. 2 DSGVO zählt verschiedener Verarbeitungsschritte auf, die im Wesentlichen den Lebenszyklus eines personenbezogenen Datums wiedergeben. Damit wird zum Ausdruck gebracht, dass jeder Umgang mit personenbezogenen Daten eine Verarbeitung im Sinne der DSGVO darstellen soll.

[1] Siehe dazu auch Kapitel 4.

Bei der Verarbeitung personenbezogener Daten im Rahmen der CA-Nutzung können unterschiedliche Verarbeitungstätigkeiten und darin Verarbeitungsvorgänge unterschieden werden (siehe Kapitel 4). Die Unterscheidung der Verarbeitungstätigkeiten und Verarbeitungsvorgänge ist Voraussetzung für eine korrekte Bestimmung der Verantwortlichkeit: Handelt es sich bei den Verarbeitungen um getrennte Vorgänge oder um Vorgangsreihen, können diese einerseits unterschiedliche Rechtsgrundlagen erforderlich machen und andererseits zu unterschiedlichen Verantwortlichkeiten führen. Für die rechtliche Einordnung können folgende Unterscheidungen getroffen werden:

- Nutzung der App auf dem Smartphone (Endgerät)
  - Verarbeitung auf dem Endgerät der Senderïn
    - Erzeugung und Übermittlung von TempIDs an andere App-Nutzerïnnen
    - Erhebung von empfangenen TempID-Token anderer App-Nutzerïnnen
    - Speicherung von empfangenen TempIDs anderer App-Nutzerïnnen
  - Übermittlung der Gesundheit-TempIDs an den oder die Server
- »Eingabe« einer TAN zur Authentisierung = Statusänderung in der App zu »infiziert« = Statusänderung der TempIDs zur Gesundheits-TempIDs in der App
- Übermittlung von Gesundheits-TempIDs an den Server
- Server
  - Anonymisierung der Gesundheits-TempIDs in infektionsanzeigende Daten ohne Personenbezug (iDoP)
  - Bereitstellen von infektionsanzeigenden Daten ohne Personenbezug (iDoP) zum Abruf
  - Speicherung von Telekommunikationsdaten
- Verarbeitung auf Empfängerïngerät
  - Abrufen der infektionsanzeigenden Daten ohne Personenbezug (iDoP) vom Server
  - Matching zwischen den TempIDs auf der eigene App und den heruntergeladenen iDoPs = Erzeugen der Kontaktdaten
  - Berechnung des Risiko-Scores auf den Kontaktdaten
  - Ergebnismeldung: Infektionswarnung, Kontakt mit Infiziertem ja/nein

Die Frage, ob die Betreiberïn der App oder die Betreiberïn des Servers Zugriff auf die verschlüsselten oder pseudonymisierten Daten nehmen kann, ist für die Frage, ob personenbezogene Daten verarbeitet werden unerheblich (vgl. EDPB und EDPS 2019, Para 8). Für die Bejahung einer Verarbeitung personenbezogener Daten reicht es aus, dass die TempIDs auf den Endgeräten der Nutzerïnnen generiert werden. Der Umstand, dass die Token über ein gesichertes Netzwerk verschlüsselt versendet werden, ändert nichts an dem Personenbezug der Token. Auch bei verschlüsselten personenbezogene Daten bleibt der Personenbezug erhalten.

Die Erforderlichkeit der Verarbeitung personenbezogener Daten kann nur im Verhältnis zu den angestrebten Zwecken ermittelt werden (siehe Kapiel 5.4.3). Die Zwecksetzung erfolgt durch die für die Verarbeitung Verantwortliche.

5.2 Verantwortlichkeit

Eine Verarbeitung personenbezogener Daten kann nur dann rechtmäßig erfolgen, wenn eine Stelle bestimmt werden kann, die für die Verarbeitung verantwortlich ist. Eingriffe in die Rechte und Freiheiten natürlicher Personen durch die Verarbeitung personenbezogener Daten sollen nicht im luftleeren Raum stattfinden (siehe EG 78 DSGVO). Die DSGVO weist in Art. 5 Abs. 2 iVm Art. 4 Nr. 7 DSGVO die Verantwortlichkeit der Stelle zu, die die Zwecke und Mittel der Verarbeitung alleine oder gemeinsam mit anderen bestimmt. Die so ermittelte natürliche oder rechtliche Person, Behörde, Einrichtung oder andere Stelle ist gem. Art. 5 Abs. 2 DSGVO dafür verantwortlich, dass die Grundsätze der Verarbeitung aus Art. 5 Abs. 1 DSGVO eingehalten werden und muss dies nachweisen können. Gem. Art. 24 Abs.1 DSGVO hat die Verantwortliche die technischen und organisatorischen Maßnahmen (EG 74 DSGVO) für die Einhaltung der Grundsätze aus Art. 5 Abs. 1 DSGVO, die einen angemessenen Schutz der Rechte und Freiheiten der Betroffenen gewährleisten, für die gesamte Verarbeitung nachweislich zu treffen. Auch die Pflicht zur Durchführung einer DSFA trifft gem. Art. 35 DSGVO die Verantwortliche.

Bei der Zuweisung der Verantwortlichkeit handelt es sich um eine Betrachtung der tatsächlichen, funktionalen Rolle, die die Verantwortliche für die Verarbeitung übernimmt (Article 29 Data Protection Working Party 2010, S. 9). Eine formale Zuweisung der Verantwortlichkeit kann in Ausnahmefällen per gesetzlicher Zuweisung erfolgen.

Die Verantwortliche definiert Art. 4 Nr. 7 DSGVO als

> »die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet«.

Verantwortliche kann danach jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle sein. Damit kommen zunächst alle, an der Verarbeitung beteiligten Akteurïnnen (siehe Kapitel 2.3) als Verantwortliche in Betracht. Da bislang keine gesetzlichen Bestimmungen über die CA oder ihren Einsatz vorliegen, kommt es darauf an, ob und wenn ja, inwieweit jede beteiligte Stelle über Zwecke und Mittel der Verarbeitung entscheidet.

Als Zweck einer Verarbeitung kommt jedes Ergebnis, das die Verarbeitung leitet, in Betracht. Zwecke müssen gem. Art. 5 Abs. 1 lit. b DSGVO vor der Verarbeitung festgelegt werden und eindeutig und legitim sein. Die Mittel beschreiben, wie das Ergebnis erreicht werden soll.

Maßgeblich ist dafür die tatsächliche Entscheidungsmacht im Hinblick auf die wesentlichen Elemente der Verarbeitung. Die Verantwortliche muss stets sowohl über Zwecke als auch die wesentlichen Mittel entscheiden. Eine Entscheidung allein über die Zwecke ist nicht ausreichend. Entscheidungen über wesentliche Mittel betreffen die Entscheidung, welche Daten verarbeitet werden, die Dauer sowie die Entscheidung, wer darauf Zugriff nehmen darf. Als nicht unbedingt wesentlich gelten zum Beispiel die Entscheidungen über die Auswahl der konkreten Hard- und Software. Die Entscheidungsmacht kann sich auch aus einer gesetzlichen Zuweisung ergeben, wenn das Gesetz Kriterien zur Bestimmung, die eine tatsächliche Entscheidungsmacht begründen, festlegt. Soweit sich der Zweck der Verarbeitung aus einer gesetzlichen Aufgabenzuweisung ergibt, kann auch dies ein Indiz für eine tatsächliche Entscheidungsmacht sein.

Für die faktische Entscheidungsmacht sind die tatsächlichen Gegebenheiten der Verarbeitung zu betrachten. Dazu kann gefragt werden »Warum wird diese Verarbeitung

durchgeführt?« und »Wer hat sie veranlasst?« (Article 29 Data Protection Working Party 2010). Hierbei ist zu berücksichtigen, dass eine Verarbeitung aus verschiedenen Verarbeitungsvorgängen bestehen kann, die für sich als unabhängige Verarbeitungsvorgänge betrachtet werden können oder die derart miteinander verbunden sind, dass sie nur gemeinsam als einheitliche Verarbeitung betrachtet werden können. Es sind insoweit die unterschiedlichen Verarbeitungsvorgänge zu unterscheiden. Ein Hinweis auf einen einheitlichen Verarbeitungsvorgang gibt der Zweck der Verarbeitung. Verarbeitungen, die demselben Zweck dienen, sind in der Regel als ein Vorgang oder eine Vorgangsreihe zu betrachten. Maßgeblich ist der entscheidungserhebliche Einfluss auf den spezifischen Verarbeitungskontext. Die Entscheidung über die Gründe der Verarbeitung und damit über ihren Zweck ist Kennzeichen tatsächlicher Entscheidungsmacht über eine Verarbeitung.

Als natürliche Personen fallen die Nutzerïnnen nicht von vornherein aus dem Begriff der Verantwortlichen heraus. Im Hinblick auf die Zwecke der Verarbeitung und die Zurverfügungstellung der CA an die Nutzerïnnen treten die Möglichkeiten der Nutzerïnnen in Bezug auf das »wie« der Verarbeitung und der technischen Ausgestaltung Entscheidungsmacht auszuüben aber in den Hintergrund, beziehungsweise sind faktisch mangels Konfigurationsmöglichkeiten nicht vorhanden. Zwar können Nutzerïnnen durch Installation der CA über das »ob« der Verarbeitung entscheiden, jedoch können sie die Zwecksetzung der Verarbeitung nicht beeinflussen. Auch der Umstand, dass Verarbeitungsschritte wie das Generieren der TempIDs oder das Matching auf den Endgeräten der Nutzerïnnen stattfindet, ist für sich genommen für die Zuordnung von Entscheidungsmacht über die Zwecke und Mittel nicht ausschlaggebend (vgl. dazu die Diskussion zu DRM-Systemen, die auf den Endgeräten von Nutzerïnnen laufen und dort die Rechte der Rechteinhaberïnnen durchsetzen (Becker u. a. 2003)). Der Austausch der TempIDs zwischen Nutzerïnnen stellt keinen eigenständigen Verarbeitungsvorgang dar, da damit ein Zweck, das Matching zwecks Information, außerhalb des reinen Austausches verfolgt wird. Daher scheidet hierfür eine eigenständige Verantwortlichkeit der Nutzerïnnen aus.

Soweit hinter der CA eine Behörde, zum Beispiel das Bundesministerium für Gesundheit (BMG) per gesetzlicher Zuweisung, oder eine andere staatliche Stelle, wie zum Beispiel das RKI, als Betreiberïn stehen wird, ist das Verhältnis zu den Nutzerïnnen nicht nur durch eine informationelle Machtasymmetrie, sondern auch durch ein Subordinationsverhältnis gekennzeichnet, welches für eine Verantwortlichkeit der öffentlichen Stelle spricht. Soweit die Betreiberïn entscheidet, warum und wie die Daten verarbeitet werden, liegt die faktische Entscheidungsmacht durch den Betrieb bei der Betreiberïn, die damit für die Verarbeitung verantwortlich ist. Dies gilt auch, wenn eine private Stelle als Betreiberïn der App auftritt. Ob es sich dabei gleichzeitig um die App-Herstellerïn handelt, ist unerheblich. Der App-Herstellerïn kommt nur dann Entscheidungsmacht zu, wenn sie über die wesentlichen Mittel und Zwecke der Verarbeitung entscheidet. Die App-Herstellerïn konfiguriert zwar das technische System und hat damit Einfluss auf dessen Wirkweise, jedoch entscheidet sie letztlich nicht über die Zwecke der tatsächlichen Verarbeitung, für die die App genutzt wird.

Werden die CA und der für die Nutzung erforderliche Server oder die Server von unterschiedlichen juristischen Personen unterhalten, so kommt es für die Verantwortlichkeit darauf an, wem für die Verarbeitungsvorgänge die tatsächliche Entscheidungsmacht zukommt. Dies ist abhängig vom Typ der CA (siehe Kapitel 1.1). Erfolgt das Matching auf dem oder den Servern einer Betreiberïn und entscheidet diese über das Verfahren des Matching und/oder der Benachrichtigung des Empfängers (Typ 1 und 2), oder speichert die Betreiberïn die ID-Listen und verarbeitet diese weiter, um beispiels-

weise daraus weitere, gegebenenfalls auch aggregierte Ergebnisse (etwa Statistiken) zu errechnen, so kommt ihr für diese Verarbeitungsvorgänge tatsächliche Entscheidungsmacht zu. Erfolgt das Matching auf den Endgeräten (Typ 3), spricht dies für eine tatsächliche Entscheidungsmacht und damit Verantwortlichkeit beim Betreiber der CA. Wird der Server von einer weiteren juristischen Person betrieben, so kommt in dieser Fallkonstellation eine Auftragsverarbeitung durch die Server-Betreiberïn in Betracht.

Ein Zugriff der Verantwortlichen auf die personenbezogenen Daten ist nicht erforderlich. Es reicht insofern, dass die Verantwortliche bestimmt, dass bzw. welche Kategorien von personenbezogenen Daten im Rahmen der App auf den Geräten der Nutzerïnnen verarbeitet werden.

Auch muss sich die Kontrolle der Verantwortlichen über die Verarbeitung nicht auf das gesamte Verfahren erstrecken; es reicht, dass sie sich auf bestimmte Verarbeitungsvorgänge bezieht und andere Vorgänge in die Verantwortlichkeit einer anderen Stelle fallen (vgl. EUGH, Fashion ID C-40/17, ECLI:EC:C:2019:629 Rn. 74).

Eine gemeinsame Verantwortlichkeit der Betreiberïnnen von CA und Server(n) liegt dann vor, wenn sie gemeinsam über Zwecke und Mittel der Verarbeitung entscheiden (Hartung Kühling und Buchner 2018, Art. 26 Rn. 11).

Eine Verantwortlichkeit der Nutzerïnnen im Rahmen einer gemeinsamen Verantwortlichkeit mit den Betreiberïnnen kommt nicht in Betracht. Als Begründung kann jedoch nicht der Ausschluss des sachlichen Anwendungsbereichs der DSGVO angeführt werden, der dann in Betracht käme, wenn die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten gem. Art. 2 Abs. 2 lit. c DSGVO erfolgt. Der Austausch der TempIDs stellt keine rein persönliche oder familiäre Tätigkeit dar, sondern dient den Zwecken des Infektionsschutzes beziehungsweise der Eindämmung der Pandemie (vgl. Kapitel 4.2). Letztlich kann diese Frage aber dahinstehen, denn zum Einen führt die Bejahung der ausschließlich persönlichen oder familiären Tätigkeit nicht zum Ausschluss der Verantwortlichkeit der Betreiberïn (vgl. EG 18 S. 3 DSGVO) und zum Anderen haben die Nutzerïnnen weder einen rechtlichen noch einen tatsächlichen Einfluss auf die Zwecksetzung und die Entscheidung, wie personenbezogene Daten auf ihren Geräten verarbeitet werden und sind auch darum nicht als Verantwortliche anzusehen.

5.3 Rechtsgrundlagen

Der Grundsatz der Rechtmäßigkeit setzt nach Art. 6 Abs. 1 DSGVO das Vorliegen von Rechtsgründen für die Verarbeitung voraus. Für jeden Verarbeitungszweck ist eine Rechtsgrundlage zu bestimmen.

Die Rechtsgrundlagen der DSGVO sind abschließend in Art. 6 Abs. 1 S. 1 DSGVO geregelt. Als Rechtsgrundlagen für die in Kapitel 5 beschriebenen Verarbeitungstätigkeiten kommen die folgenden Bestimmungen in Betracht:

- Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO;
- Vertrag nach Art. 6 Abs. 1 S. 1 lit. b DSGVO;
- Rechtliche Verpflichtung nach Art. 6 Abs. 1 S. 1 lit. c DSGVO
- Gesetzliche Aufgabe nach Art. 6 Abs. 1 S. 1 lit. e DSGVO iVm Bundesinfektionsschutzgesetz;
- Lebenswichtige Interessen der Betroffenen nach Art. 6 Abs. 1 S. 1 lit. d DSGVO;

– berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO.

Maßgeblich für die Wahl der Rechtsgrundlage ist die Rolle der Verantwortlichen, der Verarbeitungszweck und der Kontext der Verarbeitung (European Data Protection Board 2019a, Rn 18). Liegt die Verantwortlichkeit für die Verarbeitungstätigkeit bei einer öffentlichen Stelle wie dem RKI oder dem BMG, so lässt Art. 6 Abs. 1 S. 2 DSGVO ein berechtigtes Interesse als Rechtsgrundlage ausscheiden. Des Weiteren ist für die Bestimmung der geeigneten Rechtsgrundlage der Verarbeitungszweck und der Kontext der Verarbeitung zu berücksichtigen.

Für die Verarbeitung personenbezogener Daten, einschließlich der Verarbeitung von Gesundheitsdaten durch Gesundheitsbehörden oder andere Stellen, die in deren Auftrag handeln, kommen insbesondere Art. 6 Abs. 1 S. 1 lit. c und e iVm Art. 6 Abs. 3 lit. a, Art. 9 Abs. 2 lit. g und lit. i DSGVO in Betracht. Voraussetzung dafür ist u.a. dass die Verarbeitung der personenbezogenen Daten in den gesetzlichen Aufgabenbereich der Behörde nach Maßgabe des Art. 6 Abs. 3 S. 2, 3 DSGVO fällt, die Verarbeitung der personenbezogenen Daten erforderlich ist (siehe Kapitel 5.4.3) und die weiteren Bestimmungen der DSGVO und des sektorspezifischen Rechts eingehalten werden.

5.3.1 Einwilligung, Art. 6 Abs. 1 S. 1 lit. a DGSVO

Die in öffentlichen Ankündigungen mitgeteilten Informationen zur CA enthalten bisher den Hinweis, dass die Bürgerïnnen sich für eine Nutzung freiwillig entscheiden können. Bislang ist eine gesetzliche Normierung des Einsatzes und der Nutzung der CA, die eine freiwillige Nutzung ermöglichen, nicht erfolgt. Eine rechtskonforme Verarbeitung personenbezogener Daten im Zusammenhang mit der Nutzung der CA auf der Grundlage der Erteilung einer datenschutzrechtlichen Einwilligung kann nur unter der Bedingung erfolgen, dass diese den gesetzlichen Vorgaben entspricht. Daran bestehen erhebliche Bedenken im Hinblick auf die normativen Anforderungen als auch an die operative Umsetzung.

Im Hinblick auf die Möglichkeit Verarbeitungstätigkeiten auf die Rechtsgrundlage der Einwilligung aus Art. 6 Abs. 1 S. 1 lit. a DSGVO zu stützen, sind folgende Aspekte zu berücksichtigen:

– Die Nutzung der CA ist *ein* Bestandteil im Rahmen des Verfahrens (siehe Kapitel 4 zu den Verarbeitungstätigkeiten und Zwecken).

– Mit der Einwilligung in die Nutzung der App und der Verarbeitung personenbezogener Daten der Einwilligenden ist nicht automatisch eine Einwilligung in das (gesamte) Verfahren verbunden.

– Die Einwilligung in die Nutzung der App ist von der Einwilligung in die Übermittlung der TAN, d.h. der Authentisierung nach einer Positiv-Testung, an den Server und Übermittlung der eigenen Gesundheits-TempIDs zu trennen.

– Es bedarf eines Einwilligungsmanagements.

Soll die Verarbeitung personenbezogener Daten auf eine Einwilligung gestützt werden, so sind die Voraussetzungen aus Art. 6 Abs. 1 S. 1 lit. a iVm Art. 7 und Art. 4 Nr. 11 DSGVO. zu erfüllen. Art. 4 Nr. 11 DSGVO definiert die Einwilligung als eine

> »freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen

> eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.«

Die Freiwilligkeit setzt eine echte Wahlmöglichkeit für die Betroffene voraus Article 29 Data Protection Working Party 2018, S. 5, nur so erfüllt sie ihre Schutzwirkung. Zur Beurteilung der Wahlmöglichkeiten ist der Kontext, in dem die Einwilligung erteilt werden soll näher zu betrachten. Zweck der CA ist die Ermöglichung von Notifikationen über ein erhöhtes Infektionsrisiko aufgrund eines Kontaktes zu einer positiv getesteten Person, damit sich diese zur Eindämmung der Pandemie frühzeitig in Quarantäne begeben und selbst testen lassen kann. Gegen eine Freiwilligkeit spricht, wenn zwischen dem Verantwortlichen und den Betroffenen ein deutliches Machtgefälle besteht. Dies ist klassischerweise der Fall im im Über- und Unterordnungsverhältnis zwischen den Bürgerïnnen und der öffentlichen Hand (EG 43 DSGVO). Wird die Einwilligung gegenüber einer Behörde erteilt, wird grundsätzlich angenommen, dass diese nicht freiwillig erfolgt (Beweislast zulasten der Freiwilligkeit in EG 43 S. 1 DSGVO). Vielmehr muss im Einzelfall nachgewiesen werden, dass in der konkreten Situation das typischerweise bestehende Ungleichgewicht nicht zum Tragen kommt. An die Erteilung einer Einwilligung gegenüber einer Behörde sind daher besondere Anforderungen zu stellen (Bock in Specht und Mantz 2019, 570 Rn 27 f.). Diesem Ungleichgewicht soll dadurch begegnet werden, dass die Nutzung der App nicht verpflichtend erfolgt und keine normierten, direkten rechtlichen Konsequenzen nach sich zieht.

Die Abwesenheit unmittelbar normierter Nachteile im Falle der Nichtnutzung der App lässt jedoch nicht unmittelbar den Schluss zu, dass eine Einwilligung in die mit der Nutzung der App einhergehende Datenverarbeitung freiwillig im Sinne des Art. 7 Abs. 4 DSGVO ist. Im Kontext der Verarbeitung ist zu beachten, dass unter anderem die Frage der Lockerungen des Lockdowns von Regierungsvertreterïnnen ausdrücklich oder jedenfalls im Ergebnis mit dem Einsatz der App und einer möglichst weitreichenden Nutzung durch die Bevölkerung (mind. 60 %) verknüpft wird (Neuerer 2020). Tatsächlich wären damit als Konsequenz der Nichtnutzung die Verlängerung oder auch weitere Einschränkungen des öffentlichen Lebens und die Beschränkung von Grundrechten (Freizügigkeit) zu betrachten. Der Freiwilligkeit der Einwilligung steht insoweit ein erwartbares belastendes Verwaltungshandeln gegenüber. Die Besonderheit in diesem Fall liegt darin, dass sich das Verwaltungshandeln nicht gegen die einzelne Bürgerïn richtet, sondern im Form allgemeiner Freiheitsbeschränkungen unterschiedslos alle Bürgerïnnen betrifft. Es muss vor diesem Hintergrund jedenfalls die Möglichkeit berücksichtigt werden, dass sozialer Druck in nicht unerheblichem Umfang entstehen kann, sich den Erwartungen des sozialen Umfelds, des Staates oder der App-Betreiberïn entsprechend zu verhalten und die App zu nutzen, denn auch rechtlich nicht sanktionierte Verhaltensweisen können die Freiwilligkeit des Betroffenenverhaltens in Frage stellen, wenn sie einen abstrakten inneren Zwang auslösen (Heckmann/Paschke in Ehmann und Selmayr 2018, Art. 7 Rn. 51). Der Wunsch nach Rückkehr zu einem weitgehend normalisierten öffentlichen Leben ist verständlich. Die Bürgerïnnen werden sich dem kaum verschließen können.

Zur Förderung des Zwecks, der mit der hier betrachteten Datenverarbeitung verfolgt wird, könnten in der Folge sodann individuelle Lockerung der Freiheitsbeschränkungen verbunden werden und etwa der Zugang zu Spielplätzen, dem Arbeitsplatz oder der Schulbesuch von der Nutzung der App abhängig gemacht werden. Dieser soziale Druck scheint von Seiten der Behörden auch erwünscht (Randow 2020).

Hinzu kommt, dass eine realistische Alternative zur Nutzung der App und folglich

eine Möglichkeit, die mit ihr einhergehende Verarbeitung abzulehnen, nicht besteht. Eine freiwillige Testung großer Teile der Bevölkerung ist aus Kapazitätsgründen derzeit nicht möglich. Eine infizierte Person ist bereits ansteckend bevor COVID-19-Symptome auftreten. Sollen die Kontaktpersonen zur Einschränkung der Pandemie rechtzeitig gefunden werden, erfolgt dies herkömmlich durch die Gesundheitsämter mittels Fragebogen und Telefon. Ein digitales System, dass die Kontakte ermittelt und informiert wird vergleichsweise schneller sein. Dies erhöht den sozialen Druck für die Einzelne weiter, sich an dem Verfahren zu beteiligen. Weitere rechtliche oder jedenfalls faktische Nachteile könnten darin bestehen, dass der Zugang zu Tests bei Symptomen vom Nachweis des Kontakts mit einer nachgewiesen infizierten Person abhängig gemacht wird und die App als im Vergleich einzig zugängliches Mittel der Glaubhaftmachung verfügbar ist. Nicht nur diese unmittelbaren Folgen der Nichtnutzung, sondern bereits die vorhergehende Inaussichtstellung entsprechender Entwicklungen wirken sich bereits auf den Entscheidungsprozess für und gegen die Nutzung der App aus. Rein rechtlich greift die DSGVO diese Bedenken dadurch auf, dass sie die Freiwilligkeit einer Einwilligung gegenüber Behörden kategorisch zurückhaltend sieht und in Erwägungsgrund 43 S. 1 DSGVO klarstellt, dass in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, die Einwilligung keine gültige Rechtsgrundlage liefern kann. Insgesamt betrachtet handelt es sich bei der App um einen Baustein im Kontext staatlicher Pandemiebekämpfung und damit um ein Verwaltungshandeln, das verhältnismäßige Eingriffe zur Abwehr weitergehender Freiheitsbeschränkungen bezweckt. Insofern steht die Notwendigkeit der Nutzung der App im Kontext einer Eingriffsverwaltung. In diesem Zusammenhang wird die Einwilligung auch in der datenschutzrechtlichen Literatur verbreitet als Rechtsgrundlage abgelehnt (Heckmann/Paschke in Ehmann und Selmayr 2018, Art. 7 Rn. 53, siehe kritisch für den Bereich des Sozialrechts auch Hoffmann 2017).

Voraussetzung für eine wirksame Einwilligung ist des Weiteren deren Bestimmtheit. Personenbezogene Daten dürfen gem. Art. 5 Abs. 1 lit. b DSGVO nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Die Bekämpfung der Pandemie stellt ohne Zweifel einen legitimen Zweck dar, der in seiner Allgemeinheit aber unkonkret bleibt. Die Zweckbestimmung muss grundsätzlich so präzise wie möglich erfolgen und es muss sichergestellt sein, dass personenbezogene Daten nicht für Zwecke verarbeitet werden, mit denen die betroffene Person bei der Erhebung nicht rechnen musste (vgl. Kühling und Martini 2016, S. 51: »enges Verständnis«).

Wird mit der Bereitstellung der CA die schnelle Information von Personen, die mit infizierten Personen in Kontakt gekommen sind bezweckt, so dürfen über diesen Zweck hinausgehend keine weiteren Datenverarbeitungen erfolgen (siehe Kapitel 4.2).

Der Zweck, für die die Einwilligung erteilt werden soll, muss konkret beschrieben sein. Es soll damit gewährleistet werden, dass die Verantwortliche nicht im Nachhinein weitere Zwecke hinzufügt oder die Verarbeitungen ausweitet. Daher sind die Informationen, die der Betroffenen über den Zweck der Einwilligung mitzuteilen sind, klar von weiteren Informationen, die die Bearbeitung betreffen, zu trennen (Article 29 Data Protection Working Party 2018, S. 11).

Die Einwilligung ist für jeweils zusammenhängende Verarbeitungsvorgänge zu erteilen. Werden verschiedene Zwecke miteinander kombiniert, so ist die Einwilligung für jeden der Zwecke einzuholen (EG 32 S. 5 DSGVO). Für die Nutzung der App sind zwei Verarbeitungsaktivitäten zu unterscheiden. Zum Einen der Austausch der TempIDs

zwischen den Apps und zum Anderen die Übermittlung von TAN und Gesundheits-TempIDs an den Server im Falle einer Infektion (vgl. Kapitel 4). Beide Aktivitäten müssen durch eine Handlung der Nutzerïn angestoßen werden. Versteht man den Austausch der TempIDs als Voraussetzung für die Information über den Kontakt mit einer infizierten Person, kann sich die Einwilligung auf beide Vorgänge beziehen. Soweit der Nutzerïn die Möglichkeit gegeben werden soll, über die Weitergabe der Information ihrer Positiv-Testung frei zu entscheiden, sollte diese Wahlmöglichkeit auch in der Einwilligungserklärung klar zum Ausdruck kommen. Leitet die Nutzerïn die Information nicht an den Server weiter, kommt es auf die Zwecksetzung und die Ausgestaltung der Einwilligungserklärung an. Übermittelt die Nutzerïn die TAN nicht, so ist davon auszugehen, dass sie auch nicht mit der weiteren Verarbeitung der Information, dem Umstand positiver Testung, einverstanden ist.

Für die Wirksamkeit der Einwilligung muss die Verantwortliche nachweisen, dass es möglich ist, der Einwilligung zu widersprechen und dass die Einwilligung ohne negative Folgen widerrufen werden kann. Zwar entfaltet der Widerruf nur Folgen ex nunc, und damit ab dem Zeitpunkt seiner Erklärung, aber auch ab diesem Zeitpunkt muss es möglich sein, aus dem Verfahren auszusteigen. Für die Nutzung der CA ist bislang nicht dargelegt worden, welche Folgen ein Widerruf für die Betroffene hat. Es fehlen bislang insbesondere Informationen, wie mit einem Widerruf im Falle einer Infektion verfahren wird. Auch ist nicht geklärt, ob ein Widerruf technisch in der App überhaupt möglich ist oder wie er im Verfahren umgesetzt wird, auch weil ein Widerruf der zu einem Löschen der infektionsanzeigenden Daten ohne Personenbezug (iDoP) auf dem Server führt, das Risiko birgt, die grundrechtsschützende Wirkung der vorgesehenen Trennung, dh der Anonymisierung, zu unterlaufen. Vor dem Hintergrund der widerstreitenden Anforderungen kann eine rechtliche Abwägung nur im Hinblick auf eine konkrete operative Umsetzung vorgenommen werden.

Die Einwilligung muss informiert erteilt werden. Dazu hat die Verantwortliche die folgenden Informationen an die Betroffene zu geben: die Identität der Verantwortlichen, die Zwecke der Verarbeitung für die eine Einwilligung eingeholt werden soll, die Kategorien von Daten die verarbeitet werden sollen, das Recht auf Widerruf, soweit die Daten für eine automatisierte Entscheidungsfindung im Rahmen des Art. 22 Abs. 2 lit. c DSGVO genutzt werden, über die Nutzung und über die Risiken bei Übermittlungen in Drittstaaten, die nicht über ein vergleichbares Datenschutzniveau verfügen. Diese Informationen sollen nach Möglichkeit in einer klaren und einfachen Sprache zur Verfügung gestellt werden und leicht auffindbar sein und nicht zwischen anderem Text versteckt sein (Article 29 Data Protection Working Party 2018, S. 14). Informiert kann eine Einwilligung aber nur erfolgen, wenn die betroffene Person auch die Tragweite der Einwilligung, d.h. die Auswirkungen einschließlich der Risiken der Verarbeitung abschätzen kann (Buchner/Kühling in Kühling und Buchner 2018, Art. 4 Nr. 11 Rn. 5–12).

Muss im Rahmen der Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. f DSGVO die Verantwortliche ihre berechtigten Interessen mit denen der betroffenen Person sowie deren Grundrechten und Grundfreiheiten abwägen, so müssen bei einem durch die Rechtsgrundlagen vermittelten gleichwertigen Schutzniveau die Informationen der Verantwortlichen im Rahmen einer Einwilligung die betroffene Person in die Lage versetzten, diese Abwägung ebenfalls vornehmen zu können. Um die Bürde der Abwägung und damit das Risiko nicht vollständig auf die betroffene Person abzuwälzen, sind, ausgehend von der Verfahrensbeschreibung, die Grundrechtsrisiken für die Betroffene in klarer und einfacher Sprache darzustellen, um der betroffenen Person eine Abwägung der Grundrechtsrisiken gegenüber der Zweckerreichung zu ermöglichen (Rost 2018). Eine

solche Darstellung in klarer und einfacher Sprache erscheint im Hinblick auf die Komplexität des Verfahrens und den Auswirkungen des Einsatzes der CA, wie in Kapitel 4 und 7 dargestellt, kaum möglich. Die durch die Verarbeitung verursachte informationelle Machtasymmetrie zwischen der Verantwortlichen und der Betroffenen wird so nicht nur nicht ausgeglichen, sondern verstärkt. Dieses Ungleichgewicht könnte letztlich nur durch eine gesetzliche Regelung adressiert werden durch die, die Risiken der Verarbeitung aufgefangen werden.

Die Erteilung der Einwilligung muss eindeutig erfolgen. Im Sinne des Datenschutzes durch Voreinstellungen (Art. 25 Abs. 2 DSGVO) darf eine werksseitige Vorinstallation der App nur dann erfolgen, wenn diese von der Nutzerïn freigeschaltet werden muss. Zur Gewährleistung von Intervenierbarkeit durch Widerruf sollte die App leicht zu deaktivieren oder zu deinstallieren sein.

Die Erteilung einer Einwilligung von Kindern bedarf besonderer Maßnahmen. Es ist sicherzustellen, dass eine Nutzung der App für Kinder unter 16 Jahren nur bei Einwilligung eines Erziehungsberechtigen möglich ist. Die Berechtigung ist nachzuweisen.

Eine Einwilligung nach Art. 5 Abs. 3 ePrivacyRL ist ebenfalls nicht erforderlich, weil nur auf Daten des Endgeräts zugegriffen wird, die zur Erbringung des Dienstes notwendig sind.

5.3.2 Vertrag, Art. 6 Abs. 1 S. 1 lit. b DSGVO

Grundsätzlich kommt auch eine vertragliche Ausgestaltung des Nutzungsverhältnisses zwischen einer privaten App-Betreiberïn und einer Nutzerïn der App nach Art. 6 Abs. 1 S. 1 lit. b in Betracht, um iVm mit einer Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO in die Verarbeitung und Übermittlung von Gesundheitsdaten im Fall Typ Server Push Daten an Dritte/andere Nutzerïnnen zu übermitteln.

Denkbar wäre theoretisch, dass sich alle Nutzerïnnen gegenseitig dazu verpflichten, die jeweiligen erforderlichen Datenverarbeitungen durchzuführen und – auch jene betreffend Dritter – hinzunehmen. Gegen eine vertragliche Ausgestaltung spräche neben unklaren Haftungsrisiken aber vor allem, dass im Falle der Beteiligung zentraler staatlicher Betreiberïnnen wohl ein öffentlich-rechtlicher Vertrag iSd § 54 VwVfG zu schließen wäre, der gemäß § 57 VwVfG der Schriftform bedarf. Diese Formerfordernis dürfte im hier diskutierten Kontext ganz und gar unpraktikabel sein.

5.3.3 Allgemeine Voraussetzungen gesetzlicher Rechtsgrundlagen

Da die Nutzung der App mangels Freiwilligkeit nicht auf eine Einwilligung der Nutzerïnnen gestützt werden sollte, sowohl die Haftungsrisiken wie auch Formerfordernisse gegen eine Vertragslösung sprechen und vieles dafür spricht, dass die CA unter die Medizinprodukteverordnung fallen wird (European Commission 2020), ist die Gesetzgeberïn gut beraten, über eine gesetzliche Regelung für das Verfahren und den Einsatz der CA nachzudenken.

Auch bei einer gesetzlichen Regelung wird nicht ausgeschlossen, dass die Nutzung der CA selbst – allgemein oder nur für bestimmte Gruppen, etwa Nichtrisikogruppen – auf freiwilliger Basis erfolgt.

Auch kann eine gesetzliche Regelung vorsehen, dass etwa Mitglieder von Risikogruppen, die typischerweise nicht über ein Smartphone verfügen, mit einem geeigneten Gerät, auf dem ausschließlich die CA installiert ist und läuft, ausgestattet werden.

Vor allem erlaubt eine gesetzliche Regelung der Datenverarbeitung die Durchführung einer Gesetzgebungs-DSFA nach Art. 35 Abs. 10 DSGVO bereits zum Zeitpunkt

der Regulierung. Von dieser Möglichkeit sollte die Gesetzgeberïn Gebrauch machen.

5.3.4 Erfüllung einer rechtlichen Verpflichtung, Art. 6 Abs. 1 S. 1 lit. c DSGVO

Art. 6 Abs. 1 S. 1 lit. c DSGVO erfasst die aus Rechtsvorschriften folgenden Rechtspflichten. Die in der Rechtsvorschrift normierte Pflicht muss sich unmittelbar auf die Datenverarbeitung beziehen (EG 45 S. 1 DSGVO). Die Pflicht muss sich direkt an die datenschutzrechtlich Verantwortliche richten, also an die Stelle, die die Zwecke und Mittel der Verarbeitung bestimmt. Eine konkrete Rechtspflicht zum Betrieb einer CA besteht bislang nicht. Pflichten zur Erkennung von übertragbaren Krankheiten und Infektionen bei Personen sowie deren Bekämpfung und Eindämmung sind im Infektionsschutzgesetz (IfSG) geregelt. Bei SARS-CoV-2 handelt es sich um einen Krankheitserreger, d.h. um ein vermehrungsfähiges Agens, einen Virus, das bei Personen eine Infektion und übertragbare Krankheit, COVID-19, verursachen kann.

Die Information und Aufklärung der Allgemeinheit über die Gefahren übertragbarer Krankheiten und die Möglichkeiten zu deren Verhütung sind gem. § 3 S. 1 IfSG öffentliche Aufgaben, die im Infektionsschutzgesetz geregelt sind. Das IfSG dient der Prävention von Erkrankungen, die sich aufgrund ihres hohen Infektionsrisikos rasch auf große Bevölkerungsgruppen ausbreiten können und in Kombination mit ihrer Schwere somit ein großes Risiko für viele Personen darstellen.

§ 4 Abs. 1 S. 1 IfSG bestimmt das Robert-Koch-Institut (RKI) als nationale Behörde zur Vorbeugung übertragbarer Krankheiten sowie zur frühzeitigen Erkennung und Verhinderung der Weiterverbreitung von Infektionen. Die Aufgaben des Instituts schließen gem. § 4 Abs. 1 S. 2 IfSG auch die Entwicklung und Durchführung epidemiologischer und laborgestützter Analysen sowie Forschung zu Ursache, Diagnostik und Prävention übertragbarer Krankheiten ein. Weitere Aufgaben ergeben sich aus § 4 Abs. 2 IfSG; danach erstellt das RKI im Benehmen mit den jeweils zuständigen Bundesbehörden für Fachkreise als Maßnahme des vorbeugenden Gesundheitsschutzes Richtlinien, Empfehlungen, Merkblätter und sonstige Informationen zur Vorbeugung, Erkennung und Verhinderung der Weiterverbreitung übertragbarer Krankheiten (§ 4 Abs. 2 Nr. 1 IfSG) und wertet die Daten zu meldepflichtigen Krankheiten und meldepflichtigen Nachweisen von Krankheitserregern, die ihm nach diesem Gesetz und nach § 11 Absatz 5, § 16 Absatz 4 des IGV-Durchführungsgesetzes übermittelt worden sind, infektionsepidemiologisch aus (§ 4 Abs. 2 Nr. 2 IfSG). Hierbei handelt es sich um allgemeine Aufgabenbeschreibungen. Art. 6 Abs. 1 S. 1 lit. c DSGVO setzt jedoch voraus, dass sich der Verarbeitungszweck unmittelbar aus der Rechtspflicht ergibt (EG 45 DSGVO). Eine Pflicht zur App-basierten Information von Personen, die mit einer positiv getesteten Person in Kontakt gekommen sind, ergibt sich aus dem aktuellen Text des § 4 IfSG bisher jedoch nicht.

§ 4 Abs. 1a IfSG befasst sich konkret mit der durch SARS-CoV-2 verursachten Epidemie, jedoch sieht diese Regelung lediglich eine Berichtspflicht vor und regelt ebenfalls nicht den Einsatz oder ermächtigt zum Betrieb einer CA.

Aus § 6 iVm mit § 9 IfSG ergibt sich lediglich eine Meldepflicht für Infektionskrankheiten, jedoch keine konkrete Pflicht zur Warnung von möglicherweise infizierten Personen oder zum Betrieb einer CA.

§ 13 IfSG ermächtigt das RKI zur Überwachung übertragbarer Krankheiten in Zusammenarbeit mit ausgewählten Einrichtungen der Gesundheitsvorsorge oder -versorgung durch sogenannten Sentinel-Erhebungen. Diese dienen der Erfassung anonymer, stichprobenartiger Daten, durch die auf die Verbreitung von Infektionskrank-

heiten geschlossen werden soll. Der Zweck des Betriebs einer CA, die Ermöglichung der möglichst frühzeitigen Warnung einer Person, wird davon nicht erfasst.

§ 14 IfSG regelt ein elektronisches Melde- und Informationssystem. Aufgabe dieses Systems ist die Ermöglichung der elektronischen Einmeldung von melde- und benachrichtigungspflichtigen Tatbeständen nach dem IfSG durch meldepflichtige Personen und Stellen. Auch diese Norm erfasst damit nicht die Zwecke der Verarbeitung personenbezogener Daten durch eine CA, denn die rechtliche Verpflichtung muss gerade die Verarbeitung der personenbezogenen Daten durch die CA zur Erfüllung der rechtlichen Verpflichtung erforderlich machen. Damit soll sichergestellt werden, dass die Verantwortliche das rechtlich vorgegebene Ziel nicht zum Anlass nimmt, weitere personenbezogene Daten oder diese zu anderen Zwecken zu verarbeiten (Article 29 Data Protection Working Party 2018, S. 11).

Die klare und präzise Festlegung zumindest des Verarbeitungszwecks ist aber Voraussetzung, um eine rechtliche Verpflichtung zur Verarbeitung personenbezogener Daten zu schaffen (EG 41 DSGVO), auch wenn nicht zwingend jeder einzelne Verarbeitungsvorgang durch ein spezifisches Gesetz geregelt werden muss. EG 41 DS-GVO stellt insofern klar, dass die Verfassungsordnung des betreffenden Mitgliedstaates unberührt bleibt. Dazu gehört in der Rechtstradition des deutschen Grundgesetzes auch der Wesentlichkeits- und Bestimmtheitsgrundsatz, weshalb jedenfalls der deutsche Gesetzgeber gehalten sein wird, die wesentlichen Verarbeitungsziele und -schritte der CA selbst zu regeln. Diese Voraussetzungen werden durch keine der Normen des IfSG für ein CA-Verfahren oder den Betrieb einer CA erfüllt.

Gem. Art. 6 Abs. 3 S. 4 DSGVO muss die Rechtsgrundlage ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen. Regelbeispiele ergeben sich aus 9 Abs. 2 lit. h und i sowie 23 lit. e DSGVO. Die Regelung muss iSd Art. 5 Abs. 1 lit. b DSGVO bestimmt sein, d.h. ihr Regelungsinhalt muss sich klar und präzise aus der Rechtsvorschrift ergeben.

§ 13 Abs. 1 S. 1 ermächtigt den Bund und die Länder zur Überwachung übertragbarer Krankheiten weitere Formen der epidemiologischen Überwachung durchzuführen und durch Verordnung zu regeln.

Soll das RKI mit dem Betrieb der CA selbst oder mit der Möglichkeit, eine Auftragsverarbeiterïn einzubinden, betraut werden, so wären hierfür die rechtlichen Voraussetzungen im IfSG zu schaffen (§ 14 Abs. 8 IfSG) und sollten weitere Bestimmungen, insbesondere technische Vorgaben, in einer Ausführungsverordnung geregelt werden. Insbesondere muss bestimmt werden, »welche funktionalen und technischen Vorgaben einschließlich eines Sicherheitskonzepts dem elektronischen Melde- und Informationssystem zugrunde liegen müssen« (§ 14 Abs. 8 Nr. 4 IfSG), die den Anforderungen der DSGVO genügt. Eine solche Verordnung hat das zuständige Ministerium bislang nicht erlassen. Sie ist aber erforderlich.

5.3.5 Wahrnehmung einer Aufgabe im öffentlichen Interesse, Art. 6 Abs. 1 S. 1 lit. e DSGVO

Soll der Betrieb der CA auf Art. 6 Abs.1 S. 1 lit. e DSGVO gestützt werden, so müssen die Zwecke des Betriebs einer CA im öffentlichen Interesse liegen oder in Ausübung öffentlicher Gewalt erfolgen, die der Verantwortlichen übertragen wurde.

Der Zweck, die Eingrenzung der COVID-19-Pandemie durch eine möglichst frühzeitige Information über einen Kontakt mit einer positiv getesteten Person und damit eine frühzeitige Warnung vor einer möglichen Ansteckung, liegt ohne Zweifel im öffentlichen Interesse.

Die Verantwortlichkeit kann in öffentlicher Gewalt durch eine Behörde, eine andere öffentlich-rechtliche Einrichtung oder durch eine Einrichtung des privaten Rechts (Beliehene) ausgeübt werden. Erforderlich ist dafür die Übertragung einer entsprechende Befugnis zur Durchsetzung der im öffentlichen Interesse bestehenden Aufgabe.

Die weiteren Voraussetzungen des Art. 6 Abs. 1 S. 1 lit. e DSGVO decken sich mit denen der Rechtsgrundlage aus Art. 6 Abs. 1 S. 1 lit. c DSGVO. So muss die im öffentlichen Interesse liegende Aufgabe durch Rechtsvorschrift definiert werden. Die Warnung vor der Ansteckung mit einer infektiösen Krankheit und Eindämmung einer Pandemie wird zwar grundsätzlich vom Infektionsschutzgesetz gefasst, der Betrieb und Einsatz einer App zur Information über Kontakte mit einer infizierten Person ist jedoch nicht durch Rechtsvorschrift geregelt.

Eine gesetzliche Regelung, die die Verarbeitung von personenbezogenen Gesundheitsdaten im Rahmen einer CA Typ 3 (siehe Kapitel 1.1) ermöglicht mit dem Zweck, die Ausbreitung von COVID-19 einzudämmen, um das Gesundheitssystem nicht zu überlasten, muss dafür verhältnismäßige Regelungen enthalten, die die Verarbeitung personenbezogener Daten und insbesondere die Verarbeitung von Gesundheitsdaten auf ein angemessenes Maß minimiert. Eine solche Verarbeitung darf nicht zu einer allgemeinen und systematischen Erfassung, Speicherung und weiteren Verarbeitung von personenbezogenen Daten führen. Die Art und Weise der Verarbeitung muss für die Erreichung der Zwecke geeignet sein, und es dürfen nicht gleich geeignete mildere Mittel für die Erreichung der Zwecke zur Verfügung stehen. Die spezifische Rolle, die die Behörde als Verantwortliche der Datenverarbeitung übernimmt, darf nicht sachfremd sein und sollte in ihren Aufgabenbereich passen.

5.3.6 Schutz lebenswichtiger Interessen, Art. 6 Abs. 1 S. 1 lit. d DSGVO

Als Rechtsgrundlage könnte auch Art. 6 Abs. 1 S. 1 lit. d DSGVO infrage kommen, die dem Schutz lebenswichtiger Interessen der Betroffenen oder einer anderen natürlichen Person dient. Dabei handelt es sich um einen Auffangtatbestand als Ersatz für die Einwilligung, wenn diese unter den konkreten Umständen nicht erteilt werden kann, ihre Erteilung aber andererseits zu erwarten wäre (vgl. Albers in Wolf und Brink 2017, Rn. 37), vergleichbar etwa zur antizipierten Einwilligung im Falle einer Bewusstlosigkeit im Bereich ärztlicher Heileingriffe. Eine solche Konstellation ist vorliegend aber nicht gegeben. Auch dem Schutz eines lebenswichtigen Interesses einer anderen natürlichen Person dient die Datenverarbeitung nicht, weil die App und ihre Verwendung nicht vor Ansteckung schützt. Sie ist auch nicht erforderlich, denn, wie EG 46 DSGVO ausführt, soll dieser Erlaubnistatbestand nur greifen, wenn offensichtlich kein anderer Erlaubnistatbestand einschlägig ist, und ein solcher Erlaubnistatbestand liegt hier mit der Wahrnehmung einer Aufgabe im öffentlichen Interesse nach Art. 6 Abs. 1 S. 1 lit. e DSGVO vor.

5.4 Verhältnismäßigkeit

Für alle Rechtsgrundlagen gilt, dass die Verarbeitung personenbezogener Daten in Anbetracht der angestrebten Zwecke verhältnismäßig bzw angemessen sein muss. Dies formulieren die Rechtsgrundlagen der DSGVO teils ausdrücklich, etwa im Bereich der Schaffung staatlicher Verarbeitungsregelungen, vgl. Art. 6 Abs. 3 S. 4 DSGVO, und teilweise folgt dies schlicht aus der allgemeinen Vorgaben des Art. 5 Abs. 1 DSGVO.

Verhältnismäßig ist eine Verarbeitung nur, wenn ohne sie der Zweck nicht, nicht sicher oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Dies ist nach

objektiven Kriterien zu beurteilen. Es muss ein Zusammenhang zwischen den Daten und dem mit der Verarbeitung verfolgten Zweck bestehen (Heberlein in Ehmann und Selmayr 2018, Art. 6 Rn. 23).

Die Prüfung, ob dieser Zusammenhang im Einzelfall vorliegt oder nicht, ist anspruchsvoll. Sie setzt erstens eine Beschreibung des semantischen Gehalts der Informationen und der gegebenenfalls mit ihr geplanten Verarbeitung voraus, zweitens eine Beschreibung des Zwecks der Verarbeitung und drittens eine Darstellung des Grades der Abhängigkeit, mit dem die betreffende Zweckerreichung von der konkreten Verarbeitung der betreffenden personenbezogenen Daten abhängt, in einer Form, der diesen Grad der Abhängigkeit objektiv feststellbar und rational diskutierbar macht (Podlech 1982, 455f.).

In Fällen, in denen verschiedene gegenläufige Grundrechte gegeneinander abgewogen werden, muss diese Abwägung immer in Bezug auf ganz konkrete Verarbeitungen und ihre konkreten Ausgestaltungen erfolgen. Bevor eine politische Entscheidung über die gesetzliche Regelung, mit der der konkrete Zweck gesetzt und legitimiert wird sowie die dafür einzusetzenden Verarbeitungen bestimmt werden, getroffen werden kann, sind die Zwecke, die Verarbeitungen und die Zusammenhänge zwischen beiden nicht nur rechtlich, sondern auch fachlich zu fundiert zu diskutieren, denn sowohl die Bestimmung der erforderlichen Konkretheit des Zweckes als auch die der Verarbeitungen stellt eine Herausforderung dar (vgl. Härting 2020).

Der Grundsatz der Verhältnismäßigkeit erfordert, dass eine Verarbeitung personenbezogner Daten

- einem legitimen Zweck dient,
- geeignet ist, diesen Zweck zu erreichen,
- erforderlich ist, diesen Zweck zu erreichen (es also kein milderes, gleich effektives Mittel gibt), und
- angemessen, d.h verhältnismäßig im engeren Sinne, ist.

Eine Verarbeitung ist dann legitim, wenn ihr Zweck grundsätzlich im Bereich der dem Staate übertragenen Aufgaben liegt. Geeignet ist sie, wenn sie diesem Zweck grundsätzlich kausal dienen kann. Erforderlich ist sie, wenn kein milderes Mittel geeignet ist, diesem Zweck vergleichbar effektiv zu dienen. Angemessen — oder verhältnismäßig im engeren Sinne — ist eine Verarbeitung, wenn die Schwere der Grundrechtseingriffe bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht. Dies setzt eine Rechtsgüterabwägung voraus. Diese ist niemals nur rechtlich abhandelbar, sondern hat immer auch eine politische Dimension.

5.4.1 Legitimer Zweck

Der übergeordnete Zweck (siehe Kapitel 4.2) der Corona-Apps ist in der Regel jedenfalls mittelbar angesiedelt beim Schutz des Lebens und der körperlichen Unversehrtheit von Personen während einer Pandemie; sie dient also insgesamt gesehen der Pandemieeindämmung und -steuerung, konkret derzeit der Verzögerung von Neuansteckungen, um das Gesundheitswesen nicht über seine Leistungsfähigkeit zu belasten. Dieses Ziel können Individuen nicht allein verfolgen, daher ist es ein legitimer Zweck, der als Grundlage für eine rechtlichen Verpflichtung oder die Wahrnehmung als Aufgabe im öffentlichen Interesse dienen kann (BVerfG 2020, Rn 14).

Da die Abwägung im konkreten Fall erfolgen muss, sollen im Rahmen dieser DSFA folgende Zwecke beispielhaft betrachtet werden

- Zweck A sei die Informierung potentiell Infizierter, also die Warnung an Personen, die mit Infizierten Kontakt hatten, sodass diese sich in Quarantäne begeben können.
- Zweck B sei an dieser Stelle die allgemeine Überprüfung der Einhaltung von Ausgangsbeschränkungen, um politisches Handeln zu evaluieren.

Die Beispielzwecke können dabei durch den Einsatz jeweils verschiedener Technik verfolgt werden oder aber ohne Technikeinsatz. Die Zwecksetzung an sich ist allerdings keine technische Frage.

5.4.2 Geeignetheit

Die Frage der Geeignetheit der Verarbeitung hat eine technische Dimension, denn wenn eine bestimmte Technologie dem Zweck gar nicht dienen kann, so darf sie auch nicht eingesetzt werden.

Zweck A: Eine technische Evaluation von GPS- oder Mobilfunk-Metadaten ergibt, dass diese Daten für die Feststellung epidemiologisch relevanter Kontaktereignisse nicht genau genug sind. Daher scheiden diese Technologien aus. Nahbereichstechnologien wie etwa Bluetooth hingegen sind geeignet, weil sie u.a. sogar für Entfernungsmessungen im Meterbereich gedacht sind.

Zweck B: Zur Erstellung allgemeiner Bewegungsstatistiken einer Bevölkerung, so wie sie für Beispiel B benötigt werden, würden GPS- oder Mobilfunk-Metadaten technisch geeignet sein. Die Nahbereichstechnologien wiederum sind nur bedingt geeignet, weil sie nicht ohne weiteres einen Ortsbezug aufweisen. Ebenfalls geeignet wären aggregierte Daten, also zusammengefasste und rein statistische Daten, die aus GPS-, Mobilfunkmeta- oder Nahbereichsdaten errechnet werden können.

5.4.3 Erforderlichkeit

Die Erforderlichkeit ist in vielen datenschutzrechtlichen Rechtsgrundlagen des Art. 6 Abs. 1 S. 1 DSGVO eine der wesentlichen Tatbestandsvoraussetzungen. Bei der Betrachtung der Erforderlichkeit einer Verarbeitung ist eine technische Dimension zu berücksichtigen. Kann ein Zweck auch mit »milderen« technischen Mitteln erreicht werden, weil er – technisch bedingt – eine geringere Eingriffsintensität in Grundrechte aufweist, so ist das mildere Mittel zu wählen und das aktuell betrachtete Mittel nicht einzusetzen. Um zu evaluieren, ob es ein milderes Mittel gibt bzw. was ein milderes Mittel sein kann, wird in der Regel eine technische Betrachtung erforderlich sein. Bei dieser Betrachtung sind dann auch die Vorgaben aus Artikel 25 DSGVO (Datenschutz durch Technikgestaltung) zu berücksichtigen. Dies bedeutet u.a., dass Technologien dem Stand der Technik entsprechend zu berücksichtigen sind und der Grundsatz der Datenminimierung beachtet wird.

Zweck A: Der Einsatz von Nahbereichstechnologien wie etwa Bluetooth könnte erforderlich sein, wenn etwa die Aufgabe der Gesundheitsämter, Infektionsketten schnell und effizient aufzudecken, mit Hilfe einer App weit schneller und genauer erfüllt werden könnte als durch Fragebögen und Telefonate.

Zweck B: Für die allgemeine Überprüfung der Einhaltung von Ausgangsbeschränkungen sind keinerlei Einzeldaten mit Personenbezug notwendig, weshalb nur aggregiert-statistische Daten als milderes Mittel in Frage kommen. Detailliertere Daten, wie

beispielsweise konkrete Kontaktereignisdaten, individuelle GPS-Messungen oder andere Ortsdaten scheiden an dieser Stelle aus, da sie eingriffsintensiver, aber nicht zielführender sind.

5.4.4 Angemessenheit

Eine Verarbeitung ist zur Erreichung eines Zweckes nur angemessen, wenn die konkrete Interessenabwägung im Rahmen einer Zweck-Mittel-Relation zugunsten der Verantwortlichen ausfällt. Es sind daher die Interessen der Betroffenen mit den Interessen der Verantwortlichen an der Verarbeitung abzuwägen. In diese Abwägung sind auch gesamtgesellschaftliche Auswirkungen und »Nebenwirkungen« einzubeziehen. Das können medizinische Fragestellungen sein, aber auch soziale, wirtschaftliche oder psychologische, wobei auch diese jeweils miteineander verbunden sind.

Zweck A: Aus technischer Sicht kann Zweck A – wenn überhaupt – mit Nahbereichstechnologien erreicht werden. Die Angemessenheit hängt in diesem Beispiel an technischen Implementationsdetails. Selbst kleine Änderungen können hier zu einem unterschiedlichen Abwägungsergebnis führen.

Zweck B: Der Zweck B kann aus technischer Sicht allein mit aggregierten Daten umgesetzt werden. Es ist jedenfalls nicht möglich, darüber hinaus Pauschalaussagen zu machen, denn die Eingriffsintensität hängt ganz wesentlich von der konkreten technischen Implementierung ab, wie die aktuelle Diskussion um das PEPP-PT-Framework und die dezentralisierte DP-3T-Implementation zeigt.

Nicht zuletzt ist es relevant, ob das konkrete Ergebnis des App-Einsatzes überhaupt im Verhältnis zu den eingeschränkten Rechten steht. Bei experimentellen Apps wie den Corona-Tracing-App-Entwürfen ist dies besonders heikel, da deren Nutzen derzeit nicht abschätzbar ist. Der – bislang nur theoretisch modellierte – Effekt ist erst bei einer Nutzung durch mindestens 60% der Bevölkerung zu erwarten. Erkenntnisse aus Singapur mögen dafür instruktiv sein. Allerdings hatten dort nur 13% der Personen die individualisierte TraceTogether-App installiert. Die weiteren abwägungsrelevanten Aspekte werden ausführlich in der Schwellwertanalyse betrachtet (vgl. Kapitel 6).

5.5 Informationspflichten

Um die Grundsätze der Verarbeitung aus Art. 5 Abs. 1 DSGVO einzuhalten, hat die Verantwortliche dafür Sorge zu tragen, dass die Verarbeitung in einer für die betroffene Person nachvollziehbaren Weise erfolgt. Nachvollziehbarkeit wird vor allem durch die Erfüllung der Informationspflichten sichergestellt. Daher hat die Verantwortliche betroffenen Personen alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln (Art. 12 Abs. 1 S. 1 DSGVO). Dies sollte in einer Datenschutzerklärung geschehen, die aus der App heraus zugänglich ist.

Dazu gehören insbesondere Informationen über die Zwecke der Verarbeitung, die dafür eingesetzten Mittel, insbesondere die Dauer der Speicherung von personenbezogenen Daten, Datenübermittlungen und deren Empfängerïnnen, sowie darüber, wie die Betroffenen ihre Betroffenenrechte gegenüber der Verantwortlichen effektiv ausüben können, auch unter Inanspruchnahme der zuständigen Datenschutzaufsichtsbehörde.

5.6 Technische und organisatorische Maßnahmen

Art. 24 Abs. 1 DSGVO verlangt, dass die Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen (TOMs) umsetzt, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung datenschutzkonform ist. Datenschutzkonform ist sie, wenn sie die Datenschutzgrundsätze nach Art. 5 DSGVO erfüllt, die Anforderungen nach Art. 32 DSGVO wirksam umsetzt, die Betroffenenrechte von Art. 12 bis 22 DSGVO wirksam gewährleistet, dies durch Technikgestaltung und Voreinstellungen umsetzt und durch Datenschutzmanagement begleitet.

Für die umzusetzenden technischen und organisatorischen Maßnahmen siehe Kapitel 8.

Kapitel 6

Durchführung der Schwellwertanalyse

Der Zweck einer Schwellwertanalyse besteht darin, die Höhe des Risikos einer Verarbeitungstätigkeit für Betroffene zu bestimmen. Wenn für Betroffene ein hohes Risiko für die Rechte und Freiheiten besteht, sieht Art. 35 DSGVO vor, dass die Verantwortliche eine Datenschutz-Folgenabschätzung durchführen muss.

Die DSGVO unterscheidet zwei Risikostufen, nämlich ein geringes/normales Risiko und hohes Risiko. Entsprechend der Höhe des Risikos muss die Verarbeitung in Bezug auf die Intensität des Grundrechteeingriffs a) besonders umsichtig gestaltet werden, und es müssen b) gesteigert wirkungsvolle Schutzmaßnahmen sorgfältig spezifiziert und implementiert sowie prüf- und steuerbar betrieben werden. Weil allein die Tatsache der Verarbeitung von personenbezogenen Daten ein in der Regel normales Risiko für die Betroffenen darstellt, müssen in jedem Falle Schutzmaßnahmen für die eingesetzten Mittel der Datenverarbeitung getroffenen werden. Diese Maßnahmen müssen sicherstellen, dass die operativen Anforderungen an eine Verarbeitungstätigkeit aus den Art. 5, 24, 25, 32 DSGVO erfüllt werden.

Zur Bestimmung der Risikostufe für die vorliegende Verarbeitungstätigkeit werden drei Kriterienbündel herangezogen: a) Art. 9 DSGVO, b) Art. 25 DSGVO sowie c) die Liste aus dem Arbeitspapier 248 der Art. 29-Gruppe (Article 29 Data Protection Working Party 2017).

a) Art. 9 DSGVOdas listet besondere »Kategorien personenbezogener Daten« auf, zu denen »Gesundheitsdaten« zählen. Die Verarbeitung dieser Art besonderer Daten ist grundsätzlich untersagt und ausschließlich unter den im Gesetz aufgeführten Bedingungen zulässig. Für die Umsetzung in der Praxis bedeutet dies, dass mit der Verarbeitung dieses Typs von Daten ein hohes Risiko dafür besteht, dass die gesteigerten Anforderungen der DSGVO nicht intensiviert im Sinne der Betroffenen erfüllt werden.

Die Corona-App (CA) selber erhebt nur Distanzdaten zwischen Smartphones. Solange die Person nicht als infiziert diagnostiziert und ihr eine TAN ausgehängt wurde, handelt es sich nicht um Gesundheitsdaten. Mit dem Erhalt der TAN werden aus der TempID in der App besonders schützenswerte Gesundheitsdaten.

b) Art. 25 DSGVO gibt mehrere Kriterien vor, mit denen nicht das Risiko, das von Daten, sondern das von einer Verarbeitungstätigkeit ausgeht, festzustellen ist. Zu diesem Kriterien gehören die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und die Schwere, die mit den Risiken für die Rechte und Freiheiten natürlicher Personen einhergehen.

Die Art der Verarbeitung bezieht sich auf die Form der Datenverarbeitung. Im vorliegenden Fall werden aus einer Vielz.ahl von Distanzdaten auf der Basis von Heuristiken Kontaktereignisse berechnet, denen dann ein Exponierungscharakter zugeschrieben wird, aus dem sich dann schwerwiegende Rechts- und faktische Folgen für die Betroffenen ergeben, wie etwa die Pflicht zur Selbstquarantäne.

Der Umfang der Verarbeitung betrifft jede Person, die ein Smartphone mit installierter App bei sich trägt. Vor dem Hintergrund der Erwartung, dass mindestens 60% der Bürgerïnnen an diesem Verfahren teilnehmen, damit es epidemiologische Schutzwirkung entfalten kann, und des damit einhergehenden sozialen Drucks zur Nutzung, ist davon auszugehen, dass diese Verarbeitung viele Millionen Personen betrifft.

Die Umstände stellen auf den Kontext der Datenverarbeitung ab. Diese Datenverarbeitung ist geeignet, Personen mit bestimmten Eigenschaften, beispielsweise weil sie alt sind oder weil sie mit dem Corona-Virus infiziert sind, zu diskriminieren. Denkbar ist zudem, dass von der Verantwortlichen oder Betreiberïnnen des Verfahrens oder von der politischen Führung im Nachgang zusätzliche Kriterien festgelegt werden, mit denen weitere Typen von Personen »gefiltert« und dann kontrolliert oder gesteuert werden.

Der Zweck der Verarbeitung durch die Corona-App besteht darin, Personen zu erkennen und zu separieren, um Einfluss auf ihr Verhalten nehmen zu können.

Die Eintrittswahrscheinlichkeit, dass Personen mit diesem Verfahren gefunden werden, ist hoch, es ist der Zweck dieser Verarbeitung, bestimmte Typen von Personen zu finden. Außerdem besteht ein hohes Risiko beziehungsweise eine hohe Eintrittswahrscheinlichkeit, dass das Verfahren Personen herausfiltert, die nicht Corona-infiziert sind, aber trotzdem, anhand eines Anscheinsbeweis, zumindest zeitweise starke Eingriffe in ihre Grundrechte erdulden müssen.

c) Als dritte Hilfestellung zur Feststellung der Risikostufe wird die »Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist« herangezogen (DSK Liste VT), die wiederum auf die »Guidelines on Data Protection Impact Assessment« der Artikel-29-Gruppe verweist (Article 29 Data Protection Working Party 2017). In diesem Arbeitspapier werden neun verschiedene Kriterien aufgelistet, um zur Entscheidung über die Risikostufe zu gelangen. Die Datenschutzaufsichtsbehörden in der EU haben sich darauf verständigt, dass für die Fälle ein »wahrscheinlich hohes Risiko« vorliegt, wenn mindestens zwei Kriterien aus dieser Liste zutreffen:

1. »Evaluation or scoring, including profiling and predicting …«,
2. »Automated-decision making with legal or similar significant effect …«,
3. »Systematic monitoring: processing used to observe, monitor or control data subjects …«,
4. »Sensitive data or data of a highly personal nature …«,
5. »Data processed on a large scale …«,
6. »Matching or combining datasets, for example originating from two or more data processing operations …«,
7. »Data concerning vulnerable data subjects: …«,
8. »Innovative use or applying new technological or organisational solutions, …«,
9. »When the processing in itself prevents data subjects from exercising a right or using a service or a contract (Article 22 and recital 91) …«.

(siehe Article 29 Data Protection Working Party 2017)

Die letzten sieben Kriterien dieser Liste treffen, wie oben kurz ausgeführt, auf dieses Verfahren zu. Das Ergebnis der Schwellwertanalyse lautet somit, dass für diese Verarbeitungstätigkeit eine Datenschutz-Folgenabschätzung nach Art. 35 aufgrund eines hohen Risikos für die Betroffenen durchzuführen ist.

Kapitel 7

Schwachstellen und Risiken

Im Folgenden wird eine Auswahl relevanter Angriffsszenarien auf das Bluetooth-basierte System zur Nachverfolgung von Kontaktereignissen (PEPP-PT, DP-3T) präsentiert. Die Auflistung ist nach der primären Risikoquelle sortiert. Wenn ein Angriffsszenario unterschiedliche Risikoquellen besitzt, orientieren wir uns primär an den Akteuren, denen das Angriffsszenario am wahrscheinlichsten zuzutrauen ist und/oder von denen im Zusammenhang mit dem jeweiligen Angriff das größte Schadenspotenzial ausgeht. Innerhalb der drei Abschnitte wurden die Szenarien in absteigender Reihenfolge ihres geschätzten Risikos aufgelistet.[1]

7.1 Angriffe durch Betreiber, Hersteller und Behörden

Angriff A1: Gefahr falscher Positiver: Transparenz und Anfechtbarkeit der automatisiert auferlegten Selbst-Isolation

Angreiferïn: Betreiber / Behörden Die durch die Corona-App verordnete Selbst-

Isolation entspricht einer automatisierten Entscheidung mit rechtlichen Folgen. Art. 22 DSGVO spricht Nutzerïnnen in diesem Fall ein Recht auf Anfechtung der Entscheidung zu. Das ist besonders relevant bei falsch positiven Expositionsmessungen: War zum Beispiel Person A von einer infizierten Person B durch die Wand zwischen ihren Wohnungen getrennt, kann durch das Tracing-System ein nichtvalides Expositionsereignis festgestellt werden. Ähnliches ist denkbar über Passagierïnnen in benachbarten Zugabteilen, diesseits und jenseits der Fensterscheiben von Verkehrsmitteln, infizierten Bewohnerïnnen von Erdgeschosswohnung, vorbeilaufenden Passantïnnen, liegengelassenen Smartphones und sogar fehlerhafter Positivtests von Laboren etc.

- Mit der unweigerlich gegebenen Gefahr nichtvalider Expositionsmessungen ist das Risiko verbunden, dass Nutzerïnnen – potenziell auch mehrfach nacheinander – zu unrecht isoliert werden, mit erheblichen wirtschaftlichen und sozialen Folgen für die Betroffenen.

- Dieses Risiko kann nur über eine effektive Struktur der Anfechtbarkeit kontrolliert werden. Fehlt eine Anfechtungsmöglichkeit, könnte die Akzeptanz des Systems leiden, weil seine Entscheidungen als willkürlich erlebt werden. Sozialpsychologisch wäre es vorstellbar, dass einige Nutzerïnnen sich absichtlich anzustecken suchen, um durch erworbene Immunität in der Zukunft nicht jederzeit die Isolation fürchten zu müssen.

[1] Die Auflistung der Risiken kann keine Vollständigkeit beanspruchen. Bei einem sehr hohen Anspruch an die Vollständigkeit der Analyse und Bearbeitung von Risiken wären mindestens acht Risikotypen im Detail zu unterscheiden und es müssten auch diejenigen Risiken angesprochen werden, die durch die Implementation von Schutzmaßnahmen wiederum zusätzlich bzw. neu entstehen können (Rost 2018).

Aufgrund der Vielzahl denkbarer nichtvalider Expositionsmessungen durch räumliche Nähe bei gleichzeitiger räumlicher Barriere zwischen den Geräten (Wand zwischen Wohnungen, Fensterscheiben etc.) sowie aufgrund der nicht geplanten Anfechtbarkeit ist das mit dieser Schwachstelle verbundene **Risiko als sehr hoch einzuschätzen.**

Angriff A2: Behavioral Profiling und Compliance Scoring bei Infizierten

Angreiferïn: Behörden / Organisationen / Gesundheitssystem / Sozialträger

Die Betreiber können, auch im Rahmen epidemiologischer Studien, die Kontakthistorien infizierter Nutzerïnnen dazu verwenden, ein Verhaltensscoring zu erstellen: Wie viel oder wenig ist die Person mit anderen in Kontakt getreten? Hat sie sich besonders risikofreudig oder gar fahrlässig verhalten? Zu welchem Grade hat sie sich an die geltenden Kontaktregelungen gehalten? Ein behördliches Interesse an solchen Auswertungen ist zu erwarten, da die Corona-App höchstwahrscheinlich in einem Kontext zum Einsatz kommt, in dem immer noch partielle Kontaktbeschränkungen gelten; nach einem Instrumentarium für Compliance-Studien zu suchen, ist daher naheliegend.

Hieraus leiten sich ein kollektives und ein individuelles Risiko ab:

- In einer allgemeinen Variante dieses Angriffs erfolgt das Scoring anonym: Es könnten damit statistische Untersuchungen und statistische Verhaltensprofile hinsichtlich der Compliance mit den Kontaktauflagen und des Risikoverhaltens ermittelt werden. Man wird dies leicht mit dem Zweck wissenschaftlicher epidemiologischer Untersuchung rechtfertigen können. Allerdings können die Verhaltensprofile, wenn sie mit weiteren, demographischen und sozio-ökonomischen Daten korreliert werden, selektive Politiken motivieren, in denen Personengruppen, die als durchschnittlich risikofreudiger gemessen wurden, durch zukünftige Verordnungen unter Berufung auf das Infektionsschutzgesetz anders behandelt werden als andere Gruppen, deren Compliance vermeintlich höher ist.

- Die individuelle/spezifische Variante diese Angriffs ergibt sich, wenn die Betreiberïn bei infizierten Nutzerïnnen die tempID-Token mit der Identität verknüpfen können. Dann ist es denkbar, dass Behörden und Politik anhand des Verhaltensscorings Strafverfolgung einleiten möchten, eine individuelle Beteiligung an den Behandlungskosten an den Scores bemessen oder über den Zugang zu knappen medizinischen Ressourcen anhand der Scores entscheiden werden (z.B.: »wer sich gemäß Datenauswertung fahrlässig verhalten hat, hat den Beatmungsplatz nicht verdient«).

- Eine dritte Variante des Angriffes besteht in der Anwendung von Erkenntnissen aus der verhaltenswissenschaftlichen Forschung auf den Gebrauch der App: Aus dieser Forschung ist bekannt, dass es Korrelationen zwischen der App-Nutzung und riskantem Verhalten gibt. Das kann von einem Angreifer, möglicherweise im Zusammenhang mit anderen Daten, in zwei Richtungen als Kausalität interpretiert werden: 1. Wer sich im Allgemeinen riskant verhält, wird die App eher installieren, um die eigene Riskanz besser kontrollieren zu können. 2. Wer sich die App installiert, wird sich tendenziell riskanter verhalten, weil die App und deren Nutzung eine, wenn auch trügerische, Sicherheit suggeriert.

Das **Risiko dieses Angriffs ist als hoch bis sehr hoch anzusehen,** weil epidemiologische Auswertungen mit offenbar breiter Zustimmung diskutiert und geplant werden.

Angriff A3: De-Anonymisierung von Nutzerïnnen anhand von Verbindungsdaten

Angreiferïn: Betreiber / Behörden / Organisationen

Wenn eine positiv getestete Nutzerïn die von ihrer App verwendeten und (im Fall der dezentralen Variante) zunächst nur lokal gespeicherten tempID-Token auf den zentralen Server lädt, können die Betreiber anhand von Verbindungsmetadaten (zum Beispiel IP-Adresse) und Geräteinformationen die Nutzerïn identifizieren.[2] Damit kann die durch die tempID-Token repräsentierte Kontakthistorie mit der Identität der positiv getesteten Person in Verbindung gebracht werden. Das führt im Fall der dezentralen Architektur (DP-3T) zu folgenden Risiken:

- Die Betreiber können positiv getestete Personen de-anonymisieren und verfügen damit über Gesundheitsdaten, die personenbezogen sind.
- Die Betreiber können für positiv getestete Personen alle Kontakte de-anonymisieren, die ihrerseits auch positiv getestet sind. Bei einer zu erwartenden Durchseuchung im Bereich von 50–70% wäre das letztlich ein großer Teil der Kontakthistorie.
- Die Betreiber können über positiv getestete Personen detaillierte statistische Auswertungen ihres Kontakt- und Risikoverhaltens erstellen (inkl. Compliance mit den Kontaktbeschränkungsauflagen, siehe Angriff A2).

Sollte im Rahmen von PEPP-PT nicht die dezentrale Architektur (DP-3T) sondern eine zentrale Architektur umgesetzt werden, in der die tempIDs (bzw. die Seeds zur ihrer Generierung) von vornherein über den zentralen Server vergeben werden, dann entstehen sogar die folgenden Risken:

- Die Betreiber können alle Nutzerïnnen über Verbindungsmetadaten de-anonymisieren.
- Die Betreiber können von positiv getesteten Nutzerïnnen die *gesamte* Kontakthistorie de-anonymisieren.

Die Entscheidung zwischen zentraler und dezentraler Variante – die beide innerhalb von PEPP-PT möglich sind – hat somit erhebliche Datenschutzimplikationen. Beide Varianten gehen mit einem erheblichen Grundrechtseingriff einher, weil es den Betreibern leicht möglich ist, die Kontakthistorien positiv getesteter Nutzerïnnen aufzudecken.

Zwar sieht das Konzept von DP-3T vor, dass der Server die Verbindungsdaten nicht loggt. Doch eine entsprechende Änderung dieser Verfahrensweise ist mit wenig technischem Aufwand verbunden und kann auch nachträglich erfolgen, auch im Rahmen von Sekundärnutzungsbegehren.

Weil den verschiedenen (nationalen) Implementierungen innerhalb des PEPP-PT-Frameworks in den für diesen Angriff relevanten technischen Merkmalen weitgehende Freiheit eingeräumt ist, muss das **Risiko dieses Angriffs international betrachtet als hoch bewertet werden.**

[2] Schutz hiervor würde nur die Verwendung eines Anonymisierungsnetzwerkes wie Tor bieten, die von dem DP-3T-Entwurf allerdings ausgeschlossen wird (DP-3T-FAQ).

Angriff A4: Unbefristete Speicherung von Daten für eine mögliche spätere Verkettung mit anderen, personenbezogenen Daten

Angreiferïn: Betreiber, Programmiererïnnen, Organisation, Behörden

Es ist denkbar, dass einzelne nationale Implementierungen innerhalb de PEPP-PT-Rahmens auf die Löschung der erfassten Daten nach 14 Tagen verzichten. Ebenso ist es möglich, dass korrumpierte oder fehlerhafte Implementierungen von DP-3T (welches eine Löschung der Daten vorsieht) die Daten dauerhaft aufbewahren (z.B. durch Server-Backups).

Sollten die Daten nicht nach 14 Tagen gelöscht werden, wäre es möglich, sie auch rückwirkend mit anderen Daten in Verbindung zu bringen sowie Deanonymisierungsangriffe zu verüben.

Die Verantwortung, dieses Angriffsszenario zu verhindern, liegt insbesondere bei den Betreibern und Administratoren konkreter Implementierungen. **Das Risiko ist deshalb als hoch einzuschätzen.**

Angriff A5: Falsche Annahmen über Use Cases und Verfahren

Angreiferïn: Betreiber, Programmiererïnnen, Organisation, Behörden

Wird eine Nutzerïn des Systems positiv getestet, kann sie diesen Infektionsstatus zum Zeitpunkt t über das System melden. Ihren Kontaktpersonen wird es damit möglich, retrospektiv ihr Expositionsrisiko ab Zeitpunkt t – n Tage, mit n voraussichtlich 14, zu ermitteln. In den vorliegenden Spezifikationen und Use Cases bleibt offen, wie die infizierte Nutzerïn danach weiter verfährt:

- Die Nutzerïn könnte die App wie bisher weiter verwenden.
- Die Nutzerïn könnte die App deinstallieren.
- Die Nutzerïn verlässt die Quarantäne, führt dabei aber das Smartphone nicht mit sich.

Zu bedenken ist, dass eine infizierte Nutzerïn auch weiterhin andere exponieren könnte; die Infektionshistorie, die vom System erfasst werden sollte, setzt sich somit potenziell fort. Auch eine perfekte Quarantäne-Compliance ist nicht gewährleistet. Deshalb müsste die App weiterhin täglich die gesehenen tempIDs anderer Nutzerïnnen übermitteln, solange die Nutzerïn als infiziert gilt. Ob dies geboten oder vorgesehen ist, ist technisch nicht spezifiziert.

Es besteht sowohl aufgrund des technischen Designs als auch durch Unsicherheitsfaktoren in der Verhaltensweise von Nutzerïnnen ein **mäßig bis hohes Risiko,** dass die Integrität der gesammelten Daten durch diese Schwachstelle kompromittiert wird.

7.2 Angriffe durch private oder staatliche Organisationen, weitere interessierte Behörden, sowie kommerzielle Kontexte

Angriff B1: Freiheitsbeschränkungen bei Nicht-Nutzung der App

Angreiferïn: Behörden / Organisationen / Arbeitgeberïnnen / politische Entscheidungsträgerïnnen

Auch wenn die Verwendung der Tracing-App freiwillig ist, ist es möglich, dass die Nicht-Verwendung mit besonderen Restriktionen der Bewegungs- und Kontaktfreiheit belegt wird. Zum Beispiel könnten die Apps als Zugangsbarrieren zu öffentlichen und privaten Gebäuden, Universitäten, Schulen, Transportmitteln, Verwaltungen, Polizeidienststellen etc. verwendet werden, indem bei Betreten eine auf dem Gerät installierte Corona-App vorgezeigt werden muss.

Eine solche Position wird durch einzelne Akteure und Medienberichte bereits in die Diskussion eingeführt (Stand 10.04.2020): »Prinzip Führerschein: Wer mit Maske und ›Corona-App‹ sein Gefährdungspotenzial für Andere reduziert, sollte nicht weiter beschränkt werden.« – So lautet ein Vorschlag, den der Tagesspiegel am 07.04.2020 in einem Gastkommentar verbreitet (Schallbruch 2020).[3]

Ein Papier des Bundesinnenministeriums zur Strategie für eine schnellstmögliche Beendigung des Lockdowns sieht die »umfassende Kontaktsuche von positiv getesteten Personen (staatliche ›Corona-Detektive‹/RKI-Initiative) [...] mittels Apps« als zentrales Konzeptmerkmal vor (Bundesinnenministerium 2020; *Coronakrise: Innenministerium skizziert Weg aus dem Lockdown* 2020). Es wird beschrieben, dass die Wiedereröffnung von Arbeits- und Produktionsstätten an die Bedingung geknüpft werden könnte, dass Arbeitgeberïnnen »eigene (zertifizierte) Schutzsysteme aufgebaut haben«. Es ist leicht vorstellbar, dass ein de facto Zwang zur Nutzung der Tracing-App zum Beispiel von Arbeitgebern ausgeübt werden könnte, die das Vorzeigen der App zur Zugangsbeschränkung ihrer Gebäude erklären könnten.

Prinzipiell ist damit zu rechnen, dass in solchen Fällen nicht allein eine installierte Version der App vorzuzeigen ist, sondern etwa ein Bildschirm, auf dem das individuelle Expositionsrisiko anhand der Bewegungsdaten der vergangenen 14 Tage hervorgeht. Auf diese Weise wäre es leicht möglich, dass hiermit auch die kontinuierliche Nutzung der App überprüft werden würde.

Es besteht ein **hohes Risiko,** dass Nutzerïnnen selbst unter Bedingungen der »Freiwilligkeit« zur Nutzung der App genötigt werden könnten. Es ist mit erheblichen Beschränkungen der Bewegungsfreiheit und der Grundrechte für alle zu rechnen, die die App nicht benutzen können oder wollen. Da nicht jede*r ein Smartphone besitzt und die Verbreitung von Smartphones auch von demographischen und sozio-ökonomischen Faktoren abhängt, kann eine Schlechterbehandlung von Nicht-Nutzerïnnen der App überdies zu gravierenden Diskriminierungen ohnehin benachteiligter Gruppen führen.

Angriff B2: Kommerzielles Tracking

Angreiferïn: Kommerzielle Betreiberïnnen von BT-Tracking-Infrastruktur, Trittbrettfahrerïnnen

Shopping Malls, Shop, Flughäfen, U-Bahn-Stationen, Werbetafeln im Straßenland etc. sind schon heute mit BT-basierter Trackinginfrastruktur ausgestattet, um die Bewegung von Kundïnnen innerhalb eines Raumes und die Verweildauer sowie Rückkehrrate von Kundïnnen (etwa an einer Werbetafel) zu messen (Kwet 2019). Als Trackingtoken dienen diesen Techniken die (grundsätzlich invarianten und gerätespezifischen) MAC-Adressen der BT-Endgeräte.

Der flächendeckende Einsatz einer BTLE-basierter Tracing-App zur Bekämpfung der SARS-CoV-2-Pandemie führt dazu, dass deutlich mehr Personen das BT-Modul ihres mobilen Endgeräts dauerhaft einschalten. **Es kann als sehr wahrscheinlich bis**

[3] In ähnlichem Sinne erklärte der österreichische Nationalratspräsident Wolfgang Sobotka, dass derzeit verfassungsrechtlich geprüft werde, ob die Bewegungsfreiheit für Personen, die die App nicht installieren, eingeschränkt bleiben kann, vgl. Tremmel 2020.

gesichert angesehen werden, dass die Tracing-App bei ausreichender Verbreitung den bestehenden kommerziellen Trackinginfrastrukturen in die Hände spielen und als Nebeneffekt eine große Menge Daten in privaten Händen generieren wird, anhand derer sich das Bewegungsverhalten von Personen studieren lässt. Nicht nur an private Räume ist hier zu denken (Einzelhandel), sondern auch an Arbeitsumgebungen, Verkehrsknotenpunkte und urbane Flächen, die etwa von den privaten Betreibern elektronischer Werbetafeln (mit BT-Trackinginfrastruktur) abgedeckt sind.

Es ist bekannt, dass gängige MAC-Randomization-Verfahren von Apple einfach umgangen werden kann und insofern keinen wirksamen Schutz vor diesem Angriff darstellt (Martin u. a. 2019).

Angriff B3: Sekundärnutzung bei zentraler Vergabe der ID-Token

Angreiferïn: Betreiber / Polizei / Behörden / politische Entscheidungsträgerïnnen

Angenommen, gegen eine Nutzerïn A des Systems wird zugleich strafrechtlich ermittelt. Prinzipiell kann das Kontakt-Tracing-System dazu genutzt werden, A's Kontaktumfeld auszuforschen, um etwa mögliche Komplizïnnen aufzudecken (vgl. Angriff A3). Die Verwendung des Systems für solche Zwecke würde einen Sekundärnutzungsanspruch darstellen, der mit **geringen technischen Barrieren** versehen ist, also hauptsächlich von der politischen Rahmensetzung ermöglicht oder verhindert wird. Abhängig davon, was für ein Delikt der Person vorgeworfen wird, könnte dieser Sekundärnutzungsanspruch öffentlich plausibel dargestellt und durch Gesetzesänderung leicht erwirkt werden; man denke etwa an einen Terroranschlag.

Das konkrete Risiko hängt von der technischen Umsetzung ab:

- Im Fall der zentralen Architektur (hier kennt der Server für alle Nutzerïnnen die tempIDs) ist die Kontakthistorie vollständig aufdeckbar, falls A positiv getestet wird und über die Corona-App ihre Kontaktdaten an den Server gesendet hat. Ist A nicht positiv getestet, so sind diejenigen ihrer Kontakte nachvollziehbar, die ihrerseits infiziert sind und dies über die App gemeldet haben.

- Im Fall der dezentralen Architektur (DP-3T) kennt der Server nur für infizierte User die tempIDs. Gegebenenfalls durch Logging und Auswertung von Verbindungsdaten können die Betreiber die positiv getesteten Nutzerïnnen jedoch de-anonymisieren (siehe Angriff A3). In diesem Fall wäre A's Kontaktumfeld ausforschbar, wenn sie selbst infiziert ist und insofern auch Kontakte infiziert sind. (Man kann von infizierten Verdächtigen also alle ebenfalls infizierten Verdächtigen ermitteln.)

In ähnlicher Weise lassen sind Sekundärnutzungsansprüche zur Verfolgung Geflüchteter, oder, in nicht rechtsstaatlichen Ländern, politisch Verfolgter und anderer Minderheitengruppen vorstellbar. Auch wenn die politische Opportunität solcher Sekundärnutzungsansprüche zum aktuellen Zeitpunkt in Deutschland nicht gegeben zu sein scheint, wird mit der Corona-App eine Infrastruktur geschaffen, die je nach technischer Konstruktionsweise leicht dafür genutzt werden kann. Solange diese Szenario nicht durch *technische,* sondern allein durch politische Barrieren verhindert wird, ist das **Risiko dieses Angriffs international betrachtet als sehr hoch einzuschätzen.** Dieses Risiko ist insofern sogar hochrelevant, als dass etwa das PEPP-PT-Projekt eine CA-Lösung für Europa entwickeln will, doch selbst einige europäische Staaten sich jüngst von elementaren Rechtstaatsprinzipien<Rechtstaatprinzip> verabschiedet haben.

Angriff B4: Plattformen (Google / Apple) können Daten ableiten

Angreiferïn: App-Plattformen

Da die App-Plattformen die technisch-organisatorische Infrastruktur zur Distribution, Installation, Aktualisierung und Deinstallation von Apps bereitstellen, sowie exklusiv Notification-Frameworks anbieten und betreiben, können sie die bei der Nutzung anfallenden Metadaten verarbeiten und tun es auch. Einerseits aus technischen Gründen der Betriebsaufrechterhaltung, aber auch als zentralem Teil ihrer Geschäftsmodelle.

Somit entstehen sowohl bei der Installation, beim Betrieb als auch bei der Deinstallation immer personenbezogene Daten, die zu Profilen zusammengeführt werden können. Insofern die mobilen Anwendungen sich auch auf Notification-Frameworks wie Googles Firebase Cloud Messaging (FCM) bzw. Apples Push Notification Services (APN) stützen, erlangen die Anbieterïnnen die so versendeten Daten und Metadaten.

Andererseits bieten diese Plattform zugleich eine sichere Umgebung für Distribution, Aktualisierung und Betrieb der App.

7.3 Angriffe durch Hacker, Trolle, Stalker und Einzelpersonen

Angriff C1: Großflächiges Bluetooth-Hacking

Angreiferïn: Dritte, Hackerïnnen, Polizei, Geheimdienste

Eine BT-basierte Corona-App zwingt Nutzerïnnen dazu, das BT-Modul ihres mobilen Endgeräts dauerhaft einzuschalten (siehe Angriff B2). Die BT-Implementierungen sowohl von Android als auch iOS sind für zahlreiche Sicherheitslücken bekannt,[4] von denen einige sogar die unbemerkte Ausführung beliebigen Codes auf dem attackierten Gerät erlauben. Ein großflächiger, quasi zwangsweiser Einsatz von BT auf den Endgeräten einer Mehrheit der Bevölkerung könnte Angreiferïnnen, die diese Sicherheitslücken ausnutzen möchten, Vorschub leisten. Denkbar wären automatisierte Einbrüche in die Gräte beliebiger Nutzerïnnen überall dort, wo sich Angreiferïn und Ziel für eine kurze Zeit in ausreichender räumlicher Nähe befinden, etwa in Wohnhäusern, öffentlichen Verkehrsmitteln oder an Wartepunkten.

Die Corona-App erfordert, um effektiv zu sein, eine Nutzungsquote von mehr als 60 Prozent der Bevölkerung . Um diesen Verbreitungsgrad zu erreichen, wird die App nicht auf die aktuellsten Sicherheitsupdates oder Verwendung der neuesten Betriebssystemversionen bestehen können. Eine im Sinne ihrer Verbreitung effektive Corona-App müsste bezüglich der Softwareumgebung relativ geringe Anforderungen stellen. Das führt dazu, dass durch den Einsatz der Corona-App Geräte mit bekannten Schwachstellen der BT-Implementierung exponiert werden. Das **Risiko dieses Angriffs ist als mäßig einzuschätzen,** weil die Attacken lokal begrenzt ausgeführt werden und deshalb schlecht skalieren.

Angriff C2: Injektion falscher Infektionsereignisse

Angreiferïn: Dritte, Hackerïnnen, Polizei, Geheimdienste

Weder die App noch der Server können grundsätzlich prüfen, ob die positive Testung einer Nutzerïn, die als Auslöser für die Übertragung der tempID-Tokens an den Server dient, tatsächlich stattgefunden hat. So wäre es möglich, eine zur Datenübertragung ausgehändigte TAN zur Übertragung der Daten einer *anderen* Nutzerïn zu verwenden

[4] Siehe die im Abschnitt »Security« aufgeführten Verweise in Privacy International 2020.

oder auf illegalem Wege an eine TAN zu gelangen, obwohl man nicht positiv getestet wurde.

Es ist denkbar, dass einzelne Akteure falsche Infektionsereignisse in das System injizieren, mit der Folge, dass andere Nutzerïnnen unzutreffend als exponiert klassifiziert werden.

Von diesem Angriff gibt es verschiedene Klassen, die auch von den Maßnahmen abhängen, die zur Sicherung der Integrität der Verarbeitungstätigkeit gewählt wurden:

- Wenn der Server keine Prüfung der tempID-Tokens vornehmen kann und / oder vornimmt, dann können viele oder gar alle im Wertebereich möglichen tempID-Tokens an den Server gesendet werden. In der Folge bekommen alle App-Nutzerïnnen, die eine gewisse, wenn auch relativ kleine, Mindestmenge an Kontaktereignissen aufgezeichnet haben, einen Risiko-Score jenseits des Schwellwertes zugewiesen und werden dann fälschlicherweise als exponiert behandelt.

- Wenn der Server nur authentische tempID-Tokens akzeptiert, dann muss es in der Verarbeitungstätigkeit einen Verfahrensbestandteil geben, in dem die Verknüpfung des Daten-Uploads mit der positiven Testung geprüft wird, etwa von einer Gesundheitseinrichtung. Auf dieser Basis müsste ein Authentifizierungstoken, etwa ein anonymes Credential, vergeben werden, das nach dem Hochladen der tempID-Tokens geprüft werden kann. In diesem Fall lässt sich der Angriff – jedenfalls in einer Großstadt wie Berlin, Hamburg oder München – durchführen, indem eine relativ kleine Gruppe von Angreiferïnnen sich mehrere Tage lang durch die Stadt bewegt und Orte aufsucht, an denen es zu einer großen Zahl von Kontaktereignissen kommt.

Soweit die Authentifizierungstoken stark dezentral, etwa von einzelnen medizinischen Einrichtungen, vergeben werden, ist damit zu rechnen, dass Angreiferïnnen in jedem Fall Zugriff auf valide Authentifizierungstoken bekommen, um anschließend große Mengen an authentifizierten tempID-Tokens auf den Server zu laden. Soweit die Authentifizierungstoken mehr oder weniger zentral vergeben werden, verschiebt sich das Problem nur: Angreifer müssen dann nicht direkt versuchen, an Authentifizierungstoken zu kommen, sondern sie müssen nur an medizinische Bescheinigungen über ihre eigene Infektion gelangen – und diese dienen dann als Berechtigungsnachweise, um an die Authentifizierungstoken zu gelangen. Weil ein Maß an krimineller Energie und Organisiertheit zur Voraussetzung dieses Angriffs gehört und weil die Attacke nur mäßig skaliert, ist ihr **Risiko als mäßig einzuschätzen.**

Kapitel 8

Bestimmen der Schutzmaßnahmen für die Verarbeitungstätigkeiten

Auf der Grundlage der im vorhergehenden Kapitel beschriebenen Risikoquellen (zum Beispiel Angreiferïn), Gefährdungen (zum Beispiel Angriffe oder Störungen) und rechtlichen Anforderungen (vgl. Kapitel 5) sind im Folgenden weitergehende Anforderungen aufgeführt, um dem hohen Schutzbedarf der personenbezogenen Daten zu begegnen, der sich logisch auf die Komponenten der Verarbeitungstätigkeiten vererbt.

Die Schutzmaßnahmen sind jeweils mit einem »R« gekennzeichnet, um einen Bezug zu den Risiken herzustellen, die durch sie behandelt werden. Beispiel: Das Risiko, das durch den Angriff A4 entsteht, wird mit [R:A4] bezeichnet.

Die Schutzmaßnahmen werden dabei für das übergeordnete Verfahren als ganzes, also auch systematisch entlang der einzelnen Verarbeitungstätigkeiten benannt.

Alle Anforderungen sind als MUSS-, SOLL- oder KANN-Sätze formuliert. MUSS-Anforderungen sind notwendige Maßnahmen, ohne die eine Verarbeitung nicht stattfinden darf. SOLL-Anforderungen sind notwendige Maßnahmen, für die es unter bestimmten Umständen triftige Gründe geben kann, sie nicht zu erfüllen, aber die volle Tragweite der Nichterfüllung muss verstanden, sorgfältig abgewogen und die Entscheidung und die Gründe müssen klar und umfassend dokumentiert werden. KANN-Sätze bezeichnen Anforderungen, deren Erfüllung vollständig optional ist.

Im Bezug auf die vorliegende Verarbeitungstätigkeit sind mindestens die folgenden SDM-Bausteine für das Verfahren und seine Komponenten (siehe Abschnitt 4) umzusetzen:

Zielobjekte	Bausteine
CA, CA-Server	Baustein 11 “Aufbewahrung”
Verfahren, Verarbeitungstätigkeiten, Vorgänge, Daten, Formate, Fachapplikation, IT-Services, Prozesse, Kommunikationsbeziehungen	Baustein 41 “Planung und Spezifikation”
Verfahren, Verarbeitungstätigkeiten, Vorgänge, Daten, Formate, Fachapplikation, IT-Services, Prozesse, Kommunikationsbeziehungen	Baustein 42 “Dokumentation”
Vorgänge, Fachapplikation, IT-Services, Prozesse, Kommunikationsbeziehungen	Baustein 42 “Protokollierung”

Verfahren, Verarbeitungstätigkeiten, Vorgänge, Daten, Formate, Fachapplikation, IT-Services, Prozesse, Kommunikationsbeziehungen	Baustein 50 “Trennung”
Vorgänge, Fachapplikation, IT-Services, Prozesse	Baustein 60 “Löschen und Vernichtung”
Organisation	Baustein 80 “Datenschutzmanagement”

8.1 Übergreifende Schutzmaßnahmen für das ganze Verfahren

M 0.1 Datenschutz-Management (Transparenz, Intervenierbarkeit) [R:A1 R:A4].
Es MUSS ein Datenschutzmanagement (DSM) vorhanden sein, um die Datenschutzanforderungen zu identifizieren, zu überwachen und zu steuern (siehe rechtliche Anforderung auf Seite 45). Umsetzungshinweise sind im SDM-Baustein »Datenschutzmanagement« vorhanden.

Ein DSM muss bei einem hohen Risiko für die Rechte und Freiheiten einer Person als ein Datenschutzmanagementsystem eingerichtet sein, das seinerseits, nach dem Stand der Technik, einer kontinuierlichen Verbesserung unterzogen wird. Reife Managementsysteme weisen *Key Performance Indicators (KPI)* aus. Ein in diesem Kontext wünschenswerter KPI zur Messung der Reife des DSMS des Verfahrens könnte darin bestehen, die Häufigkeit der durchgeführten Prüfungen, dass die Uploads von Gesundheits-TempIDs ohne Protokollierung stattfindet, auszuweisen.

M 0.2 Einsatz einer dezentralisierten Architektur (Nicht-Verkettbarkeit) [R:A3 R:B3]
Um die Risiken der De-Anonymisierung oder der Erstellung von sozialen Graphen zu minimieren, MUSS eine dezentralisierte Architektur bevorzugt werden.

M 0.3 Spezifikation des Verfahrens (Transparenz, Integrität) [R:A5]
Die Verarbeitungstätigkeiten MÜSSEN vollständig geplant und spezifiziert werden (siehe SDM-Baustein »Planung und Spezifikation«). Dabei MÜSSEN alle relevanten Use Cases erfasst und beschrieben sein.

Bei Verfahren mit hohem Risiko MUSS die Phase der Planung von dessen Architektur sorgfältig gestaltet sein. Dazu zählt die Verwendung einer erprobten Projektmanagemanagementmethode wie Wasserfall-Methode oder PRINCE2. Projektmanagementmethoden sollten ihrerseits von einem generellen Framework zur Sicherung des Qualitätsmanagements eingefasst sein. An der Schnittstelle von Organisationsstruktur und IT-Systemen MÜSSEN standardisierte Prozesse etabliert sein, die Störungen von Problemen und Änderungsbedarfen mit Bezug auf die Organisationsstruktur zu unterscheiden gestatten. Hier hat sich in der Europäischen Union insbesondere ITIL als Standard etabliert (Rost und Welke 2020).

Es MUSS ein Test-Konzept vorliegen, mit denen Testphasen, die einer kontrollierten Freigabe unterliegen, und Protokolle, aus denen Designentscheidungen hervorgehen, dokumentiert sind.

M 0.4 Schutz vor (nicht-)nutzungsabhängiger Diskriminierung (Nicht-Verkettbarkeit) [R:B1]
Flankierend zur Veröffentlichung der CA MUSS rechtlich und faktisch sichergestellt werden, dass Nutzerïnnen anderen gegenüber weder den Status der CA noch die Existenz der CA auf dem eigenen Gerät bekannt geben müssen. Ausnahmen KÖNNEN dabei etwa das ärztliche Personal bilden, um Heimquarantäne auch bei Arbeitgeberïnnen anhand von Krankschreibungen durchzusetzen. Ziel dieser Regelungen ist das Sicherstellen der Zweckbindung der CA. CA-basierte Zugangsbarrieren zu öffentlichen und privaten Gebäuden, Universitäten, Schulen, Transportmitteln, Verwaltungen, Polizeidienststellen etc. MÜSSEN unterbunden werden. Es MUSS geprüft werden, inwiefern die nötigen Maßnahmen außerhalb ihrer Kontrolle – etwa im gesetzgeberischen Bereich – zu verorten sind.

Zweckbindung wird wesentlich durch Trennung von Datenbeständen, IT-Systemen und Diensten sowie von Teilprozessen durchgesetzt. In diesem Kontext ist zum einen die Konditionierung des Personenbezugs durch eine Pseudonymisierung etwa der TempID-Token als auch die Anonymisierung der auf den CA-Server hochgeladenen Gesundheits-TempIDs und deren Überführung in »infektionsanzeigende Daten ohne Personenbezug (iDoP)« wesentlich. Es MUSS überlegt werden, wie man die Betriebe verschiedener IT-Systeme auf der CA-Serverseite und deren organisationale Trennung durchsetzt.

Die Prüfbarkeit einer Verarbeitungstätigkeit hängt von den Vorbereitungen aus der Planungsphase ab in Bezug auf die Dokumentation der Eigenschaften der beteiligten Komponenten, mit denen sich Soll- und Ist-Werte ermitteln lassen sowie der Protokollierung, mit denen sich Systemereignisse in der Vergangenheit nachvollziehen lassen. Bei einem hohen Risiko MUSS die Protokollierung über einen zertifizierten Zeitstempel verfügen sowie Vorkehrungen dafür treffen, dass die Bezeichner für die beteiligten Instanzen eindeutig und sprechend sind, um Menschenlesbarkeit zu erlauben. Die Protokollierung MUSS dann so eingerichtet werden, dass Protokolldaten nicht auf den Produktionsmaschinen liegen, sondern auf einem dedizierten Protokolleserver. Stattgefundene Prüfungsaktivitäten von Protokolldaten MÜSSEN ihrerseits protokolliert sein. Diese dienen der Verantwortlichen zum Nachweis der Wirksamkeit der Schutzmaßnahmen.

Es folgen die Schutzmaßnahmen, die einzelnen Verarbeitungstätigkeiten zugeordnet werden können.

M 0.5 Sichere App-Entwicklung (Integrität) [R:B4]
Es SOLLTE darauf geachtet werden, eine sichere Entwicklungsumgebung für die App-Entwicklung zu nutzen.

Hier gilt sicherzustellen, was oben im Kontext der Planung einer Verarbeitungstätigkeit gesagt wurde. Agile Entwicklungsmethoden können für die Entwicklung von Software auch für hochriskante Verarbeitungstätigkeiten genutzt werden, gleichwohl sollte hier besonderer Wert auf die Berücksichtigung rechtlicher Vorgaben gelegt werden. Nicht die schnelle Entwicklung von Funktionalitäten hat oberste Priorität, sondern die Datenschutz- und Rechtskonformität.

M 0.6 Sichere Verteilung der App (Integrität) [R:B4]
Es SOLLTE Prüfmechanismen zur Verfügung gestellt werden, die es der Benutzerïn erlaubt, die Integrität der App nach dem Herunterladen zu prüfen.

M 0.7 Sicherer Einsatz der App (Integrität, Vertraulichkeit, Nicht-Verkettbarkeit) [R:B4]
Es SOLLTE eine IT-Nutzungsrichtlinie für die Benutzerïn bereitgestellt werden. Zudem SOLLTEN Angaben über unterstützte Geräte und Betriebssystemversionen bereitgestellt werden, die von der Verantwortlichen getestet und hinsichtlich möglichen Datenflüssen geprüft wurden.

Die App SOLLTE Teil des IT-Sicherheits-Audits nach BSI-Grundschutz sein, um insbesondere die Kommunikation mit dem CA-Server durch Verschlüsselung und Authentisierung zu sichern.

M 0.8 Abwägung zwischen Verbreitungsgrad und sicherer Nutzung der CA (Integrität, Verfügbarkeit, Vertraulichkeit) [R:C1]
Auf dem Markt und mehr noch in Benutzung befinden sich diverse Smartphone-Betriebssysteme und Betriebssystem-Versionen, viele davon nicht auf dem aktuellen Stand und somit mit bekannt-offenen Sicherheitslücken, inklusive unsicherem Bluetooth-Stack. Beim Einsatz der CA ist eine dauerhafte Aktivierung des Bluetooth-Moduls vonnöten. Die Betreiberin MUSS überprüfen und abwägen, inwiefern ein hoher Verbreitungsgrad der CA tatsächlich viel wichtiger ist, als der garantiert sichere Betrieb in jeder Nutzung. Im ersten Falle MUSS die CA so viele Smartphone-Betriebssystem-Versionen unterstützen wie möglich, im zweiten Falle MUSS die Möglichkeit zur Installation der CA auf aktuelle, noch unterstützte Betriebssystem-Versionen beschränkt werden.

Prüfbarkeit und Prüfung: Öffentliche Dokumentation und Begründung der Entscheidung.

M 0.9 Bereitstellung einer Datenschutzerklärung (Transparenz)
Der Benutzerïn MUSS vor Nutzung eine Datenschutzerklärung nach Art. 21 Abs. 1 DSGVO vorgelegt werden (siehe auch Seite 63). Diese MUSS mindestens in der Landessprache vorliegen, KANN in allen in Einsatzbereich häufig gesprochenen Sprachen vorbereitet werden, aber SOLLTE auch in den Sprachen besonders gefährdeter Gruppen vorhanden sein, sofern diese Differenzierung sinnvoll erscheint.

Die Datenschutzerklärung SOLLTE dabei genaue Informationen darüber enthalten, was die genauen Parameter der Kontakt- und des Risikowerterrechung sind.

M 0.10 Schutzmaßnahmen für die Fachapplikationen CA und CA-Server, sowie der TAN-Verwaltung (Vertraulichkeit, Integrität, Zuverlässigkeit)
Aufgrund des hohen Schutzbedarfes MÜSSEN die üblichen Sicherheitsmaßnahmen der IT-Sicherheit nach BSI-Grundschutz oder im Rahmen von ISO-27001 zertifiziert werden.

M 0.11 Schutzmaßnahmen für alle IT-Services (Vertraulichkeit, Integrität, Zuverlässigkeit)
Zu den verwendeten IT-Serivces gehören Smartphone, BTLE-Dienst, Internet, Datenbank-Server, Server-OS, HW, RZ und allgemein das Internet. (Prüfung auf möglichen Grundschutz/ISO von verlangen. Illusorisch, aber sollte geprüft werden)

M 0.12 Schutzmaßnahmen für alle Kommunikationsbeziehungen über TCP/UDP (Vertraulichkeit, Integrität)

Die Transportverbindung zwischen Server und Client MUSS nach Stand der Technik Ende-zu-Ende gesichert und authentifiziert sein. Dazu ist gegebenenfalls eine Public-Key-Infrastruktur in mittlerer oder hoher Validierungsstufe zu verwenden.

M 0.13 Herstellung der Prüffähigkeit des Quellkodes (Transparenz)
Der Quellkode für die CA und den CA-Server MUSS öffentlich einsehbar sein. Er MUSS mindestens den Aufsichtsbehörden stets aktuell vorliegen.

M 0.14 Veränderung der Software revisionssicher protokollieren (Transparenz, Integrität)
Die Veränderung von Software-Ständen MUSS revisionssicher und öffentlich einsehbar protokolliert werden.

M 0.15 Evaluation der Nutzung von App-Plattformen (Vertraulichkeit, Nicht-Verkettbarkeit)
[R:B4] Die Verantwortliche MUSS evaluieren, inwiefern bei der Nutzung von App-Plattformen die Datenschutzrisiken oder die IT-Sicherheitsvorteile überwiegen. Jedenfalls MUSS durch rechtliche, technische und/oder organisatorische Maßnahmen verhindert werden, dass die Nutzungsdaten der Plattformen mit den Daten der CA verknüpft werden können.

8.2 Schutzmaßnahmen für die Verarbeitungstätigkeit »App-seitige Verarbeitung von Kontaktereignissen«

M A.1 Getrennte Speicherung in der App (Nicht-Verkettbarkeit) [R:A2]
Die Speicherung von einerseits gesendeten und andererseits empfangenen TempIDs auf dem Smartphone MUSS getrennt von einander erfolgen, um die Rekonstruktion von Kontaktereignissen zu verhindern.

Wesentliche Ereignisse, wie etwa der Zeitpunkt der Inbetriebnahme der App, SOLLTEN protokolliert werden.

M A.2 Kontaktereignisse nur lokal vorhalten (Nicht-Verkettbarkeit) [R:A2 R:A4]
Falls Kontaktereignisse so gespeichert werden, dass eigene und fremde TempIDs verknüpft werden können, so MUSS dieser Datensatz immer auf dem Endgerät verbleiben.

M A.3 Zusammenhangslosigkeit von TempIDs (Nicht-Verkettbarkeit) [R:A2] [R:A4]
Es MUSS unmöglich sein, verschiedene TempIDs der gleichen Benutzerïn in Zusammenhang zu setzen. Sie dürfen beispielsweise nicht auf einem mathematischen Seed basieren, der eine spätere Verkettung ermöglicht.

Der Quellkode der Erzeugungsfunktion (meist die CA) MUSS einsehbar sein und geprüft werden (siehe M 0.13).

M A.4 Schutz gegen Tracking durch Drittanbieter (Nicht-Verkettbarkeit, Vertraulichkeit) [R:B2]
BTLE-Beacons MÜSSEN mit einem geeigneten Verfahren generiert werden, so dass das Format und die Daten keine Rückschlüsse auf die Benutzerïn und das verwendete Gerät zulassen. Es MUSS sichergestellt werden, dass die ausgesendeten TempIDs in geeigneten zeitlichen Abständen geändert werden.

M A.5 Backup der eigenen TempIDs (Verfügbarkeit)
Die Verantwortliche SOLLTE prüfen, inwiefern Backups der selbsterzeugten, eigenen TempIDs gemäß deren Schutzbedarf möglich ist.

8.3 Schutzmaßnahmen für die Verarbeitungstätigkeit »Autorisierung des Uploads, Anonymisierung, Zwischenspeicherung und Verbreitung des positiven Infektionsstatus«

M B.1 Schutz der Anonymität (Vertraulichkeit, Integrität, Nicht-Verkettbarkeit) [R:A3 R:B3]

Es MUSS sichergestellt sein, dass serverseitig keine Protokolle existieren, die eine De-Anonymisierung der Benutzerïn ermöglicht.

Es MUSS ein starker Zutritts-, Zugangs- und Zugriffsschutz für den Server vorhanden sein.

Es MUSS sichergestellt werden, dass Zugriffsschutz durch eine Datenträgerverschlüsselung nach Stand der Technik auf dem Server umgesetzt ist.

Der Zugangsschutz zum Server MUSS durch ein Mehr-Augen-Prinzip umgesetzt werden, das auf einer rechtlichen und organisatorischen Trennung beruht. Diese Trennung MUSS technisch gestützt umgesetzt sein. Der Zugang MUSS zudem über eine Multi-Faktor-Authentisierung durchgeführt werden.

Der Einsatz eines geeigneten Anonymisierungsdienstes auf der Client-Seite MUSS geprüft werden. Der Verzicht auf einen Anonymisierungsdienst muss durch eine überorganisatorische Trennung ausgeglichen werden, indem beispielsweise eine außerorganisatorische Institution Teil der Zugangskontrolle ist. Andernfalls MUSS die Inbetriebnahme dieser Verarbeitungstätigkeit ausgesetzt werden.

Die Transportverbindung zwischen Server und Client MUSS nach Stand der Technik Ende-zu-Ende gesichert und authentifiziert sein.

Es MUSS geprüft werden, inwiefern die zu treffenden Maßnahmen hinsichtlich dem Schutz der Anonymität eine angemessene Schutzwirkung entfalten können oder ob eine neue rechtliche Form zur organisatorischen Trennung für den Server-Zugang Seitens der Gesetzgeberïn geschaffen werden muss (siehe auch Seite 57).

M B.2 Planung und Spezifikation des Vorgangs nach Infektionsmeldung (Transparenz, Integrität) [R:A5]

Es MUSS der Vorgang geplant und spezifiziert werden, was nach einer Infektionsmeldung an den Server seitens der Benutzerïn passiert. Es MUSS spezifiziert werden, welche Funktion die CA nach der Meldung besitzt. Die Benutzerïn MUSS aussagekräftige Hinweise in klarer und einfacher Sprache bekommen, wie nach der Meldung fortzufahren ist und wann das Verfahren für sie abgeschlossen ist. Es SOLLTE geprüft werden, ob die Fortsetzung der Meldung des Infektionsstatus per TempIDs sinnvoll ist, um die Kontakthistorie fortzuschreiben und aktuell zu halten.

M B.3 Serverstatistiken veröffentlichen (Transparenz) [R:A4]

Um den datenschutzfreundlichen Serverbetrieb zu gewährleisten, KANN der Server regelmäßig aggregierte Zustandsdaten veröffentlichen, etwa Gesamtzahl der vorgehaltenen infektionsanzeigenden Daten ohne Personenbezug.

M B.4 Personengebundene Nutzung der TAN (Integrität) [R:C2]

Es MUSS sichergestellt werden, dass die TAN nur personengebunden genutzt werden kann. Eine Möglichkeit kann darin bestehen, dass TAN-Listen mit je zwei TAN-Hälften an Ärztïnnen ausgegeben werden, die dann bei der ärztlichen Behandlung die erste Hälfte der TAN an die Patientïnnen geben, die zweite Hälfte der TAN jedoch erst, nachdem das Labor jeweils eine positive Diagnose gemeldet hat und die Ärztïnnen die

Patientïnnen über die Diagnose informieren. Die Patientïnnen haben dann während des Telefonats Zeit, mit der gesamten TAN die Übertragung der Gesundheits-TempIDs an den Server zu initiieren, anschließend wird die TAN von der Ärztïn gegenüber den Server für nicht mehr gültig erklärt. Da die erste Hälfte der TAN unter Anwesenden ausgetauscht wird, können Dritte die gesamte TAN nicht rekonstruieren. Da die gesamte TAN nur während des Telefonats gültig ist, kann sie mit hoher Wahrscheinlichkeit nur von der infizierten Person genutzt werden. Da die Ärztïn der Person nicht auf das Smartphone schaut, kann sie nicht feststellen, ob die TAN genutzt oder nicht genutzt wurde.

Es KANN ein anderes Verfahren für die Sicherstellung einer ausschließlich personengebundenen Nutzung entwickelt und implementiert werden. Es MUSS nachgewiesen werden, dass dieses andere Verfahren mindestens ebenso gute Datenschutzeigenschaften besitzt.

M B.5 Schutz vor Spoofing/Tampering/Impersonation der TempIDs (Integrität, Vertraulichkeit, Nicht-Verkettbarkeit) [R:C2]
Es MUSS gewährleistet sein, dass die TempIDs weltweit eindeutig sind und der Wertebereich nicht effizient abzählbar ist (Enumeration Attack). Der Einsatz eines Anonymen Nachweis-Systems (siehe unter anderem Camenisch und Lysyanskaya 2001) SOLLTE geprüft werden.

M B.6 Planung und Spezifikation des Vorgangs zur TAN-Verwaltung (Transparenz, Integrität, Vertraulichkeit, Nicht-Verkettbarkeit, Verfügbarkeit) [R:C2]
Der Vorgang zur Erstellung, Übermittlung, Verwendung und Freigabe von TANs MUSS geplant und spezifiziert werden. Es MUSS sichergestellt werden, dass die Verknüpfung von TAN und Gesundheits-TempIDs streng vertraulich bleibt.

M B.7 Rückholung, Widerruf oder Löschung schon an den Server gesendeter tempIDs (Intervenierbarkeit, Transparenz) [R:A1]
Da Labortests auch fehlerhaft sein können (Proben vertauscht, nachträgliche Korrektur der Messung, genauerer Test doch negativ) oder wenn die Nutzerïn sich umentscheidet, ihre Daten freizugeben, so MUSS technisch die Möglichkeit geschaffen werden, schon hochgeladene tempIDs wieder vom Server zu löschen. Dies geschieht entlang einer rechtlichen Fristenregelung. Zudem MUSS die Benutzerïn über die Folgen und das weitere Vorgehen informiert werden.

M B.8 Verzögerung des Hochladens bei Nicht-Verfügbarkeit des CA-Servers (Verfügbarkeit)
Für den Fall, dass der Server beim anzustoßenden Hochladeprozess nicht verfügbar ist, SOLLTE dieser Prozess verzögert werden, bis der Server wieder erreichbar ist. Ein Abbruch ist zu vermeiden.

M B.9 Miteinbezug der Backups bei Löschfristen (Nicht-Verkettbarkeit)
Da der Server aus Gründen der Verfügbarkeit Backups anlegen wird, MUSS die Verantwortliche prüfen, inwiefern Löschanforderungen der Benutzerïn sich auch auf diese Zweitspeicher auswirken müssen.

M B.10 Maßnahmen zur Sicherstellung der angemessenen Verfügbarkeit des Servers (Verfügbarkeit)
Die Verantwortliche MUSS prüfen, inwiefern an den Server Anforderungen der Hochverfügbarkeit zu stellen sind und wie diese gegebenenfalls umzusetzen sind.

8.4 Schutzmaßnahmen für die Verarbeitungstätigkeit »Dezentrale Kontaktnachverfolgung«

M C.1 Planung und Spezifikation des Vorgangs zur Einflussnahme auf Entscheidung durch CA (Transparenz, Intervenierbarkeit, Integrität) [R:A1]
Es MUSS ein Vorgang geplant und spezifiziert werden, der die Einflussnahme auf die Entscheidung der CA durch die Benutzerïn ermöglicht.

Es MUSS möglich sein, die Entscheidung rückgängig zu machen. Die Benutzerïn MUSS über die Rechtsmittel aufgeklärt werden und diese jederzeit abrufen können.

Es MUSS ein Single-Point-of-Contact vorhanden sein. Der SPoC MUSS in der CA abrufbar sein.

M C.2 Backup der gesehenen TempIDs (Verfügbarkeit)
Die Verantwortliche SOLLTE prüfen, inwiefern Backups von gesehenen TempIDs gemäß deren Schutzbedarf möglich ist.

Kapitel 9

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 Ausgaben auf den Smartphones von Betroffenen nehmen können. Die Gesetzgeberïn muss eine Verordnung nach § 14 Abs. 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 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 Betreiberïn 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 Betreiberïn 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 Verantwortlich strategisch und die Betreiberïn 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 Betreiberïn 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 Betreiberïn. 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.

3. Die IT-Sicherheit der genutzten IT-Komponenten in der gesamten Prozesskette, unter Einbeziehung auch der Interaktion mit Ärztïnnen und Gesundheitsämter, muss nach BSI-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.

4. Flankierend zur Veröffentlichung der App *muss* rechtlich und faktisch sichergestellt werden, dass Nutzerïnnen 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 Arbeitgeberïnnen 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.

Abkürzungen

Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BMG	Bundesministerium für Gesundheit
BT	Bluetooth
BTLE	Bluetooth Low Energy
CA	CA-Typ 3 dezentral / Corona-App
COVID-19	Corona virus disease 2019
CV	Corona-Virus
DP-3T	*Decentralized Privacy-Preserving Proximity Tracing* (Projekt)
DSB	Datenschutzbeauftragte/r
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
DSM	Datenschutzmanagement
DSMS	Datenschutzmanagementsystem
FIfF	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung
GPS	Global Positioning System
iDoP	Infektionanzeigendes Datum ohne Personenbezug
IfSG	Infektionsschutzgesetzes
KPI	Key-Performance-Indicator
PEPP-PT	*Pan-European Privacy-Preserving Proximity Tracing* (Framework)
RKI	Robert Koch-Institut
SDM	Standard-Datenschutzmodell
SPoC	Single-Point-of-Contact
TCP	Transmission Control Protocol

TAN	Transaktionsnummer
TempID	Temporärer pseudonymer Identifikator
UDP	User Datagram Protocol
VT	Verarbeitungstätigkeit

Glossar

Datenarten

A. Lokal auf dem Sender-Smartphone mit der CA
   a. TempID (Zeichenfolge, vom Smartphone errechnet und gespeichert)
   b. TempID-Token (Zeichenfolge, als Bluetooth-Nutzdaten gesendet, kann Hardware-Adressdaten enthalten)
   c. Gesundheits-TempID (wie TempID plus TAN-Authorisierung, zum Server gesendet)

B. CA-Server
   a. Gesundheits-TempID (wie TempID plus TAN-Authorisierung, vom Client empfangen)
   b. Hier muss das Trennungsverfahren stattfinden.
   c. infektionsanzeigendes Datum ohne Personenbezug (als Updates an Apps übermittelt), Abkürzung: »iDoP«

C. Lokal auf dem Empfänger-Smartphone mit CA
   a. infektionsanzeigendes Datum ohne Personenbezug (vom Server empfangen)
   b. Kontaktdatum (gemessene fremde TempID, Zeitdauer, Signalstärkenprofil über die Zeit)
   c. Match = Expositionsereignis (berechnet)
   d. Risiko-Score
   e. Infektionswarnung (Binarisierung des Risiko-Scores)

Zum grundsätzlichen Verhältnis von Daten, deren Kontext und der Beziehung zum Informationsbegriff, einem Kernelement des Trennungsverfahrens, siehe auch Dreyfus 1972, S. 197 ff.

Datenschutzbegriffe

Prozesse Ein Verfahren kann auf mehreren organisatorischen, technischen oder personellen Prozesse aufbauen, die zum Betrieb des Verfahrens notwendig sind.

Andere Bezeichner hierfür sind Support-Prozess, Betriebsprozess, Unterprozesse.

Verantwortliche, die (früher: die verantwortliche Stelle) Nach Art. 4 DSGVO (Begriffsbestimmungen) bezeichnet dies die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Verarbeitung, Verarbeitungstätigkeiten »Im Sinne dieser Verordnung bezeichnet der Ausdruck [...] ›Verarbeitung‹ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.« (Art. 4 Abs. 2 DSGVO)

Die einzelne Verarbeitungstätigkeit von personenbeziehbaren Daten ist der Gegenstand der DSFA und damit auch ihr Ausgangspunkt. Die Verarbeitungstätigkeit findet zudem im Kontext statt. Zwar ist der Verarbeitungskontext Teil der Analyse und der Folgenabschätzung, aber die daraus abgeleiteten und den Kontext in sich einbegreifenden technischen und organisatorischen Maßnahmen werden im Allgemeinen allein auf den Gegenstand angewendet.

Verfahren Das Verfahren beschreibt die Ausführung einer Verarbeitung bzw. Verarbeitungstätigkeit und hat damit einen Prozesscharakter. Während das Verfahren im wesentlich die Frage beantwortet, wie eine Verarbeitung auszuführen ist, so ist die Verarbeitung wesentlich durch ihren funktionalen Zweck bestimmt, den sie dem Verfahren mitgibt.

Gemäß dem Standard-Datenschutzmodell ist der Verfahrensbegriff folgendermaßen bestimmt: »Der Begriff ›Verfahren‹ wird benutzt, um vollständige Datenverarbeitungsvorgänge zu beschreiben. Unter Datenverarbeitung fällt insbesondere jedes Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen, Nutzen, Anonymisieren, Pseudonymisieren und Verschlüsseln von personenbezogenen Daten. Ein Verfahren beschreibt eine formalisierte, wiederholbare Folge dieser oben genannten Schritte der Datenverarbeitung zur Umsetzung einer Fachaufgabe bzw. eins Geschäftsprozesses. Dabei ist es gleichgültig, ob sie manuell oder mit Hilfe von Informationstechnik ausgeführt werden. Ein Verfahren ist immer gekennzeichnet durch seine Zweckbestimmung und wird dadurch von anderen Verfahren abgegrenzt.«

Die Legaldefinition steht in Art. 4 Abs. 2 DSGVO.

Im Organisationsleben sind Verfahren typischerweise als »Fachverfahren« oder »Geschäftsprozesse« bekannt.

Verfahrensanalyse Aufschließung des Verfahrens nach Vorgängen und den zugehörigen Aspekten (1) Daten und Datenformate, (2) Systeme und Schnittstellen, (3) Prozesse und Rollen.

Vorgang Ein Vorgang ist die Summe aus Daten, Systemen und Prozessen (vgl. DSK 2018, Kurzpapier Nr 5).

Ein Vorgang ist ein Verarbeitungsschritt innerhalb eines Verfahrens. Ein Vorgang kann mit anderen Vorgängen verknüpft eine Vorgangsreihe bilden. Ein Vorgangsreihe ist vollständig und als Verfahren begreifbar, wenn der Verfahrenszweck dadurch umsetzbar ist.

Zweck Funktionale Begründung für eine Verarbeitung oder Verarbeitungstätigkeit innerhalb eines gesellschaftlichen Kontext.

Zustand von Gesundheit/Krankheit

Infiziert Person hat sich mit dem Virus angesteckt (kann noch latent sein, nicht ansteckend; kann bereits ansteckend sein ohne Symptome; kann COVID-19-erkrankt sein). Infektion endet mit der Heilung der Krankheit (Abklingen der Symptome, evtl. Immunisierung) oder mit dem Tod.

Erkrankt (an CoViD-19) Person ist infiziert und hat Symptome.

Ansteckend Akut infizierte Person in der Verlaufsphase, in der die Infektion auch ansteckend ist.

Positiv getestet Infizierte Person wurde mit geeigneten Methoden (zum Beispiel PCR-Test auf Viren-RNA) positiv auf das Virus getestet und ist somit akut infiziert.

Exponiert, potenziell infiziert Person war auf epidemiologisch relevante Weise (zum Beispiel hinreichend lang, hinreichend nah) einer ansteckenden Person ausgesetzt.

Referenzen

DP-3T Project (2020a). *Decentralized Privacy-Preserving Proximity Tracing: Overview of Data Protection and Security*. Project paper on Data Protection and Security 3rd April 2020.

– (2020b). *Decentralized Privacy-Preserving Proximity Tracing: Simplified Overview*. Simplified Three Page Brief 3rd April 2020.

– (2020c) [DP-3T-FAQ]. *FAQ: Decentralized Proximity Tracing*. URL: `https://github.com/DP-3T/documents/blob/master/FAQ.md` (besucht am 08. 04. 2020).

Apple App Store (2020). *Corona-Datenspende App des Robert Koch-Instituts*. URL: `https://apps.apple.com/de/app/corona-datenspende/id1504705422` (besucht am 08. 04. 2020).

Article 29 Data Protection Working Party (2007). *Opinion 4/2007 on the concept of personal data*. Working Paper WP 216.

– (2010). *Opinion 1/2010 on the concepts of »controller« and »processor«, adopted on 16 February 2010*. Working Paper WP 169.

– (2013). *Opinion 03/2013 on purpose limitation*. Working Paper WP 203.

– (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is »likely to result in a high risk« for the purposes of Regulation 2016/679, as last revised and adopted on 4 October 2017*. Working Paper WP 248.

– (2018). *Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017, as last revised and adopted on 10 April 2018*. Working Paper WP 259 rev.01.

Becker, Eberhard u. a. (2003). *Digital Rights Management: Technological, Economic, Legal and Political Aspects*. Berlin: Springer Science & Business Media.

Bieker, Felix, Benjamin Bremert und Marit Hansen (2018). »Die Risikobeurteilung nach der DSGVO«. In: *DuD – Datenschutz und Datensicherheit* 42 (8), S. 492–496.

Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das durch Artikel 12 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist (BDSG 2018) [BDSG 2018].

Bundesinnenministerium (4. Apr. 2020). *COVID-19-Eindämmung: Übergang von Verlangsamung zu Viruskontrollphase*. URL: `https://behoerden.blog/wp-content/uploads/2020/04/Transformation_zur_Post-Pandemie_Phase2_010_Final-1.pdf-1.pdf` (besucht am 11. 04. 2020).

BVerfG (10. Apr. 2020). Az. 1 BvQ 28/20.

Camenisch, Jan und Anna Lysyanskaya (2001). »An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation«. In: *Advances in Cryptology–EUROCRYPT 2001*. Hrsg. von Birgit Pfitzmann. Berlin: Springer, S. 93–118.

Coronakrise: Innenministerium skizziert Weg aus dem Lockdown (6. Apr. 2020). URL: `https://www.spiegel.de/politik/deutschland/coronakrise-innenministerium-skizziert-moeglichen-weg-aus-dem-lockdown-a-76007151-31ed-4383-a198-22dbaf781ccc` (besucht am 11. 04. 2020).

Dreyfus, Hubert L. (1972). *What Computers Can't Do*. 1. Aufl. New York: Harper & Row.

EDPB und EDPS (2019). *EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI)*. Adopted on 12 July 2019.

Ehmann, Eugen und Martin Selmayr, Hrsg. (2018). *Datenschutz-Grundverordnung*. 2. Aufl. München: C.H.Beck.

European Commission (2020). *Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*. Recommendation C(2020) 2296 final. URL: `https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf` (besucht am 10. 04. 2020).

European Data Protection Board (2019a). *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*. Version 2.0, adopted on 8 October 2019.

– (2019b). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. Adopted on 13 November 2019.

European Union (2002) [ePrivacy Directive]. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 4.7.2002, 37–47*.

– (2016) [GDPR]. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, 1–88*.

Friedewald, Michael u. a. (2017). *Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz*. White Paper. Version 3. Forum Privatheit.

GDPRhub (2020) [GDPRhub-Liste]. *Projects using personal data to combat SARS-CoV-2*. URL: `https://gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2` (besucht am 11. 04. 2020).

Gonscherowski, Susan, Marit Hansen und Martin Rost (2018). »Resilienz – eine neue Anforderung aus der Datenschutz-Grundverordnung«. In: *DuD – Datenschutz und Datensicherheit* 42 (7), S. 442–446.

Google, Inc. (2020). *Apple and Google partner on COVID-19 contact tracing technology. Company Announcements*. URL: `https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology` (besucht am 10. 04. 2020).

Halbfinger, David M., Isabel Kershner und Ronen Bergman (16. März 2020). »To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data«. In: *The New York Times*. URL: `https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html` (besucht am 08. 04. 2020).

Härting, Niko (13. Apr. 2020). »Zweck und Zweckbindung: Warum die Lockerung der Corona-Maßnahmen verfassungsrechtlich notwendig ist«. In: *CR-online.de Blog*. URL: `https://www.cr-online.de/blog/2020/04/13/zweck-und-zweckbindung-warum-die-lockerung-der-corona-massnahmen-verfassungsrechtlich-notwendig-ist/` (besucht am 13. 04. 2020).

Hoffmann, Bernhard (1991). *Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes*. Baden-Baden: Nomos Verlagsgesellschaft.

Hoffmann, Birgit (2017). »Einwilligung der betroffenen Person als Legitimationsgrundlage eines datenverarbeitenden Vorgangs im Sozialrecht nach dem Inkrafttreten der DSGVO«. In: *Neue Zeitschrift für Sozialrecht* (21), S. 807–812.

Kim, Nemo (6. Apr. 2020). »›More scary than coronavirus‹: South Korea's health alerts expose private lives«. In: *The Guardian*. URL: `https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives` (besucht am 08. 04. 2020).

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2018a) [DSK KP5]. *Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO*. Kurzpapier Nr. 5.

– (2018b) [DSK Liste VT]. *Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist*. Version 1.1, 17.10.2018. URL: `https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf` (besucht am 11. 04. 2020).

– (2018c) [DSK KP18]. *Risiko für die Rechte und Freiheiten natürlicher Personen*. Kurzpapier Nr. 18.

– (2019) [DSK SDM2.0a]. *Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele*. Version 2.0a.

Krempl, Stefan (6. Apr. 2020). »Polizei sammelt per Notstandsparagraf Daten von Corona-Infizierten. Die niedersächsische Datenschutzbehörde hat den Transfer von Listen über Covid-19-Patienten an die Polizei untersagt, doch die macht weiter«. In: *Heise Online*. URL: `https://heise.de/-4698172` (besucht am 06. 04. 2020).

Kühling, Jürgen und Benedikt Buchner, Hrsg. (2018). *Datenschutz-Grundverordnung / BDSG*. 2. Aufl. München: C.H.Beck.

Kühling, Jürgen und Mario Martini (2016). »Die Datenschutz-Grundverordnung – Revolution oder Evolution im Datenschutzrecht im europäischen und nationalen Datenschutzrecht?« In: *Europäische Zeitschrift für Wirtschaftsrecht*, S. 448–454.

Kwet, Michael (14. Juni 2019). »In Stores, Secret Surveillance Tracks Your Every Move«. In: *The New York Times*. URL: `https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html` (besucht am 08. 04. 2020).

Landau, Noa, Yaniv Kubovich und Josh Breiner (18. März 2020). »Israeli Coronavirus Surveillance Explained: Who's Tracking You and What Happens With the Data«. In: *Haaretz*. URL: `https://www.haaretz.com/israel-news/.premium-israeli-coronavirus-surveillance-who-s-tracking-you-and-what-happens-with-the-data-1.8685383` (besucht am 08. 04. 2020).

Laufer, Daniel (8. Apr. 2020). »Niedersachsen schickt weiter Coronalisten an die Polizei«. In: *Netzpolitik.org*. URL: `https://netzpolitik.org/2020/niedersachsen-schickt-weiter-coronalisten-an-die-polizei/` (besucht am 09. 04. 2020).

Lewis, Paul, David Conn und David Pegg (12. Apr. 2020). »UK government using confidential patient data in coronavirus response. Documents seen by Guardian show tech firms using information to build ›Covid-19 datastore‹«. In: *The Guardian*. URL: `https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response` (besucht am 14. 04. 2020).

Martin, Jeremy u. a. (2019). »Handoff All Your Privacy: A Review of Apple's Bluetooth Low Energy Continuity Protocol«. In: *arXiv:1904.10600*.

Neuerer, Dietmar (6. Apr. 2020). »Regierung startet Vorbereitungen für Corona-App-Kapagne«. In: *Handelsblatt*. URL: `https://www.handelsblatt.com/technik/`

medizin/digitale-virus-eindaemmung-regierung-startet-vorbereitungen-fuer-corona-app-kampagne/25717362.html (besucht am 11. 04. 2020).
Neumann, Linus (2020). *»Corona-Apps«: Sinn und Unsinn von Tracking*. URL: https://linus-neumann.de/2020/03/corona-apps-sinn-und-unsinn-von-tracking/ (besucht am 09. 04. 2020).
Österreichisches Rotes Kreuz (24. März 2020a). *Datenschutzinformation Stopp Corona App*. URL: https://www.roteskreuz.at/site/faq-app-stopp-corona/datenschutzinformation-zur-stopp-corona-app/ (besucht am 08. 04. 2020).
– (2020b). *Stopp Corona – FAQ*. URL: https://www.roteskreuz.at/site/faq-app-stopp-corona/ (besucht am 08. 04. 2020).
Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) (2020). URL: https://www.pepp-pt.org/ (besucht am 08. 04. 2020).
Podlech, Adalbert (1976). »Die Trennung von politischer, technischer und fachlicher Verantwortung in EDV-unterstützten Informationssystemen«. In: *Informationsrecht und Informationspolitik*. Hrsg. von Wilhelm Steinmüller. Rechtstheorie und Informationsrecht. München: Oldenbourg Verlag, S. 207–216.
– (1982). »Individualdatenschutz – Systemdatenschutz«. In: *Beiträge zum Sozialrecht – Festgabe für Grüner*. Hrsg. von Klaus Brückner und Gerhard Dalichau. Percha: Verlag R. S. Schulz, S. 451–462.
Privacy International (2020). *Bluetooth tracking and COVID-19: A tech primer*. URL: https://privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer (besucht am 10. 04. 2020).
Randow, Gero von (8. Apr. 2020). »Kleines Übel«. In: *Die Zeit* 16, S. 1.
Robert Koch-Institut (2020a). *Corona-Datenspende-App*. URL: https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Corona-Datenspende.html (besucht am 08. 04. 2020).
– (2020b). *Datenschutzhinweise der »Corona-Datenspende-App«*. URL: https://corona-datenspende.de/datenschutz-app/ (besucht am 09. 04. 2020).
Rost, Martin (2018). »Risiken im Datenschutz«. In: *Vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik* 57.1/2, S. 79–92. URL: http://www.maroki.de/pub/privacy/2018-05_Vorgaenge.html (besucht am 11. 04. 2020).
Rost, Martin und Sebastian Welke (2020). »SDM 2.0 und ITIL 4 ›verschränkt‹«. In: *DuD – Datenschutz und Datensicherheit* 44.4, S. 258–262.
Rudl, Tomas (23. Feb. 2020). »Jens Spahn lässt Testballon steigen«. In: *Netzpolitik.org*. URL: https://netzpolitik.org/2020/jens-spahn-laesst-testballon-steigen/ (besucht am 09. 04. 2020).
Schallbruch, Martin (7. Apr. 2020). »Lockdown ja – aber nur für Gefährder!« In: *Der Tagesspiegel*. URL: https://www.tagesspiegel.de/25719078.html (besucht am 08. 04. 2020).
Schulzki-Haddouti, Christiane (9. Apr. 2020). »Corona-Tracking-Apps mit PEPP-PT: ›Entscheidend ist für uns, dass der Datenschutz gewährleistet wird‹«. In: *Heise Online*. URL: https://heise.de/-4700336 (besucht am 09. 04. 2020).
Seidel, Ulrich (1984). »Voraussetzungen und Gestaltungsgrundsätze ›ordnungsgemäß wirkender Systeme‹«. In: *Koordination von Informationen*. Hrsg. von Rainer Kuhlen. Berlin: Springer, S. 190–194.
Specht, Luisa und Reto Mantz, Hrsg. (2019). *Handbuch Europäisches und deutsches Datenschutzrecht*. München: C.H.Beck.
Tremmel, Moritz (5. Apr. 2020). »Coronavirus: Österreich diskutiert verpflichtendes Tracking«. In: *Golem.de*. URL: https://www.golem.de/news/coronavirus-

`oesterreich-diskutiert-verpflichtendes-tracking-2004-147718.html` (besucht am 11. 04. 2020).

Troncoso, Carmela u. a. (2020). *Decentralized Privacy-Preserving Proximity Tracing*. White Paper Version: 10th April 2020.

Wolf, Heinrich Amadeus und Stefan Brink, Hrsg. (2017). *Beck'scher Online-Kommentar Datenschutzrecht*. München: C.H.Beck.

Index