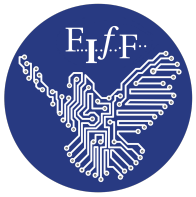


Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

Analyse und konstruktive Kritik der offiziellen Datenschutzfolgenabschätzung der Corona-Warn-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

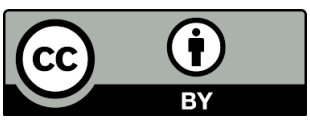
Version 1.0 – 29. Juni 2020

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

Kontakt: dsfa-corona@fiff.de

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

Version 1.0 erschienen am 29. Juni 2020.



Abstract

Am 15. Juni 2020 wurde die offizielle Datenschutzfolgenabschätzung (DSFA) für die Corona-Warn-App öffentlich zur Verfügung gestellt. Kurz darauf wurde die App dann in den App-Stores zum Download angeboten. Die vorliegende Analyse kommt zu dem Ergebnis, dass die vorgelegte DSFA ganz wesentliche grundsätzliche Schwächen aufweist und führt diese beispielhaft aus. Zunächst wird die in jedem Falle anzuerkennende Leistung der Projektgruppe zur Erstellung der App und der dazugehörigen DSFA gewürdigt. Danach wird schlaglichtartig an den Zweck einer DSFA erinnert. Dieser besteht nach Art. 35 DSGVO vornehmlich im Ausweis der Risiken für die Grundrechte und -freiheiten natürlicher Personen. Diese sind dabei unabhängig zu ermitteln und dürfen nicht im Sinne der Verantwortlichen zur Rechtfertigung der Verarbeitungstätigkeit nur vage angedeutet, kleingeredet oder anderweitig aus den Blick gestellt werden. In der Folge werden konkrete markante methodische, technische und rechtliche Mängel der vorliegenden DSFA zur CWA aufgezeigt. Als Hauptmängel der DSFA werden identifiziert: 1) die Konzentration nur auf die App selbst, nicht auf das ganze Verfahren, 2) das Fehlen der Einbeziehung der Verantwortlichen als datenschutzspezifischer Angreiferïn, 3) die geringe datenschutzrechtliche Durchdringung der Verarbeitung sowie 4) die unzureichende Diskussion effektiver Schutzmaßnahmen zu allen Risiken. Diese Mängel verweisen auf das geringe Niveau der Befassung der DSFA-Projektgruppe mit den Anforderungen an einen operativen Datenschutz. Dieser Beitrag unterbreitet konstruktive Anmerkungen und Vorschläge, die einen Weg zur Behebung dieser Mängel im Rahmen des notwendig zu betreibenden Datenschutz-Managementsystems weisen sollen.

Siehe auch: https://www.fiff.de/presse/dsfa-corona-cwa

Inhaltsverzeichnis

Nachdem sich Deutschland für einen datenschutzfreundlichen, dezentralen Ansatz zur automatisierten, App-basierten Kontaktnachverfolgung entschieden hatte, wurde am 16. Juni 2020 die Corona-Warn-App (CWA) durch das Robert Koch-Institut veröffentlicht. Im Vergleich mit anderen deutschen IT-Projekten wurde innerhalb kurzer Zeit ein technisch herausragendes System geschaffen. Es bedient sich aktueller Softwareframeworks, ist quelloffen und wurde teilweise mit transparenten partizipativen Arbeitsprozessen erstellt. Dabei wurden öffentlich formulierte Kritik sowie Beiträge der interessierten (Fach-)Öffentlichkeit vielfach berücksichtigt. Nun bleibt zu hoffen, dass damit ein neuer Standard auch für zukünftige IT-Projekte etabliert worden ist.

Der CWA wurde mit ihrer Veröffentlichung eine umfangreiche Datenschutz-Folgenabschätzung (DSFA) mitgegeben[1], die viele kritische Kernprobleme der CWA erkennt und entsprechende Datenschutzfragen aufwirft. Sie reagiert zudem explizit auf mehrere kritische Diskussionsbeiträge zu zentralen oder dezentralen Ansätzen sowie auf die Muster-DSFA des FIfF vom 14. April 2020 (https://www.fiff.de/dsfa-corona). Mit dem öffentlichen Zur-Verfügung-Stellen der CWA-DSFA wurde eine unserer politischen Forderungen an eine DSFA zu diesem gesellschaftlich hoch bedeutenden Thema erfüllt. Denn selbst mit einer tatsächlich grundrechteschonenden, vergleichsweise harmlosen Umsetzung einer Warn-App kann sehr gut begründet die Ansicht vertreten werden, dass damit die Hürde in eine technische Vollüberwachung von Einzelpersonen genommen wird. Die CWA gewöhnt Personen daran, sich unmittelbar in ihren Alltagsvollzügen kontinuierlich überwachen zu lassen. Ein Weg, diese Kritik aufzunehmen und mit ihr umzugehen, besteht gerade in öffentlichen Datenschutz-Folgenabschätzungen. DSFAen leisten insofern einen Beitrag zur systematischen und öffentlichen Diskussion der Überwachungs- und Kontrollaspekte der digitalisierten Gesellschaft.

Die CWA-DSFA hat einige Risiko-Aspekte zutreffend herausgearbeitet. So wurde die problematische Rolle des Exposure Notification Frameworks (ENF) von Google und Apple

1 https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf
https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung-anlage1.pdf
https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung-anlage2.pdf
https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung-anlage3.pdf
https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung-anlage4.pdf
https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung-anlage5.pdf

erkannt und analysiert bis hin zur Erkenntnis, „dass diese das ENF gemeinsam nach ihren Vorstellungen entwickelt und als eigene Systemfunktion in ihre jeweiligen Betriebssysteme integriert haben; die Speicherdauer von Tagesschlüssel und RPIs, die Konfigurationsparamater der BWE und die Verfügbarkeit des ENF werden einseitig von Google und Apple festgelegt. Apps dürfen nur auf die Funktionen und Daten des ENF zugreifen, wenn einseitige Vorgaben von Apple bzw. Google eingehalten werden. Insoweit bestimmen Apple und Google den Zweck und die wesentlichen Mittel der Verarbeitung durch das ENF.“ (Abschnitt 8.8.3)

Auch dem Identifikationsmerkmal „IP-Adresse“ wurde die verdiente wesentliche Relevanz zugeschrieben, die andernorts oft unterschlagen wird. Aus Datenschutzsicht geht es gemeinhin nicht darum, anhand von IP-Adressen den Klarnamen einer Person zu erlangen, um diese dann damit zu identifizieren. Nein, die IP-Adresse selbst ist bereits die Identifikation und daher personenbezogenes Datum, wie auch in den entsprechenden Urteilen des EuGH von 2016 und des BGH von 2017 festgestellt worden ist. Insofern heißt es richtig „Sofern und solange das RKI für sich genommen anonyme Daten in Verbindung mit einer IP-Adresse speichert oder anderweitig verarbeitet, handelt es sich für das RKI somit insgesamt um personenbezogene Daten.“ (Abschnitt 10.1.1). Die CWA-DSFA geht bezüglich der Schutzwürdigkeit der Daten an verschiedenen Stellen der Verarbeitung zum Teil sogar über unsere Analysen und Erkenntnisse von Mitte April 2020 hinaus, wenn es bspw. heißt: „Bei den vom CDN-Magenta heruntergeladenen Liste der Positivschlüssel anderer Nutzer, die lokal auf dem Smartphone des Nutzers weiterverarbeitet werden, handelt es sich für das RKI, solange sich diese Daten auf dem CDN-Magenta befinden, um Gesundheitsdaten, da sie auf eine Coronavirus-Infektion der Personen, die hinter dem jeweiligen Positivschlüssel bzw. der (früheren) Tagesschlüssel stehen, schließen lassen“ (Abschnitt 10.1.3).

All diese Punkte wurden treffend herausgearbeitet, doch es muss dennoch auch Kritik geübt werden. Im Folgenden werden wir jedoch keine detaillierte Analyse der CWA-DSFA vornehmen, sondern nur einige wenige, aber dafür wesentliche und kritische Aspekte der CWA-DSFA im Hinblick auf methodische, technische und rechtliche Defizite herausgreifen. Zunächst führen wir allgemeine Kritikpunkte an, wonach wir dann konkrete Stellen angehen und dafür Verbesserungen vorschlagen.

1. Allgemeine Kritikpunkte

Der vorgelegte DSFA-Bericht weist typische Mängel von DSFA-Projektgruppen auf, die über wenig Erfahrung in der Durchführung einer DSFA und des Berichts verfügen. Das ist deshalb ein bedrückendes Fazit, weil DSFAen seit Mai 2016 aufgrund der DSGVO zum Standard-Repertoire eines jeden Projekts zur Verarbeitung personenbezogener Daten gehören müssen und es inzwischen auch Expertise, Anleitungen und Methoden zur Durchführung von DSFA gibt. Nach unserem Eindruck wurde einzig das Kurzpapier Nr. 5 der Datenschutzbeauftragtenkonferenz (DSK) halbherzig zur Strukturierung des DSFA-Berichts angewendet. Jedenfalls war es auch nicht zu wenig Zeit für die Anfertigung einer angemessenen DSFA, denn die FIfF-Muster-DSFA hat gezeigt, wie in vierzehn Tagen mit in operativem Datenschutz – nicht nur in IT-Sicherheit und Datenschutzrecht – ausgebildeten Autorïnnen die bestehenden Grundrechtsrisiken, unter Annahme einiger technischer Voraussetzungen (z.B. der Dezentralität), ausweisen kann. Diese bereits Mitte

April ausgewiesenen Risiken sind aktuell nach wie vor gültig für alle dezentralen Umsetzungen.

Der vorliegende CWA-DSFA-Bericht impliziert ein hohes Maß an Orientierungslosigkeit bezüglich Datenschutz im allgemeinen, der Funktion einer DSFA im Besonderen sowie der methodischen Erfüllung der Anforderungen der DSGVO auf. Der DSFA-Bericht weist keinerlei Systematik aus, die aus der Problemstellung und der Erfüllung der – einzig maßgeblichen – Anforderungen der DSGVO abgeleitet ist. Anstatt die normativen Anforderungen des Datenschutzrechts vollständig und systematisch in funktionale Anforderungen zu transformieren – dass man dazu das von der DSK seit 2018 empfohlene Standard-Datenschutzmodell (SDM) nutzen kann und sollte, hatten wir mit unserer FIfF-DSFA gezeigt – werden die zu bearbeitenden Problemstellungen vornehmlich aus allgemeinem Wissen zur IT-Sicherheit sowie aus einer Sammlung von externen Beiträgen herangezogen. Neben unserer FIfF-DSFA wurden die Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 vom 21. April 2020 des Europäischen Datenschutzausschuss EDSA, die „10 Prüfsteine“ des CCC und die „Einordnung“ von Digitalcourage genutzt. Das ist sicherlich pragmatisch, diskursaufgreifend und geschickt, um in das Thema einzusteigen, als Form der Erarbeitung der Risiken aber unzureichend. Maßgeblich fehlt eine weitere Orientierung an den einschlägigen Leitlinien des EDSA, insbesondere zur Einwilligung (5/2020).

Es liegen drei substanzielle Mängel vor, die viele weitere Fehler in der Risikoanalyse einer DSFA nach sich ziehen. Zum einen bezieht sich die DSGVO – und damit eine DSFA – niemals auf nur eine ausgewählte technische Komponente, sondern immer auf die Verarbeitungstätigkeit als ganze. Zum zweiten fehlt ein durchgängig datenschutzspezifisches Angreifermodell insbesondere im Zusammenhang mit der Riskobearbeitung, das systematisch die Grundrechtseingriffe der Verantwortlichen und der von diesen beauftragten Technikbetreiber¨innen in den Vordergrund stellt, diskutiert und beurteilt. Und drittens werden auch die rechtlichen Konstellationen und Entscheidungen bzgl. Risikominimierung nicht hinreichend dargestellt und beurteilt.

1.1 Schutzfunktion einer DSFA

Die Funktion einer DSFA gem. Art. 35 DSGVO besteht darin, die Risiken einer Datenverarbeitung für Grundrechte von natürlichen Personen in erster Linie für die Verantwortliche – wir übernehmen generisch „die Verantwortliche“ als generelle Rollenbezeichnung aus der DSGVO – selber überhaupt sichtbar zu machen. Das ist oftmals eine Provokation, weil die Verantwortliche analytisch als Hauptangreiferïn für die Rechte und Freiheiten betroffener Personen gilt. Die Konstruktion ist gewagt: Die als Hauptangreiferïn geltende Verantwortliche ist zugleich diejenige, die Maßnahmen bestimmen und dann umsetzen soll, mit denen sich diese Risiken für die Betroffenen auf ein verantwortbares Maß verringern lassen. Dies ist aber zugleich der Grund für die Normierung von Schutzvorschriften durch das Datenschutzrecht und für die Anforderung einer DSFA für besonders riskante Verarbeitungstätigkeiten.

Ein DSFA-Bericht soll die Verantwortliche in die Lage versetzen zu veranlassen, dass Maßnahmen ergriffen werden, mit denen die aufgezeigten Risiken wirkungsvoll auf ein verantwortbares Maß verringert werden können. Sie muss aber ebenfalls auch explizit

aufzeigen, wenn wesentliche Risiken eben nicht verringert werden können. Letzteres kann zur Folge haben, dass eine Verarbeitungstätigkeit, gemessen an den Anforderungen der DSGVO, nicht wie geplant umsetzbar und damit unzulässig ist.

Eine abwiegelnde Thematisierung von Risiken – im vorliegenden DSFA-Bericht besonders deutlich im Kontext des Umgangs mit den von Google und Apple bereitgestellten betriebssystemeigenen Funktionen, und dem Verweis darauf, dass die Verantwortliche hier keine Schutzmaßnahmen plant – geht dann vollends am Zweck einer DSFA vorbei. Eine DSFA muss ganz im Gegenteil nämlich hinsichtlich erkannter Risiken hilfreiche Empfehlungen für Schutzmaßnahmen einfordern oder aber darstellen, dass die Risiken unbehandelt bestehen bleiben, d.h. offen bleibende Probleme und unbehandelte Risiken müssen als solche benannt werden. Es kann in Bezug auf die Problematik der bestehenden eklatanten Abhängigkeiten von den Herstellern von Smartphone-Betriebssystemen auch durchaus zu dem Schluss gekommen werden, dass diese proprietären Funktionen mangels hinreichender Prüfbarkeit der daran angeknüpften Verarbeitungen seitens der Hersteller nicht genutzt werden sollten.

1.2 Anforderungen und Methodik einer DSFA

Art. 35 DSGVO führt aus, welche Anforderungen an eine DSFA bestehen. Grundlage ist eine Beschreibung der Verarbeitungstätigkeit, wobei die Beschreibung notwendigerweise auf eine Dokumentation der Eigenschaften aller genutzten Komponenten zugreift. Die dafür sinnvollerweise heranziehbaren Methoden und Orientierungshilfen haben wir in unserer FIfF-DSFA ab S. 12 aufgelistet.

Der methodische Hauptfehler der vorgelegten CWA-DSFA besteht darin, dass nur die Funktionen der App in den Blick genommen werden, nicht aber die Prozesse der gesamten Verarbeitung mit all ihren Daten, allen eingesetzten IT-Komponenten und Prozessen (teilweise abgebildet im Überblick über die Architektur der CWA, Abb. 2, Abschnitt 8.1). Die Einbindung der Verifikationshotline in die DSFA zeigt in die richtige Richtung, aber auch dies hätte konsequenter erfolgen können (s. z.B. Abschnitt 10.2.3.5). Der Scope einer DSFA ist eine Verarbeitung (gem. Art. 4 Abs. 2 DSGVO), nicht nur eine IT-Komponente. Im vorliegenden CWA-Bericht werden zwar wesentliche Komponenten, wie etwa der Serverbetrieb in den Abbildungen 2 und 16 benannt, aber deren Funktionalitäten werden nur grob umrissen. Es wären die Datenflüsse und Datenbestände bis hin zu den Gesundheitsämtern und den beteiligten Ärztïnnen detailiert darzustellen, inklusive der Rechtsbeziehungen aller Beteiligten untereinander sowie letztlich immer mit Bezug zur Verantwortlichen.

Eine integre Datenschutzrisikoanalyse hätte z.B. großen Wert auf die Darstellung des bzw. der Server gelegt, auf den die Tagesschlüssel von Corona-Infizierten hochgeladen werden. Genau auf diese hochriskante Stelle hat die FIfF-DSFA eindringlich aufmerksam gemacht, weil vom Grad des Personenbezugs der infektionsanzeigenden Daten das gesamte datenschutzrechtliche Risiko abhängt. Es bleibt gegenwärtig jedenfalls intransparent, welche datenschutzrechtlich relevanten Eigenschaften die beteiligten Server aufweisen, welche Transaktionen und Daten dort protokolliert, ausgewertet und gelöscht werden. Eine vage Aussage, dass „seitens des RKI geplant ist, die IP-Adresse aus den Server-Logfiles auf dem CWA Server und CDN-Magenta unmittelbar nach Beantwortung eines Requests zu löschen“ und daher „der oben beschriebene Personenbezug in

Verbindung mit einer IP-Adresse für das RKI jedoch nur für eine ‚technische Sekunde'“ (Abschnitt 10.1.1) bestünde, genügt bei weitem nicht, weil diese Stelle bzw. dieser Moment in der gesamten Verarbeitungskette der heikelste Punkt ist, da hier die Tagesschlüssel von Infizierten via IP-Adresse personalisiert sind. Ein Versprechen der Verantwortlichen ist keine Schutzmaßnahme, vor der Verantwortlichen. Dazu folgen detailliertere Ausführungen weiter unten im Dokument.

Im übrigen ist eine DSFA als solche nicht als ein „lebendiges Dokument“ (Abschnitt 1) aufzufassen bzw. anzulegen. Ein DSFA-Bericht beansprucht einen gewissen Abschluss der Analyse und Erkennentisse und schließt mit konkreten Empfehlungen zur Risikominimierung. Gleichwohl muss der Verantwortliche für die Verarbeitungstätigkeit selbstverständlich auf weitere Änderungen im Kontext der Verarbeitungstätigkeit reagieren können. Das jedoch ist die Funktion eines Datenschutzmanagements. Das heisst, eine DSFA ist an ein Datenschutzmanagement zu übergeben, in diesem Falle an das hoffentlich tatsächlich existierende Datenschutzmanagementsystem, und das meint mehr und anderes als nur die Bestellung einer oder eines Datenschutzbeauftragten, beim RKI.

1.3 Die Verarbeitungstätigkeit (vor DSGVO: „das Verfahren“)

Zur Beschreibung der Verarbeitungstätigkeit als einem systemischen Zusammenhang empfiehlt sich, a) die Abfolge der Zwecksetzung, Zweckbeschreibung, Zwecktrennung und Zweckbindung, so wie es das SDM V2 vorschlägt, zu beschreiben und b) sich zumindest an den 14 Subprozessen zu orientieren, die in Art. 4 Nr. 2 der DSGVO als Komponenten einer Verarbeitung aufgezählt sind. Die Darstellung der datenschutzrechtlich wesentlichen funktionalen Eigenschaften kann dann entlang der Risiken, gebildet aus den Grundsätzen des Artikel 5 DSGVO, bzw. bei primär funktionaler Orientierung aus den kompakten Gewährleistzungszielen des SDM, erfolgen.

Sich nicht am Verfahren, sondern hauptsächlich an der CWA App zu orientieren, hat im Konkreten dann zu der fatalen Annahme in Abschnitt 10.1 geführt, nämlich dass die lokal bzw. „offline“ verarbeiteten Daten auf dem Smartphone nicht als Teil der Verarbeitungstätigkeit des Verantwortlichen gelten. Die CWA App ist Teil des Verfahrens, insofern sie zur Zweckverwirklichung beiträgt. Sie ist zudem ein Produkt der technischen Gestaltung durch oder im Auftrag des Verantwortlichen und bestimmt damit prinzipiell die möglichen Folgen des Technikeinsatzes. Nicht zuletzt kontrolliert und steuert der Verantwortliche den Patch- und Update-Management-Prozess der CWA App (über die Bereitstellung neuer signierter Software-Versionen im „App bzw. Play Store“), an dem die CWA-Nutzenden teilnehmen, und beeinflusst damit auch zukünftig das Verfahren und seine Folgen. Bei einer verfahrensorientierten Analyse wäre dies im Unterschied zu einer anwendungsorientierten Analyse ersichtlich geworden. Die hier nachgelagert zu betrachtenden Folgen hätten dann nicht nur das Risiko der Deanonymisierung durch den Verantwortlichen selbst zu behandeln (Abschnitt 10.1.2), sondern auch Risiken durch Software-Fehler oder verwendeter Be1.3 Die Verarbeitungstätigkeit (vor DSGVO: „das Verfahren“)triebssystemfunktionen, die zum Beispiel zu einer Deanonymisierung durch Dritte führen können. Damit dies nicht geschieht, muss ein dem Risiko angemessenes Schutzniveau auch auf den Smartphones gewährleistet sein (Art. 32 Abs. 1 DSGVO).

Obwohl in der DSFA unter „Corona-Warn-App“ nicht nur die App selbst, sondern an vielen Stellen auch die CWA Server verstanden werden, finden sich keine Ausführungen zu den Servern. Gerade dieser Bereich ist aber sensibel und für das (nicht vorhandene) Angreifermodell relevant. Weil neben Angriffen Dritter es gerade die Server-Betreiberïn selbst ist, die die Verarbeitungen auf dem Server relativ leicht beeinflussen kann. So wäre beispielsweise zu erläutern gewesen, wie sich der CWA Server von den übrigen Servern (Testresult-, Portal-, Verification-Server, CDN) im Hinblick auf die von ihrer Funktion ausgehenden Risiken unterscheiden. Weiterhin fehlt eine systematische Beschreibung von Schnittstellen bzw. Kommunikationsbeziehungen sowie deren Zweck, Art der übertragenen Informationen, Zugriffsarten und zugehörige Schutzmaßnahmen. Daraus muss dann vor allem hervorgehen, inwiefern Daten an andere (gemeinsam) Verantwortliche oder zur Auftragsdatenverarbeitung weitergeleitet werden, z. B. von oder zu Arztpraxen, Laboren, Rechenzentren von SAP/Telekom oder Betriebssystemherstellern, um riskante Stellen für pontentielle Zweckentfremdung (gemäß dem Schutzziel der Nicht-Verkettbarkeit und Vertraulichkeit) zu identifizieren. Sie sind von „entscheidender Bedeutung für die rechtliche Verantwortlichkeit, Beherrschbarkeit und Prüfbarkeit von Datenflüssen“ (SDM V2, S. 39).

1.4 Risikomodellierung

Ein weiterer eklatanter konzeptioneller Methodik-Fehler ist das Fehlen einer datenschutzspezifischen Risikomodellierung. Das liegt ersichtlich am generellen Fehlen einer hinreichenden Orientierung im operativen Datenschutz. Aus Datenschutzperspektive gilt der Verantwortliche selber als Hauptangreifer auf die Rechte und Freiheiten natürlicher Personen; die Grundsätze aus Artikel 5 DSGVO bilden dann die Kriterien, mit denen Risiken zu beobachten und zu beurteilen sind. Diese methodische Herangehensweise gilt seit spätestens 2017 als gute DSFA-Praxis („Stand der Technik“) bei denjenigen, die operativen Datenschutz von Themen der IT-Sicherheit zu unterscheiden wissen. Das kann und das muss man inzwischen auch wissen, wenn man ein solches Projekt auf die Beine stellen soll.

Das spezifische Datenschutzrisiko für CWA Nutzende besteht darin, dass die Grundrechtseingriffe durch den Verantwortlichen und „seine“ Datenverarbeitung zu intensiv sind und die Datenschutzgrundsätze nicht erfüllt werden. Das heisst konkretisiert, dass bspw. die Vertraulichkeit, Integrität und Zweckbindung der Datenverarbeitung an irgendeiner Stelle in der gesamten Verarbeitungskette – und nicht nur auf dem Smartphone selber – nicht hinreichend gesichert werden und keine Prüf- und Testmöglichkeiten (Transparenz) dafür bestehen, um zu erkennen, ob die Schutzmaßnahmen auch tatsächlich wirksam sind und nachweisbar sicher funktionieren. Und zwar zum Schutze der Betroffenen, was nicht der Sicht der IT-Sicherheit entspricht. Deshalb sind solche notwendigen Zusicherungen wie im Glossar (Abschnitt 4.1) zu vage und nutzlos, wenn es z.B. heisst, dass „die Begegnungs-Aufzeichnung vom CWA-Nutzer jederzeit auch als Ganzes aktiv gelöscht werden kann. Die Daten im Betriebssystem (gesammelte und eigene Tagesschlüssel) werden nicht gelöscht, sondern verbleiben für 2 Wochen gespeichert im geschützten Betriebssystemspeicher.“ An dieser Stelle entfällt die Kontrollfähigkeit durch die CWA Nutzenden und es kommt ein weiteres Transparenzproblem hinzu. Es bleibt unklar, was mit den Begegnungs-Aufzeichnungen im folgenden geschieht. Können diese Informationen z. B. trotz Löschung auf den Server hochgeladen werden? Welche Rolle spielt es, dass der Betriebssystemspeicher ein

besonders geschützter Bereich ist? Und was bedeutet das genau? Hat die Tatsache, dass es ein besonders geschützter Bereich ist, überhaupt Auswirkungen auf die Risiken für Grundrechte oder auf deren Minimierung, wenn dieser Bereich durch keine der betroffenen Instanzen – RKI, CWA Nutzende, DS-Aufsichtsbehörden – kontrollfähig ist?

Die Durchführung einer DSFA ist, innerhalb der DSGVO, wiederum eine wesentliche Anforderung, um Art. 25 DSGVO umzusetzen. Art. 25 verlangt, dass Datenschutz-Anforderungen bereits in der Planungsphase zu berücksichtigen sind, also insbesondere die Einsichten, Beurteilungen und letztlich die Empfehlungen aus der DSFA. Ein DSGVO-konformer DSFA-Bericht kann deshalb niemals zwei Tage, oder wie im vorliegenden Fall, zehn Stunden vor der Auslieferung einer Applikation und dem Beginn der eigentlichen Verarbeitung zweckbestimmt vorliegen. Ein solcher Bericht kann dann nicht der umsichtigen Planung dienen sondern nur der formalen Legalisierung des Verfahrens. Diese zeitliche Verzögerung ist auch im Hinblick auf das Einbeziehen des Standpunkts der betroffenen Personen (Art. 35 Abs. 9) kritisch zu sehen, da Art, Umfang und Umstände dieser Verarbeitung eine gesellschaftliche Debatte im Vorfeld nahe legen. Erst eine frühzeitige Veröffentlichung schafft Öffentlichkeit und damit die Bedingungen für die Einbeziehung von verschiedenen Standpunkten für genau diese Verarbeitungstätigkeit. Ein passives Abwarten von Fachveröffentlichungen und Medienberichten wird dieser Verantwortung nicht gerecht und Internet-Recherchen im thematischen Umfeld sind leider zu wenig bzw. nicht zielführend, da der kritische Diskurs am Gegenstand selbst stattfinden muss. Aus Projektleitungssicht wäre daher die Verschiebung des Go-lives der richtige Weg gewesen.

2. Konkrete Punkte konstruktiver Kritik

2.1 Abspaltung des Personenbezuges beim Upload der Positivschlüssel

Ein zentraler, wenn nicht sogar der zentrale verwundbare Punkt für die Betroffenen besteht in dem Moment, in dem die Tagesschlüssel von positiv Getesteten auf den CWA-Server hochgeladen werden und dadurch zu Positivschlüsseln werden. Durch die Metadaten der Verbindung, konkret die IP-Adresse beim Upload, ist die infizierte Person direkt identifizierbar. Ein Vertrauen in simples Löschen der entsprechenden Einträge in den Logdateien durch die Betreiberin reicht bei einem solchen garantiert hohen Risiko für die Betroffenen (Abschnitt 10.1.1) mit Rückblick auf die lange Geschichte grundrechtseinschränkender Anti-Terror- und Sicherheitsgesetze nicht aus. Vielmehr müssen umfassende, nicht nur technische Anforderungen gestellt werden, um eine De-Pseudonymisierung oder sonstige Identifikation der App-Nutzenden hinreichend zu erschweren. Dies ist konkret durch rechtliche, organisatorische und technische Maßnahmen zu verhindern, wie wir in den Empfehlungen in unserer DSFA (siehe DSFA-Kapitel 9 – Empfehlungen) ausführen. Organisatorisch müssen der Verantwortliche strategisch und die Betreiberïnnen operativ eine Mischstruktur etablieren, um dieses Ziel zu erreichen. Der Verantwortliche – also das RKI – kann etwa strategisch mehrere unterschiedliche Betreiberïnnen auswählen: eine betreibt die Eingangsknoten im Netzwerk und die andere die Server, auf denen gespeichert wird. Operativ sollte die Abtrennung des Personenbezuges innerhalb der Organisationen durch eine zweckdienliche

Abteilungsstruktur, Funktionstrennung und Rollentrennungen etc. sichergestellt werden, die die informationelle Gewaltenteilung – also die funktionale Differenzierung – innerhalb der Organisation durchsetzen. Der mit Abstand wirksamste Schutz bestündet in einem technischen Maßnahmenbündel, um eine ausreichende Sender-Anonymität an der Schnittstelle zur Infrastruktur der Betreiberïn zu gewährleisten. Hier sind Lösungsansätze wie „distributed trusted server“ oder Anonymisierungsinfrastrukturen von unabhängig en Organisationen denkbar (ohne an dieser Stelle die Lösungsarchitektur vorwegzunehmen). Denn als Betreiberïnnen kommen in einer „trusted infrastructure“ nur solche Organisationen in Frage, die kein eigenes Interesse an den Daten haben. Damit bestände auch ein wirksamer Schutz gegen die Pflicht zur Herausgabe von Daten, auch gegenüber Sicherheitsbehörden, die es einfach mal versuchen. Die Auslassung einer solchen kritischen Komponente der Datenschutzarchitektur könnte als ein schwerwiegender Grund für die Einstellung der Verarbeitung beurteilt werden. Man darf sich nicht auf Fiktionen wie das „Vertrauen der Nutzer, dass sich der Betreiber rechtskonform verhält und nur bei Vorliegen der gesetzlichen Voraussetzung Daten an Strafvervolgungsbehörden herausgibt“ (Designentscheidung D-11-1) berufen, wenn es darum geht, Risiken auszuweisen. Zur rechtlichlichen Absicherung kann die Abspaltung des Personenbezugs durch ein Begleitgesetz festgeschrieben werden.

2.2 Der Umgang mit Risiken beim ENF

Der Rückgriff auf Techniken und Services der Betriebssysteme Google Android und Apple iOS ist ein weiterer ganz zentraler Punkt, an dem es architektonisch besonders heikel wird. Die damit verbundenen Risiken werden nur indirekt thematisiert, indem die Verantwortung dafür zurückgewiesen wird. Der Rückzug auf Nichtwissen gleich am Anfang des DSFA-Berichts (ENF, S. 2) ist unangemessen und wird den Anforderungen an das schonungslose detailierte Explizieren von Risiken und der Verantwortlichkeit, die trotz allem besteht, nicht gerecht. Die DSGVO verlangt genau das, nämlich die Übernahme der Verantwortung für das Funktionieren und die Datenschutzkonformität des gesamten Systems. Insbesondere, wenn auf S. 43 konstatiert wird, dass „die CWA App und das ENF […] zentrale Komponenten des Gesamtsystems der CWA“ sind. An diesem Punkt zeigt sich insofern nicht nur methodische Imkompetenz, sondern auch rechtliche Orientierungs- und vielleicht sogar politische Verantwortungslosigkeit. Diese Risiken müssen vom Verantwortlichen erkannt, bearbeitet und zumindest unter rechtliche Bedingungen gestellt werden. Diese Risiken dürfen – anders als im Kontext der IT-Sicherheit – eben nicht schlicht akzeptiert werden. An dieser Stelle müsste eine integre DSFA das Konzept der „gemeinsamen Verantwortung“ prüfen und Möglichkeiten rechtskonformer Ausgestaltung der CWA empfehlen. Zwar ist es zweifelsohne schwierig, Google und Apple auf Augenhöhe die rechtlichen und praktischen Konsequenzen aufzuzwingen, gerade wenn man von deren Techniken abhängig ist. Aber so wie hier von vornherein ganz auf die rechtliche Erörterung und ein Ausloten der Möglichkeiten zu verzichten, ist jedenfalls keine Lösung. Natürlich: Die Ergebnisse einer Analyse können sehr unangenehm sein, doch das sind die Folgen für die Betroffenen umso mehr.

Wenn also „eigene Erkenntnisse über die innere Funktionsweise […] nicht gewonnen werden [können], da dieses Framework aus Sicherheitsgründen in einer Art und Weise implementiert ist, die eine Untersuchung ausschließen“, dann kann eben nicht einfach „auf die Richtigkeit der Verarbeitung in den Frameworks und der Beschreibungen vertraut“ (Abschnitt 1) werden. Das genau geht in einer DSFA nicht! Natürlich wird hier eine weltweit

bestehende Clinch-Situation angedeutet, die aber als gravierendes Risiko deutlich gemacht werden muss, ebenso wie die Tatsache, dass diesem Risiko aktuell in keiner Weise tatsächlich auf einem insgesamt korrekten Wege begegnet werden kann. Eine Einsichtnahme in den Quellcode des ENF wäre jedoch das Mindeste, was überhaupt nur in die Nähe einer Schutzmaßnahme käme.

Ein weiterer Vermeidungsansatz zur Beschäftigung mit den Risiken besteht in der Schutzbehauptung, dass „die Nutzer durch die Verwendung eines Android- bzw. iOS-Smartphones zum Ausdruck gebracht [haben], dass sie grundsätzlich Vertrauen zu diesen Herstellern haben oder sich jedenfalls mit den Datenschutzrisiken, die mit der Verwendung eines Smartphones dieser Hersteller für persönliche Zwecke einhergehen, abgefunden oder andernfalls ihr Nutzungsverhalten entsprechend angepasst haben“ (Abschnitt 11.2.4). Im Unterschied jedoch zu universellen und grundsätzlichen Multizweck-Betriebssystemfunktionen wie WLAN, Mobilfunk, Kamera oder Datenspeicher ist das ENF ein hochspezialisierter Service, der einzig und allein für Corona-Apps geschaffen worden ist und nur mit diesen funktioniert und somit notwendig für den CWA-Betrieb ist. Er ist also nicht normaler „Infrastrukturbestandteil“ des Smartphone-Betriebssytems, sondern fester Bestandteil – also Mittel – der App und ihres Zweckes.

2.3 Einwilligung und Verantwortlichkeit

Die DSFA ist gem. Art. 35 Abs. 1 DSGVO von dem datenschutzrechtlich Verantwortlichen durchzuführen. Die datenschutzrechtliche Verantwortlichkeit für eine Verarbeitungstätigkeit kann nicht einfach einer Instanz zugewiesen oder behauptet werden „Das RKI [sei] Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO für die mit dem Betrieb der CWA einhergehenden Verarbeitung von personenbezogenen Daten der Nutzer“(Abschnitte 6.1 und 8.8.1). Eine datenschutzrechtliche Verantwortlichkeit ist entsprechend der Regelung in Art. 4 Nr. 7 DSGVO zu bestimmen. Danach ist verantwortlich, wer die Zwecke und Mittel der Verarbeitung bestimmt. Etwas anderes kann nur dann gelten, wenn die Zwecke und Mittel dieser Verarbeitung durch ein Gesetz vorgegeben werden. Nur in diesem Fall kann der Verantwortliche bestimmt werden beziehungsweise können die in einem Gesetz bestimmten Kriterien die Benennung des Verantwortlichen nach rechtlichen Vorgaben vorsehen.
Eine solche gesetzliche Bestimmung der Verantwortlichkeit ist bislang nicht erfolgt. Für alle Verarbeitungen der CWA wäre daher konkret zu bestimmen gewesen, welche Stelle(n) die Zwecke der Verarbeitung festlegen und wer die Mittel dafür bestimmt. Ausweislich der Projektskizze (Abschnitte 5 und 8.8.4.1) hat das Bundesministerium für Gesundheit die Zwecke der Verarbeitung (Warnung vor Infektion und Benachrichtigung bei Infektion) und das Mittel, nämlich die Verwendung einer App, bestimmt. In der DSFA wäre zu diskutieren, welche Aufgaben im Hinblick auf die Bestimmung der Mittel und Zwecke auf das RKI im Rahmen des Betriebs tatsächlich übergehen. Genauso wäre zu ermitteln gewesen, ob eine gemeinsame Verantwortlichkeit mit Apple und Google durch Einbindung der ENF-Funktionalität entsteht und welche Folgen sich daraus ergeben (Abschnitt 8.8.3). Denn ausweislich der CWA-DSFA hat weder das Bundesministerium noch das RKI noch deren Auftragsverarbeiter Einfluss auf diesen Teil der App-Funktionalität. Es ist aber nicht von der Hand zu weisen, dass eine gemeinsame zweckgerichtete Bestimmung der ENF stattgefunden hat, denn das Bundesministerium hat sich öffentlichkeitswirksam für die von Apple und Google angebotene Technologie entschieden (https://www.zeit.de/digital/datenschutz/2020-04/datenschutz-corona-tracing-app-

dezentrale-speicherung).

Die Verantwortlichkeit setzt nicht voraus, dass auch die technischen Details hochauflösend durch den Verantwortlichen bestimmt werden. Soweit aber eine gemeinsame Verantwortlichkeit angenommen wird, hätte auf Art. 26 DSGVO und die daraus resultierenden Risiken hingewiesen werden müssen. Die Diskussion der Verantwortlichkeit der App-Nutzenden und damit eine Verkehrung der Rolle als Betroffene zeugt von einem grundsätzlichen Unverständnis des Datenschutzrechts. Sie käme maximal in Bezug auf die Speicherung und den Abgleich der Positivschlüssel anderer Nutzender in Betracht. Vor dem Hintergrund, dass die CWA-DSFA von der Rechtsgrundlage einer Einwilligung ausgeht, deren wesentlicher Regelungsgegenstand genau diese Verarbeitungen darstellt, befremden diese Ausführungen aber ebensosehr wie diejenigen, die die Ablehnung der Verantwortlichkeit für die Betroffenendaten thematisieren. Denn die Ausübung von Betroffenenrechten (z.B. Widerruf) gegenüber dem Verantwortlichen kann nicht zu einer Verantwortlichkeit der Betroffenen führen (Abschnitt 8.8.3). In Abgrenzung zur Verantwortlichkeit wären vielmehr die Auftragsverarbeiter zu bestimmen und die Risiken, die sich aus einer Auftragsverarbeitung ergeben, zu diskutieren gewesen.

Im Abschnitt 10 wäre eine stärker an den rechtlichen Vorgaben orientierte Gliederung hilfreich gewesen. Grundvoraussetzung für eine datenschutzrechtliche Bewertung ist ein Verständnis des Artikels 1 Abs. 2 DSGVO bzgl. der Rechte und Freiheiten natürlicher Personen, der datenschutzrechtlichen Grundprinzipien und der Begrifflichkeiten. Bei der Bestimmung und der Befassung mit dem Personenbezug an sich ist die Frage nach dem Umfang (so aber gestellt in Abschnitt 10.1) der personenbezogenen Daten irrelevant. Dieser spielt lediglich für die Einschätzung des Risikos, das durch eine Verarbeitung großer Mengen an personenbezogenen Daten entsteht, eine Rolle. Die Nichtauflösung des Personenbezugs zwischen Inhalts- und Transportdaten in den Server-Logfiles (Abschnitt 10.1.1) stellt ein Risiko dar, das auch als solches auszuweisen und zumindest unter rechtliche Bedingungen zu stellen gewesen wäre. Dies ist eines der Hauptrisiken möglicher Angriffsszenarien (siehe oben) und müsste fortan Gegenstand regelmäßiger Audits sein.

Die Unterscheidung der anfallenden Datenkategorien nach ihrem Verarbeitungsort (Personenbezogene Daten "beim RKI" in Abschnitt 10.1.1 und Lokale Datenverarbeitung auf dem Smartphone in Abschnitt 10.1.2) ist zwar grundsätzlich sinnvoll, jedoch ist die DSFA nicht der geeignete Ort, anhand der Datenkategorien Fragen der Verantwortlichkeit zu diskutieren. Zudem liegt die lokale Verarbeitung (Abschnitt 10.1.2) auf den Apps nicht außerhalb des faktischen Einflussbereichs des Verantwortlichen, dieser bestimmt die Technikgestaltung und damit die Möglichkeiten, mit denen die Nutzenden z. B. ihre Einwilligungen durch explizite Handlungen zum Ausdruck bringen können. Auch haben die Nutzenden keine Einflussmöglichkeiten auf die technische Gestaltung der CWA. Warum es sich überhaupt bei einer lokalen Datenverarbeitung um Kategorien von personenbezogenen Daten handeln soll, bleibt unerfindlich und wäre in der Beschreibung der Verarbeitung zu thematisieren gewesen. Zu vermuten ist, dass in diesem Abschnitt eigentlich die Kategorien personenbezogener Daten, die auf den Smartphones verarbeitet werden, diskutiert werden sollten, offenbar mit dem Ziel, den Verantwortlichen aus dem Verfahren heraus zu subsumieren. Der Hinweis auf die Bedenken des BfDI daran, die Verantwortlichkeit für die Verarbeitung auf den Smartphones zu verneinen, zeigt in diese

Richtung. Verkannt wird in diesen Erörterungen, dass es beim Personenbezug nicht darauf ankommt, ob dieser vom Verantwortlichen überhaupt oder zu jeder Zeit hergestellt werden kann. Die Anforderungen des Datenschutzes durch Technikgestaltung (Art. 25 DSGVO) gebieten vielmehr, die Datenschutzgrundsätze wirksam umzusetzen. Maßnahmen ändern nichts an der Verantwortlichkeit für das Verfahren der CWA.

Entgegen der Ausführungen in der CWA-DSFA kommt es nach Ausführungen im Breyer-Urteil des EuGH (C-582/14) darauf an, dass der Verantwortliche „über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen“ (Rn. 49). Solche rechtlichen Möglichkeiten, auf IP-Adressen der Nutzenden zuzugreifen, hat auch das RKI als Betreiberin. Damit ist es grundsätzlich in der Lage, die Identifier der Tages- oder Positivschlüssel auf die Nutzenden zurückzuführen. Der Umstand, dass der Verantwortliche die Daten bei Google und Apple nicht zuordnen kann, ändert nichts an deren Personenbezug, sondern unterstreicht noch einmal die gemeinsame Verantwortlichkeit für deren Verarbeitung im Verfahren.

Art. 5 Abs. 2 i.V.m. Abs. 1 lit. a DSGVO verlangen vom Verantwortlichen die Rechtmäßigkeit der Verarbeitung. Mit dieser Frage beschäftigt sich Abschnitt 10.2 der CWA DSFA. Hier ist anzumerken, dass die Erfüllung der Voraussetzungen einer Rechtsgrundlage eine notwendige Bedingung für die Rechtmäßigkeit der Verarbeitung ist. Die Rechtsgrundlage allein macht eine Verarbeitung aber noch nicht zulässig. Hinzukommen muss die Erfüllung weiterer Voraussetzungen, die die DSGVO an Verantwortliche stellt. Im Hinblick auf die Einwilligung als Rechtsgrundlage ist zu beachten, das deren Wirksamkeit nicht pauschal angenommen werden kann, sondern das Vorliegen der Voraussetzungen im Einzelfall, d.h. für jede einwilligende Person und für jeden Zweck nachzuweisen ist. Die Voraussetzungen der Einwilligung ergeben sich aus Art. 6 Abs. 1 S. 1 lit. a, 7 und 4 Nr. 11 DSGVO. Zur Auslegung und Anwendung hat der EDSA eine Stellungnahme herausgegeben (Guidelines 05/2020 on consent under Regulation 2016/679, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf). An dieser Stelle ist darauf hinzuweisen, dass es gem. Art. 70 Abs. 1 DSGVO die Aufgabe des EDSA ist, Hinweise für die Auslegung der DSGVO zu geben; deren Lektüre und Beachtung im Rahmen der DSFA zur CWA ist dringend anzuraten.

Art. 4 Nr. 11 setzt voraus, dass die Einwilligung 1) freiwillig, 2) konkret, 3) informiert und 4) mit einer unmissverständlichen Willensbekundung in Form einer Erklärung oder eindeutigen bestätigenden Handlung abgegeben wird. Zu unterscheiden ist die Einwilligung als Rechtsgrundlage im Hinblick auf das Verfahren und die Einwilligung in die Verarbeitung besonderer Kategorien von Daten gem. Art. 9 Abs. 2 lit a DSGVO. Der DSFA mangelt es auch hier an dem erforderlichen Detailierungsgrad der Darstellung und der Risikodiskussion. Gerade bei einer Verarbeitung von Gesundheitsdaten unter Verwendung einer, für diese Zwecke neuartigen, Tracing-Technologie hätte es einer detaillierten Erörterung bedurft. In einer DSFA geht es auch nicht nur darum, gesetzlich vorgegebene Kriterien zu wiederholen, sondern es bedarf einer Auseinandersetzung mit den Anforderungen im Hinblick auf die Gewährleistung ihrer Erfüllung, also mit einer Operationalisierung normativer Anforderungen in funktionale Anforderungen. So wäre z. B. auszuführen gewesen, welche Informationen über das Verfahren und seine Zwecke für die

Informiertheit der Einwilligung erforderlich sind, welche Risiken sich ergeben können und Hinweise darauf, wie dies in der CWA umgesetzt wurde bzw. wie den Risken begegnet wird. Ein Hinweis darauf, dass „nicht ersichtlich [sei], dass diese Information dem Nutzer im Vorfeld einer Einwilligungserteilung nicht zuverlässig vermittelt werden könnten“ (Abschnitt 10.2.3.2) reicht dafür keinesfalls aus. Es kann eben nicht von einer Handlung der Nutzenden auf deren Informiertheit geschlossen werden.

Auch in Bezug auf Freiwilligkeit ist auf das Dokument des EDSA zu verweisen. Insbesondere fehlt in der CWA-DSFA eine Erörterung des Umstandes, dass mit der Nutzung der App beim Erhalt einer Warnung eine symptomunabhängige Testmöglichkeit verbunden ist; diese Möglichkeit wird Nicht-Nutzenden der CWA nicht zugestanden. Der Hinweis, der Gesetzgeber plane derzeit keine verpflichtende Nutzung oder mache die App zur Voraussetzung für Lockerungen, sind nur bedingt für eine Risikoabschätzung geeignet, auch weil bereits Bundestags- und Landtagsabgeordnete genau diese Forderung öffentlich erhoben haben. Hier wäre z. B. die Möglichkeit einer „zweiten Welle“ zu diskutieren und Anforderungen an den Verantwortlichen bzw. den Gesetzgeber zu formulieren gewesen, wie Freiwilligkeit dauerhaft sichergestellt werden kann. Weder der Umstand, dass nicht alle Bürgerinnen und Bürger über ein App-fähiges Smartphone verfügen noch der Umstand, Personen könnten eine App auf einem alten oder Zweit-Smartphone installieren, um die Bedingungen der Freiwilligkeit der Nutzung nachzuweisen, sind taugliche Argumente. Die aktuellen Diskussionen (s. z.B. https://www.golem.de/news/lockerungsdebatte-steuervorteile-fuer-corona-app-nutzer-gefordert-2004-148137.html) um die CWA als Einlass-Voraussetzung oder andere mit ihr verbundenen Vorteile zeigen die alltägliche Relevanz dieses Risikos. Entscheidend ist aber, dass die Anforderungen der Einwilligung bei jedem individuellen Nutzenden vorliegen müssen und damit auch die der Freiwilligkeit. Eine DSFA muss sich mit der Frage auseinandersetzen, wie eine Situation zu beurteilen ist, in der bei einer Mehrzahl oder zumindest großen Zahl von Nutzenden aufgrund von Solidaritätsgefühlen oder Arbeitgeberzwang nicht mehr von einer freiwilligen Nutzung ausgegangen werden kann. Im Mindesten wäre also eine gesetzliche Regelung als Maßnahme anzusprechen gewesen.

Zu diesem Thema der Durchdringung der Bevölkerung mit CWA-fähigen Geräten und deren freiwilligen Nutzung finden sich zwei gegenläufige Aussagen. So heisst es in Bezug auf Freiwilligkeit: „Auch insoweit könnte sich die Freiwilligkeit der Nutzung der CWA zu einem faktischen Zwang durch sozialen Druck umwandeln. Jedoch ist zu bedenken, dass ein erheblicher Teil der Bevölkerung gar kein oder kein geeignetes Smartphone besitzt, insbesondere wenn es sich um besonders junge, alte oder kaufschwache Personen handelt.“ (Abschnitt 10.2.3.3) Beim Abschnitt zur Eignung auf findet sich wiederum einen gegensätzlich Erwartung: „Es wird davon ausgegangen, dass ein Großteil der Bevölkerung ein geeignetes Smartphone besitzt und meistens bei sich trägt und dass die Technologie BLE grundsätzlich geeignet sein kann, um eine ausreichend präzise Entfernungsmessung für die Protokollierung von Kontakten im Rahmen der Risiko-Ermittlung durchzuführen.“ (Abschnitt 11.2.2) Was ist also die Grundannahme? Vom Verantwortlichen muss entweder die Annahme zur Freiwilligkeit oder die zur Eignung fallengelassen werden.

2.4 Offene Fragen

Viele weitere Datenschutzfragen bleiben offen, die in einer DSFA angesprochen und

analysiert werden müssten. Wie funktioniert die Generierung der TeleTANs für Gesundheitsämter und Hotline? Was passiert auf dem PortalServer? Wie verhält sich der Registration Token, schließt er eine Rückverfolgbarkeit via QR-Code aus? Welche Einstellungen kann der CWA Nutzende vornehmen? Wer ist der tatsächliche Verantwortliche, wer die Auftraggebende, wer hat welche Zuständigkeiten aufgrund von Weisungen? Kann das RKI einfach ohne gesetzliche Zuweisung zum Verantwortlichen werden? Wieso wird die personenbezogene Verarbeitung auf die „Auswertung personenbezogener Daten“ reduziert, wenn beide eine eigene (rechtliche und technische) Bedeutung haben?

3. Fazit

Datenschutz kann nicht ausschließlich durch Technik umgesetzt werden und daher auch nicht durch reine Technikanalyse der in diesem Falle hervorragenden IT-Komponente evaluiert werden. Die bestehenden Risiken, die durch die Aktivitäten der Verantwortlichen und der von ihr beauftragten Dienstleisterïnnen entstehen, müssen entlang der gesamten Kette der Verarbeitungsschritte ausgewiesen und Schutzmaßnahmen zu deren Verringerung vorgeschlagen, diskutiert und beurteilt werden. Um einen Maßstab für die Qualität – man kann auch sagen: für deren Integrität – der Erarbeitung einer DSFA auszuweisen: Eine DSFA und ein daraus erstellter DSFA-Bericht sollte selber den Grundsätzen aus Art. 5 DSGVO bzw. den Gewährleistungszielen genügen.

Die rechtliche Auseinandersetzung hat die Anforderungen vorzugeben, an der sich die rechtlichen, technischen und organisatorischen Maßnahmen zur Risikominimierung anschließend ausrichten. Eine solche Auseinandersetzung fehlt gerade für die kritischen Punkte der Verantwortlichkeit, Zweckbindung der Verarbeitung, dem Vorliegen der Nutzung einer Einwilligung sowie der Freiwilligkeit bei der Nutzung und dem Nachweis der Freiwilligkeit. Die umgangene Risikodiskussion führt dazu, das eine wesentliche Maßnahme zur Risikoreduzierung für die Betroffenen, nämlich das Erlassen eines Gesetzes, das den Verantwortlichen und andere Interessenten an der App bindet, nicht einmal auch nur diskutiert wird.

Es ist nicht Sinn und Zweck einer DSFA, die Verarbeitung personenenbezogener Daten im Rahmen einer technischen Lösung zu rechtfertigen, wie dies insbesondere in der Bewertung der Verhältnismäßigkeit der Verarbeitung in der vorgelegten DSFA erfolgt. Es ist vielmehr Aufgabe der DSFA, die Risiken, die sich aus der Verarbeitung ergeben, dazu getroffene Schutzmaßnahmen auszuweisen und insbesondere unbehandelte Risiken in den Vordergrund zu stellen. Letztlich wäre zu wünschen, dass die vorhandenen zarten Ansätze einer ernsthaften datenschutzrechtlichen Befassung ausgebaut werden, um dann in einem reifen Datenschutzmanagement aufzugehen.