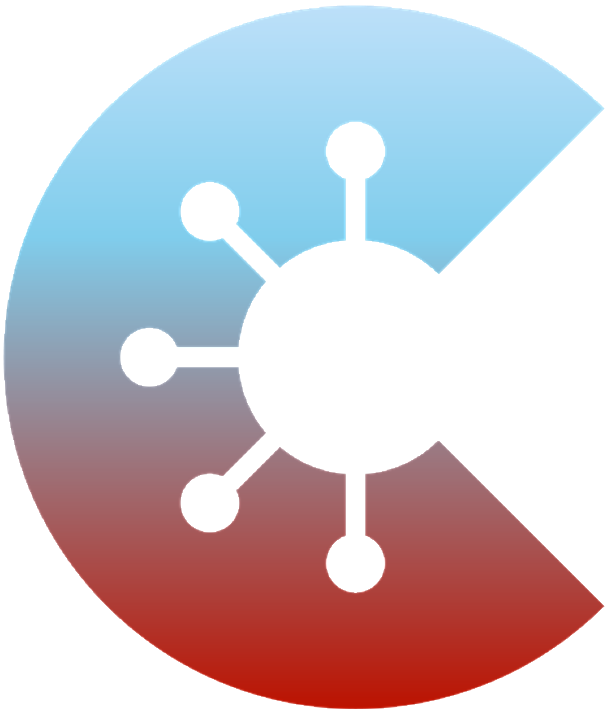


CORONA

WARN-APP

Bericht zur Datenschutz-Folgenabschätzung für die

Corona-Warn-App

der Bundesrepublik Deutschland

Version 1.0, 14.06.2020

1 Vorausgehende Hinweise

Dieses Dokument enthält die Version 1.0 des Berichts zur Datenschutz-Folgenabschätzung (DSFA)[1] für die CWA der Bundesrepublik Deutschland, die nach Fertigstellung durch das Robert Koch-Institut herausgegeben und betrieben werden soll.

Infolge der zu erwartenden zügigen technischen Weiterentwicklung der CWA wird auch die DSFA einer regelmäßigen Aktualisierung unterliegen. Dementsprechend handelt es sich bei dem vorliegenden DSFA-Bericht um ein „lebendiges Dokument“, welches zu gegebenem Zeitpunkt aktualisiert und in Form einer neuen Version zur Verfügung gestellt werden wird. Abweichungen des Prüfgegenstands von der tatsächlichen Umsetzung der CWA sind daher möglich und werden gegebenenfalls bei der Wiederholung der DSFA berücksichtigt.

Dem vorliegenden DSFA-Bericht liegt der Stand der Architektur vom 12.06.2020 zugrunde. Die Änderungshistorie ist unter Ziffer 2 in Tabellenform abgebildet.

Dieses Dokument basiert – soweit die Funktionalität, die Datenverarbeitung und der Umfang der Datenverarbeitung in dem Expositionsbenachrichtigungswerkzeug (Exposure Notification Framework (ENF)) der Unternehmen Apple Inc. und Google Inc. beschrieben wird – auf den verfügbaren Beschreibungen zu diesem Framework. Eigene Erkenntnisse über die innere Funktionsweise können nicht gewonnen werden, da dieses Framework aus Sicherheitsgründen in einer Art und Weise implementiert ist, die eine Untersuchung ausschließen. Insoweit wurde bei der Erstellung dieses Dokuments auf die Richtigkeit der Verarbeitung in den Frameworks und der Beschreibungen vertraut, wie auch beim Betrieb der Frameworks auf die Richtigkeit der Datenverarbeitung und deren Beschreibung vertraut wird. Die Behauptung einer eigenen Prüfung, eigenen Wissens oder Gewähr soll mit den in diesem Dokument vorgenommenen Beschreibungen nicht verbunden sein.

In diesem DSFA-Bericht wird – ausschließlich zum Zweck der besseren Lesbarkeit – auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen in diesem Dokument sind somit geschlechtsneutral zu verstehen.

[1] Aus Gründen der besseren Lesbarkeit werden die Begriffe „DSFA“ und „DSFA-Bericht“ nachfolgend teilweise synonym bzw. in Abhängigkeit des jeweiligen Kontexts verwendet.

2 Änderungshistorie

Änderung			Beschreibung der Änderung	Freigabe des Berichts	Stadium
Nr.	Datum	Version			
1	12.06.2020	0.9	Finalisierung des vorläufigen DSFA-Berichts	-	-
2	14.06.2020	1.0	Erstellung DSFA Bericht 1.0	15.04.2020	final

3 Inhalt

4 Abkürzungsverzeichnis / Glossar

Das nachfolgende Glossar enthält wesentliche Begriffe und wurde aus dem Rahmendokument des Datenschutzkonzeptes übernommen. In aller Regel wurde einer deutschen Schreibweise der Vorrang gegeben, englische Bezeichnungen und Abkürzungen referenzieren auf die deutschen Begriffe / Definitionen.

Verwendete Rechtsbegriffe werden möglichst im Originalwortlaut der DSGVO unter Wahrung wissenschaftlicher Zitierweise wiedergegeben.

4.1 Glossar

Die Art des Begriffes wird wie folgt definiert:

§ Begriff mit einer rechtlichen Bedeutung oder einem rechtlichen Bezug

O Begriff, der organisatorische Aspekte beschreibt.

T Begriff, der technische Aspekte beschreibt.

→ Referenz im Glossar

Anmerkung:

Zur besseren Lesbarkeit des Dokumentes wurde auf die Kenntlichmachung der Referenzen im Glossar verzichtet.

Begriff	Art	Beschreibung	Verweise
Android	T	Android ist sowohl ein Betriebssystem als auch eine Software-Plattform, die von der von Google gegründeten Open Handset Alliance entwickelt werden.	→ Betriebssystem
Anonyme Daten	§	Die nachfolgende Definition ist wörtlich aus den Erwägungsgründen der DSGVO übernommen: Anonyme Daten sind solche, „die sich nicht auf eine identifizierte oder identifizierbare natürliche Person	

		beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.“ (ErwG 26 DSGVO).	
Ansteckend	O	Die (vorübergehende) Eigenschaft einer Person, das Cornavirus auf eine andere Person übertragen zu können.	→ Coronavirus
Ansteckung	O	Übertragung des Coronavirus von einer Person auf eine andere.	
Ansteckungsrisiko	O	Das Risiko, dass es zu einer Ansteckung kommt.	→ Risiko → Ansteckung
Anwendungslog	T	Das Anwendungslog ist ein Werkzeug zum Sammeln von technischen Meldungen wie z.B. Ausnahmen und Fehlern. Diese Informationen werden in ein Protokoll zusammengefasst und dargestellt.	
Applikation Versionsnummer	T	Die „Application Version“ erlaubt es dem mobilen Endgerät festzustellen, ob eine neue Version der CWA App verfügbar ist. Dies ist notwendig, um den Nutzer auf ein Update hinzuweisen (Da die CWA APP auf iOS und Android verfügbar ist, werden auch Versionen für beide Plattformen vorgehalten). „Latest“: Die aktuelle Version der CWA App, wie sie derzeit beim Download angeboten wird. „Min“: Die minimal benötigte Version der CWA App, damit sie benutzbar bleibt. Die Versionen folgen dem Prinzip der semantischen Versionierung, welches aus drei Teilen besteht:	→ mobiles Endgerät → CWA → iOS → Android

		„Major“, „Minor“ und „Patch“ je durch einen Punkt getrennt.	
Attenuation Duration Thresholds	T	Es gibt zwei sogenannte „Attenuation Duration Thresholds“, mit denen die Dauer einer Begegnung in Abhängigkeit von der Signaldämpfung gewichtet werden kann. Bei geringer Signaldämpfung (= großer Nähe des Kontakts) geht die Begegnung mit ihrer vollen Dauer in die Risikoberechnung ein, bei mittlerer Signaldämpfung nur hälftig, bei hoher Signaldämpfung gar nicht. Die Gewichtung (voll, hälftig, gar nicht) ist durch das RKI konfigurierbar. Diese Konfiguration kann sich durch Erkenntnisse verändern.	
Auftragsverarbeiter (Processor)	§	Die nachfolgende Definition ist wörtlich aus der DSGVO übernommen: „Auftragsverarbeiter (ist) eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;“ (Art 4 Nr. 8 DSGVO).	
Backend	→	Als Backend wird der Teil eines IT-Systems bezeichnet, der sich mit der Datenverarbeitung im Hintergrund beschäftig.	→ CWA Server
Begegnung	O	Jedes Zusammentreffen, das zum Austausch und zur Speicherung von kurzlebigen zufälligen Bluetooth-IDs (Zufallscodes) führt. NB: Über Begegnungen per se werden CWA-Nutzer nicht informiert.	→ Bluetooth-IDs → Zufallscodes → Begegnungen → CWA-Nutzer
Begegnungs-Aufzeichnung	O	Liste der empfangenen und vorübergehend im Betriebssystemspeicher abgelegten	→ Betriebssystemspeiche → Bluetooth-IDs → Zufallskennungen

		kurzlebigen zufälligen Bluetooth-IDs (Zufallskennungen). Die Begegnungs-Aufzeichnung wird bei der Risiko-Überprüfung gelesen. Alle Zufallscodes werden automatisch gelöscht, wenn sie 14 Tage alt sind. Die Begegnungs-Aufzeichnung kann vom CWA-Nutzer jederzeit auch als Ganzes aktiv gelöscht werden. Die Daten im Betriebssystem (gesammelte und eigene Tagesschlüssel) werden nicht gelöscht, sondern verbleiben für 2 Wochen gespeichert im geschützten Betriebssystemspeicher.	→ Begegnungs-Aufzeichnung → Risiko-Überprüfung → Zufallscodes → CWA-Nutzer → CWA
Behandelnder Arzt / Testeinrichtung	O	Der behandelnde Arzt / die Testeinrichtung ist die medizinische Stelle, welche die Corona-Probe der Testperson abnimmt. Die Stelle unterliegt der Schweigepflicht.	
Benutzer	T, O	Nutzer synonym für Nutzer.	→ Nutzer
Besondere Kategorien personenbezogener Daten	§	Die nachfolgende Definition ist wörtlich (gekürzt) aus der DSGVO übernommen: “Personenbezogene(r) Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie … genetische … Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person” Art. 9 Abs. 1 DSGVO.	→ personenbezogene Daten
Betriebssystem	T	Das die Basisfunktionen eines mobilen Endgerätes steuernde Programm, in das Apple (iOS) und Google (Android) zusätzliche	→ mobiles Endgerät → iOS → Android → Risiko-Ermittlung

		Funktionen für eine Risiko-Ermittlung eingebaut haben, die von der CWA App genutzt werden, um den Nutzer über sein Coronavirus-Infektionsrisiko zu informieren und um ihm zu ermöglichen, andere Nutzer über deren Risiko zu informieren, falls er positiv getestet werden.	→ CWA → Nutzer → Coronavirus → CWA-Nutzer → Risiko
Betriebssystem-speicher	T	Ein besonders geschützter Datenspeicher im Betriebssystem, in dem die Begegnungs-Aufzeichnung gespeichert wird.	→ Betriebssystem → Begegnungs-Aufzeichnung
Bewertungseinstell-ungen	T	Die Bewertungseinstellungen bestehen aus einer Reihe von Werten, die zur Ermittlung möglicher Kontakte mit Erkrankten hinzugenommen werden. Die BWE werden vom „RKI“ festgelegt und werden vom mobilen Endgerät aus dem CDN zusammen mit den Positivschlüsseln geladen.	→ mobiles Endgerät → CDN → Positivschlüsseln
Bluetooth	T	Ein Funkstandard, mit dem mobile Endgeräte über kurze Entfernungen Daten austauschen können. Für die Risiko-Ermittlung der CWA App wird der fortgeschrittene Standard Bluetooth Low Energy genutzt, der besonders geringen Einfluss auf die Akkuleistung hat.	→ mobiles Endgerät → Risiko-Ermittlung → CWA → Bluetooth Low Energy
Bluetooth Low Energy	T	Die Bluetooth Low Energy ist eine Funktechnik, mit der mobile Endgeräte in einem Abstand von etwa 10 Metern Daten via Bluetooth austauschen können. Die BLE dient im weiteren Verfahren zum Austausch von wechselnden Entfernungsschlüssel.	→ mobiles Endgerät → Bluetooth → wechselnden Entfernungsschlüssel → BLE
Call Center	O	Hotline, Call-Center u.ä. Synnonyme.	

Certification Chain	→	Verbund von zusammengehörigen Zertifikaten.	→ Zertifikat
Consent	→	Engl. Synonym für Einwilligung.	→ Einwilligung
Container	T	Eine technisch abgeschlossene Umgebung in der ein Programm läuft.	
Content Delivery Network, CDN-Magenta	T	Das CDN-Magenta stellt die Positivschlüssel zur Verfügung. Die mobilen Endgeräte könne die Fallschüssel jederzeit vom CDN laden und damit eine erneute Ermittlung möglicher Kontakte mit Erkrankten anstoßen. Des Weiteren stellt es gemeinsam mit den FAS die Bewertungseinstellungen (BWE) zur Verfügung.	→ Positivschlüssel → mobiles Endgerät → Bewertungseinstellung-en
Corona	O	Bezeichnung für verschiedene Begriffe, die mit dem Coronavirus oder der von ihm verursachten Krankheit COVID-19 in Verbindung stehen, z.B. Corona-Pandemie Corona-Test, Corona-Warn-App. In den Dokumenten wird der Begriff Corona benutzt werden.	→ Coronavirus → COVID-19 → Corona-Warn-App
Corona-positiv getestete Person	O	Eine Person, bei der mittels eines anerkannten Labortests das Coronavirus direkt (z.B. per PCR) nachgewiesen wurde. Serologische Nachweise zählen nicht als direkte Nachweise. Im Datenschutzkonzept wird aus Gründen der Lesbarkeit der verkürzende Begriff “infizierter Nutzer” verwendet.	→ Coronavirus → Infizierter Nutzer
Corona-Warn-App	O	Die Bezeichnung Corona-Warn-App umfasst gesamthaft sowohl die CWA App (also die App, die der CWA Nutzer auf seinem mobilen Endgerät nutzt) als auch die zur Verarbeitung notwendigen Lösungsbestandteile des CWA Servers.	→ CWA App → mobiles Endgerät → CWA Server → Kontaktperson

Corona-Warn-System	→	Risiko-Mitteilungssystem.	
Coronavirus	O	Ein Krankheitserreger aus der Familie der Coronaviren; wird in der CWA auch umgangssprachlich für Corona verwendet.	→ CWA → Corona
COVID-19	O	Die durch das Coronavirus verursachte Krankheit.	→ Coronavirus
CWA App	T	Anwendung für mobile Endgeräte der Bundesregierung zur Begleitung von Corona-Labortestungen und zur Risiko-Benachrichtigung von Kontaktpersonen, um Infektionsketten frühzeitig zu unterbrechen.	→ mobiles Endgerät → Corona- → Risiko-Benachrichtigung → Kontaktperson
CWA Backend	→	Unerwünschtes Synonym für CWA Server	→ CWA Server
CWA Nutzer	T	Ein Nutzer der Corona-Warn-App.	→ Nutzer → Corona-Warn-App
CWA Server	T	Software Service, der Positivschlüssel von Nutzern sammelt und im Zuge dessen die Korrektheit/Gültigkeit dieser sicherstellt. Das bedeutet, dass überprüft wird ob diese tatsächlich von einer Corona positiv getesteten Person stammen und in den letzten beiden Wochen Kontakt mit dieser Person hatten.	→ Positivschlüssel → Nutzern
Diagnose Schlüssel	→	Synonym für Positivschlüssel.	
Diagnoseunterstützung	→	Unangemessenes Synonym für Testergebnisabruf.	→ Testergebnisabruf
Diagnosis Key	→	Unangemessenes Synonym für Positivschlüssel.	
Distribution Services	T	Komponente des CWA Server. Im gegebenen Verfahren bereitet dieser die Positivschlüssel zur Verteilung	→ CWA Server → Positivschlüssel → CDA-Magenta

		vor, so dass diese aus dem CDA-Magenta Objektstore verteilt werden können.	→ Objektstore
Docker Container	T	Der Docker Container ist ein Container in einem Kubernetes Umfeld.	→ Kubernetes
Dritter	§	Die nachfolgende Definition ist wörtlich aus der DSGVO übernommen: „Dritter (ist) eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;“ (Art 4 Nr. 10 DSGVO).	
Eigenschüssel (EGS)	T	Der EGS ist ein Schlüssel, der durch die am Verfahren teilnehmenden mobilen Endgeräte geräteindividuell erzeugt wird. Der EGS dient im weiteren Verfahren anderen mobilen Endgeräten zur Ermittlung möglicher Kontakte mit Erkrankten. Er besteht aus Tageschlüsseln. Jeden Tag wird ein neuer zufälliger Tagesschlüssel erzeugt und im Expositionsbenachrichtigungswerkzeug (ENF) des mobilen Endgerätes für 14 Tage gespeichert. Die Tagesschlüssel sind die Initialwerte zur Erzeugung der wechselnden Entfernungsschlüssel (RPI), die das mobile Endgerät über die Bluetooth Low Energy (BLE) aussendet.	→ mobiles Endgerät → Tageschlüsseln → Expositionsbenachrichtigungswerkzeug → wechselnden Entfernungsschlüssel → Bluetooth Low Energy

Einwilligung	§	Die nachfolgende Definition ist wörtlich aus der DSGVO übernommen: „Einwilligung der betroffenen Person (ist) jede 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;“ (Art 4 Nr. 11 DSGVO).	
Empfänger	§	Die nachfolgende Definition ist wörtlich aus der DSGVO übernommen: „Empfänger (ist) eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;“ (Art 4 Nr. 9 DSGVO).	
Empfangsschlüssel	T	Die Empfangsschlüssel bestehen aus wechselnden Entfernungsschlüssel und werden von anderen mobilen Endgeräten im Expositionsbenachrichtigungswerkze	→ wechselnde Entfernungsschlüssel → mobiles Endgerät → Expositionsbenachricht -igungswerkzeug

		ug erzeugt und über deren Bluetooth Low Energy ausgesandt. Das eigene mobile Endgeräte kann diese empfangen und als Teil der Kontaktschlüssel speichern. Dies dient der Ermittlung möglicher Kontakte mit Erkrankten.	→ Bluetooth Low Energy → mobile Endgerät → Kontaktschlüssel
Expositions-benachrichtigungs-werkzeug	T	Das Expositionsbenachrichtigungswerkzeug ist ein Bestandteil des Betriebssystems der mobilen Endgeräte von Apple Inc. und Google Inc. Diese Bestandteile sind neu und stehen nur zur Verfügung, wenn das Betriebssystem der mobilen Endgeräte auf einem neueren Stand sind. Das Expositions-benachrichtigungs-werkzeug übernimmt große Teile der Generierung der Schlüssel sowie deren Austausch.	→ Betriebssystem → mobilen Endgeräte → ENF
ExposureNotification framework	→	Englisches Synonym für: Expositionsbenachrichtigungswerkzeug	
Fachseitiger Datenverantwort-licher	O	Der fachseitige Datenverantwortliche verantwortet die Einhaltung der datenschutzrechtlichen Verpflichtungen. Der fachseitige Datenverantwortliche verpflichtet einen fachseitigen Systemverantwortlichen. Der fachseitige Systemverantwortliche ist auf operativer Ebene für die Datenschutzkonformität des jeweiligen Systems verantwortlich. Diese Verpflichtung ist bei personellen oder organisatorischen Änderungen oder, sofern erforderlich, bei technischen Änderungen zu aktualisieren. Alle Änderungen der fachseitigen	

		Systemverantwortung sind für jedes IT-/NT-System des Verantwortungsbereichs des fachseitigen Datenverantwortlichen chronologisch zu dokumentieren. Der fachseitige Datenverantwortliche gewährleistet die ordnungsgemäße Aufgabenwahrnehmung der fachseitigen Systemverantwortlichen.	
Fachseitiger Systemverantwort-licher	O	Der fachseitige Systemverantwortliche unterstützt den fachseitigen Datenverantwortlichen bei der Wahrnehmung der Verantwortung für die Datenverarbeitung für das System, für dessen operative Betreuung er vom fachseitigen Datenverantwortlichen verpflichtet wurde. Im Rahmen dieser Aufgabe folgt er den Weisungen des fachseitigen Datenverantwortlichen. Der fachseitige Systemverantwortliche ist operativ verantwortlich für die Datenschutzkonformität des von ihm betreuten Systems. Dies gilt für jede Änderung oder Neueinführung des von ihm betreuten IT-/NT-Systems. Der fachseitige Systemverantwortliche stellt sicher, dass ein technischer Systemverantwortlicher für das System benannt ist. Der fachseitige Systemverantwortliche prüft im angemessenen Umfang die ordnungsgemäße Aufgabenwahrnehmung des technischen Systemverantwortlichen.	

Factory Reset	→	Englisches Synonym für Rücksetzen auf Auslieferungszustand.	
Fake Delay Function	→	Englisches Synonym für Täuschanfrageninterpretation.	
Fake Request	→	Englisches Synonym für Täuschanfrage.	
Fehlender Verdachtsfall (FVF)	O	Endanwender, die sich bei einer infizierten Persona mit COVID-19 angesteckt haben, deren Kontakt mit der betreffenden Person von unserer App aber nicht bemerkt oder nicht als riskant angesehen wurden.	
Gesundheitsamt	O	Das Gesundheitsamt / die Gesundheitsbehörde ist eine staatliche oder kommunale Behörde nach Landesrecht und Teil des öffentlichen Gesundheitsdienstes. Das Gesundheitsamt empfängt im Rahmen der Meldepflicht (§4 IfSG) einer Corona-Infektion in der Regel durch die Leitung des Labors die personenbezogenen Daten der infizierten Person.	→ Corona
GUID	T	Globally Unique Identifier. In diesem Verfahren eine Kennung für einen Corona Test. Diese Komponente behandelt nur gehashte Instanzen der GUID. Einzelheiten zum Hashing finden Sie unter Verwendete kryptografische Algorithmen. Die GUID hat eine Länge von 152 Bit, besteht aus einem Präfix von 24 Bit und einem Hauptteil von 128 Bit. Nur der Hauptteil wird durch einen kryptografisch zuverlässigen Prozess erzeugt.	
Health Authority	→	Englisches Synonym für Gesundheitsbehörde, im Deutschen	

		genauer: die Menge der Gesundheitsbehörden	
Hotline	O	Call-Center u.ä. Synonyme.	
Infektionskette	O	Eine Reihe von Ansteckungen, bei der eine Person eine andere ansteckt und diese wiederum eine Dritte.	→ Ansteckungen
Infektionsrisiko	O	Das von der CWA App ermittelte Risiko, sich mit dem Coronavirus angesteckt bzw. infiziert zu haben.	→ CWA → Risiko → Coronavirus
Infizierte Person	→	Relevant für die Lösung als potentiell Infizierter Nutzer.	→ Infizierter Nutzer
Infizierter	→	Relevant für die Lösung als potentiell Infizierter Nutzer.	
Infizierter Nutzer	O	Ein Infizierter Nutzer ist ein Nutzer, bei dem eine Ansteckung mit Corona nachgewiesen wurde. Synonym für Corona-positiv getestete Person.	→ Nutzer → Corona
iOS	T	iOS ist sowohl ein Betriebssystem als auch eine Software-Plattform die von Apple entwickelt wurde und nur auf Geräten der Firma Apple läuft.	→ Betriebssystem
Irrtümlicher Verdachtsfall (IVF)	O	Nutzer, die von der CWA App über einen riskanten Kontakt mit einer infizierten Person informiert worden sind, aber anschließend negativ auf COVID-19 getestet werden:	→ Nutzer
Isolation	O	Vermeidung von Begegnungen. Bei einer nicht Corona-positiv getesteten Person, bei der der Verdacht auf eine Infektion besteht, auch als Quarantäne bezeichnet.	→ Corona-positiv getesteten Person
Kontaktperson	O	Kontakte oder Kontaktpersonen sind Personen, in deren Nähe der Nutzer sich aufgehalten hat und daher potentiell eine Corona Übertragung stattgefunden haben kann. Kurz:	→ Nutzer → Corona → Risiko-Begegnungen

		Jede Person, die Risiko-Begegnungen hatte.	
Kontaktschlüssel	T	Der Kontaktschlüssel besteht aus wechselnden Entfernungsschlüsseln anderer mobiler Endgeräte die über Bluetooth Low Energy von diesen anderen mobilen Geräten empfangen werden und im Expositionsbenachrichtigungswerkzeug des eigenen mobilen Endgerätes für 14 Tage gespeichert werden. Der Kontaktschlüssel dient im weiteren Verfahren dem eigenen mobilen Endgerät zur Ermittlung möglicher Kontakte mit Erkrankten.	→ wechselnde Entfernungsschlüsseln → Bluetooth Low Energy → Expositionsbenachricht-igungswerkzeug
Kontaktverfolgung	→	Synonym für Risiko-Ermittlung, um dem Sachverhalt Ausdruck zu verleihen, dass zur Ermittlung eines Risikos sachverhaltlich neben dem fortlaufenden Senden und Empfangen auch noch die Berechnung durch das Expositions-Benachrichtigungswerkzeug gehört.	→ Risiko-Ermittlung → Expositionsbenachricht-igungswerkzeug
Kryptographischer Schlüssel	T	Ein mit kryptographischen Verfahren erzeugter Schlüssel. „Der Schlüssel beinhaltet bei einem symmetrischen Verfahren … die Information, die geheim bleiben muss, während der Algorithmus, also das Verschlüsselungsverfahren selbst, öffentlich bekannt sein darf. Bei asymmetrischen Verschlüsselungsverfahren, auch als „Public-Key-Kryptographie“ bezeichnet, übernimmt die Rolle des Geheimnisses der private Schlüssel, während der dazugehörige öffentliche Schlüssel allgemein bekannt ist.“ Nachweis: https://de.wikipedia.org/wiki/Schlüssel_(Kryptologie).	
Kubernetes	T	Eine von Google bereit gestellte Software, in der Prozesse technisch	

		zusammengebracht werden können. Siehe auch https://de.wikipedia.org/wiki/Kubernetes.	
Lab Client	T	Teil des LIS welches im Labor verwendet wird.	→ Test Result Server
Labor	O	Das Labor ist die Stelle, welche die Corona Proben testen und ein vertrauenswürdiges Testergebnis erstellen. Die Stelle unterliegt der ärztlichen Schweigepflicht.	
Laborgateway	T	Schnittstelle zwischen Labor Clients und dem Test Result Server.	
Laboratory Information System (LIS)	O	Laborsoftware die zur Abwicklung des Tagesgeschäft im Labor genutzt wird. Sendet die Daten über das Laborgateway an den Test Result Server.	→ Test Result Server → Laborgateway
Local Health Authority	→	Englisches Synonym für Gesundheitsamt.	
Medizinische Fachkraft / Testeinrichtung	O	Die medizinische Fachkraft / Testeinrichtung erhält Informationen über infizierte Personen als Teil ihrer normalen Tätigkeiten zur Diagnose von Patienten, entweder im Rahmen der Probenerstellung oder Probentestung. Auch sie unterliegen der Schweigepflicht.	
Mobiles Endgerät	T	Mobile Endgeräte sind mobilfunkfähige Geräte, die entweder mit dem Betriebssystem Android ausgestattet sind, oder solche des Herstellers Apple, die mit dem Betriebssystem iOS ausgestattet sind.	→ Betriebssystem → Android → iOS
Nutzer	T	Eine Person (Nutzer oder Nutzerin), die die CWA auf ihrem mobilen	→ CWA → mobiles Endgerät

		Endgerät installiert hat und ihre Funktionen aktiviert hat. Steht auch synonym für Nutzer, User.	
Objektstore	T	Der Objektsore dient im Verfahren als Ablageort für den Abruf vorbereiteter Dateien Schlüssel und Konfigurationsdateien. Für eine technisch genauere Beschreibung siehe auch: https://en.wikipedia.org/wiki/ObjectStore.	
Open Telekom Cloud	T, O	Eine von der Telekom in Deutschland bereitgestellte Cloud-Lösung, im Rahmen der Auftragsverarbeitung.	→ Auftragsverarbeitung
Pairing	T	Die technische Koppelung zweier technischer Geräte.	
Personenbezogene Daten	§	Die nachfolgende Definition ist wörtlich aus der DSGVO übernommen: „Personenbezogene Daten (sind) 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;" (Art. 4 Nr. 1 DSGVO).	

Personenbezogene Verarbeitungen	→	Auswertung personenbezogener Daten.	
Portal Server	T	Der Portal Server dient als zentrale Generierungsmöglichkeit für teleTANs. Dieser wird sowohl vom Gesundheitsamt als auch von der Hotline genutzt.	→ teleTAN
Positivschlüssel	T	Der zufällige Geräteschlüssel (Zufallscode) eines infizierten Nutzers nach Verifikation ihres Testergebnisses [engl. *Diagnosis Key*].	→ Zufallscode → infizierter Nutzer → Verifikation
Positivschlüssel Paket	T	Ein Positivschlüssel Paket ist eine Sammlung von Positivschlüsseln unterschiedlicher Betroffener, die vom CDN-Magenta an die mobilen Endgeräte verschickt werden.	
Processor	→	→ Auftragsverarbeiter.	
Pseudonyme Auswertungen	T	In Abgrenzung zu Auswertung personenbezogener Daten hebt dieser Begriff hervor, dass es sich um pseudonyme Daten handelt.	→ Auswertung personenbezogener → pseudonyme Daten
Pseudonyme Daten	§	Personenbezogene Daten die einem Verfahren der Pseudonymisierung unterworfen wurden.	→ Personenbezogene Daten → Pseudonymisierung
Pseudonymisierung	§	Die nachfolgende Definition ist wörtlich aus der DSGVO übernommen: „Pseudonymisierung (beschreibt) die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen	

		Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“ (Art 4 Nr. 5 DSGVO).	
QR-Code	T	Ein auf einen Probenbegleitschein aufgedruckter eindeutiger Code, der Ihnen das Einlesen eines angeforderten Tests in die CWA (Testregistrierung) ermöglicht. Das Ergebnis eines so registrierten Tests wird von der CWA abgerufen und Ihnen als CWA-Nutzer angezeigt. Es ist dann bereits verifiziert, so dass Sie bei einem positiven Ergebnis Ihre zufälligen Geräteschlüssel (Zufallscodes) der letzten bis zu 14 Tage als Positivkennungen ohne Eingabe einer teleTAN freigeben und auf den CWA Server hochladen können.	→ CWA → Testregistrierung → Positivkennungen → teleTAN → CWA Server
Registration Token	T	Vom Verification Server erzeugte Kennung, die den QR-Code oder eine TAN oder eine teleTAN ersetzt, um eine Identifizierung des Nutzers durch natürliche Personen zu erschweren und gleichzeitig die technische Zuordnenbarkeit ermöglicht. zur Kommunikation mit dem Verification Server.	→ Verification Server → QR-Code → TAN → teleTAN
Response	T	Antwort.	
Risiko	O	Als Risiko wird in der CWA je nach Kontext entweder das von der CWA App ermittelte Risiko, sich mit dem Coronavirus angesteckt bzw. infiziert zu haben (Ansteckungsrisiko, Infektionsrisiko), oder das Risiko, das eine infizierter Nutzer insbesondere aufgrund ihrer Infektiosität (Ansteckungsfähigkeit) für ihre Kontaktpersonen darstellt	→ Risiko → CWA → Coronavirus → Ansteckungsrisiko, → Infektionsrisiko → infizierter Nutzer → Kontaktpersonen → Übertragungsrisiko

		(Übertragungsrisiko), bezeichnet. NB: Risiko wird hier nicht von Wahrscheinlichkeit unterschieden, d.h. die mehr oder weniger schweren Folgen einer Ansteckung fließen nicht in die Bewertung des Risikos ein.	
Risiko-Begegnungen	O	Jede Serie von Begegnungen (dies beinhaltet ggf. auch einzelne Begegnungen) mit einem infizierten Nutzer, deren über einen Kalendertag aggregierter Risikowert einen festgelegten Schwellenwert überschreitet. NB: Über Risiko-Begegnungen werden Sie als CWA-Nutzer pro Person und Tag informiert.	→ Begegnungen → infizierter Nutzer → Risikowert → CWA-Nutzer
Risiko-Benachrichtigng	T	Die Anzeige von Risiko-Begegnungen in der CWA App [engl. *Exposure Notification*]. NB: Informationen, die das Betriebssystem dem Nutzer sendet, werden von Google (Android) als Benachrichtigungen, von Apple (iOS) hingegen als Mitteilungen bezeichnet. Dementsprechend werden im iOS (z.B. bei Einstellungen, die solche Benachrichtigungen erlauben) Risiko-Benachrichtigungen durch die CWA App als Mitteilungen referenziert.	→ Risiko-Begegnungen → CWA App → Betriebssystem → Nutzer → Android → iOS
Risiko-Ermittlung	T	Fortlaufendes Senden und Empfangen von kurzlebigen zufälligen Bluetooth-IDs (Zufallscodes), die in der Begegnungs-Aufzeichnung gespeichert werden.	→ Bluetooth-IDs → Zufallscodes → Begegnungs-Aufzeichnung
Risiko-Mitteilung	T	Die Freigabe und das Hochladen der zufälligen Geräteschlüssel (Zufallscodes) der letzten bis zu 14	→ Zufallscodes → infizierter Nutzer) auf → CWA Server

		Tage einer infizierter Nutzer auf den CWA Server, wo sie als Positivschlüssel von anderen CWA-Nutzern abgefragt und mit ihren in der Begegnungs-Aufzeichnung gespeicherten kurzlebigen zufälligen Bluetooth-IDs verglichen werden können.	→ Positivschlüssel → CWA-Nutzer → Begegnungs-Aufzeichnung → Bluetooth-IDs
Risiko-Mitteilungssystem	T	Das gesamte Corona-Warn-System, bestehend aus der CWA App, dem Betriebssystem des mobilen Endgerätes und dem CWA Server. In technisch detaillierteren Beschreibungen abzugrenzen von Expositionsbenachrichtigungswerkzeug	→ Corona-Warn-System → CWA → Betriebssystem → mobiles Endgerät → Expositionsbenachricht-igungswerkzeug
Risiko-Überprüfung	O	Abfrage der Begegnungs-Aufzeichnung und Abgleich mit den Risiko-Mitteilungen anderer Nutzer. Die Risiko-Überprüfung erfolgt mittels dieser Daten mittels eines Algorithmus.	→ Begegnungs-Aufzeichnung → Risiko-Mitteilungen → Nutzer → Risiko-Überprüfung
Risikostatus	O	Unbekanntes Risiko. Niedriges Risiko. Erhöhtes Risiko.	→ Risiko
Risikowert	O	Der über einen Kalendertag aggregierte Risikowert [engl. Total Risk Score] der Begegnungen mit einem infizierten Nutzer.	→ Begegnungen → infizierter Nutzer
Risikowerte	O	Werte, die das individuelle Risiko beschreiben und vom mobilen Endgerät errechnet werden.	→ mobiles Endgerät
Rolling-Proximity-Identifier	→	Begriff von Apple für wechselnde Entfernungsschlüssel	→ Wechselnde Entfernungsschlüssel
Rotating Proximity Identifier	T	Begriff von Google für Wechselnde Entfernungsschlüssel	→ Wechselnde Entfernungsschlüssel

Rücksetzen auf Auslieferungs-zustand	T	Das Rücksetzen auf den Auslieferungszustand bedeutet, dass die App wieder so konfiguriert ist, wie sie zum Auslieferungszeitpunkt auf das mobile Endgerät geladen wurde. Damit sind alle Einstellungen des Users und alle erzeugten Daten entfernt.	→ mobiles Endgerät
Sendeschlüssel	T	Die Sendeschlüssel bestehen aus wechselnden Entfernungsschlüssel und werden vom eigenen mobilen Endgerät im Expositionsbenachrichtigungswerkzeug erzeugt und über die Bluetooth Low Energy ausgesandt werden. Andere mobile Endgeräte können den RPI empfangen und als Teil ihrer Kontaktschlüssel speichern. Im weiteren Verfahren dient sie der Ermittlung möglicher Kontakte mit Erkrankten.	→ wechselnde Entfernungsschlüssel → mobiles Endgerät → Expositionsbenachricht-igungswerkzeug → Bluetooth Low Energy Kontaktschlüssel
Smartphone	T	Ein Mobiltelefon oder anderes mobiles Endgerät, auf dem die CWA installiert werden kann. Im Datenschutzkonzept wird der Begriff mobiles Endgerät benutzt.	→ mobiles Endgerät → CWA
Submission Services	T	Komponente des CWA Servers Im gegebenen Verfahren nimmt dieser die Positivschlüssel entgegen	→ CWA Servers → Positivschlüssel
Tagesschlüssel	T	Die Tagesschlüssel werden jeden Tag im Expositionsbenachrichtigungs-werkzeug des mobilen Endgerätes erzeugt. Die Tagesschlüssel sind die Initialwerte zur Erzeugung der wechselnden Entfernungsschlüssel. Sie dienen im weiteren Verfahren zu der Berechnung des individuellen Expositionsrisikos, falls sich der Besitzer infiziert und dann beschließt andere mit Hilfe seinen Tagesschlüssel zu warnen. Dadurch	→ Expositionsbenachricht-igungswerkzeug → mobiles Endgerät → wechselnde Entfernungsschlüssel

		werden die Tagesschlüssel zu Positivschlüsseln.	
Täuschanfrage	T	Mobile Endgeräte von Nutzern, die keine Positivschlüssel senden, senden diese Täuschanfragen, so dass das Sende- und Empfangsverhalten der mobilen Endgeräte keinen Rückschluss auf den Gesundheitszustand zulässt. Gesendet werden „Dummydatenpakete“ (also Datenpakete ohne Inhalte) aus der Täuschanfrage wird dann serverseitig durch die Fake Delay Function eine Antwort oder Response mit gleich langer Response Zeit	→ mobiles Endgerät → Nutzer → Positivschlüssel
Täuschanfragen-interpretation	T	Die Täuschanfrageninterpretation des CWA Servers sogt für die zeitliche Gleichbehandlung der Response auf eine Täuschanfrage	→ CWA Server → Response → Täuschanfrage
Technischer Systemverantwort-licher	O	Der technische Systemverantwortliche klärt jeweils systembezogene Rollen- und Aufgabenverteilung mit dem fachseitigen Systemverantwortlichen. Der technische Systemverantwortliche und der fachseitige Systemverantwortliche tauschen sich regelmäßig über aktuelle Entwicklungen in ihrem Bereich aus und stimmen weitere Maßnahmen ab.	
teleTAN	T	Einmalgültiger Schlüssel für die Echtheitsprüfung eines positiven Testergebnisses. Menschenlesbare Transaktionsnummer, die einem infiziertem Nutzer über die Verifikations-Hotline ausgegeben wird, so dass diese ihr positives Testergebnis verifizieren und ihre	→ infizierter Nutzer → CWA Server → CWA-Nutzer → Risiko-Überprüfung

		zufälligen Geräteschlüssel der letzten bis zu 14 Tage auf den CWA Server hochladen und dadurch anderen CWA-Nutzern eine Risiko-Überprüfung ermöglichen kann.	
Temporary-Exposure-Key	→	→ Tagesschlüssel.	
Test lab processing samples (Lab Client)	→	Lab Client.	
Test Result Server	T	Software Service, das die Ergebnisse der Labors zur weiteren Verwendung bereitstellt.	
Testergebnis	T	Das Ergebnis eines Labortests zum Nachweis des Coronavirus, das nach ärztlicher Bewertung als Befund mitgeteilt wird.	→ Coronavirus
Testergebnisabruf	T	Der Abruf des Testergebnisses durch den Nutzer mittels der CWA.	→ Testergebnis → Nutzer → CWA
Testperson	O	Person, die sich auf Corona testen lässt.	
Testregistrierung	T	Das Einlesen eines angeforderten Tests in die CWA mittels eines QR-Codes.	→ CWA → QR-Codes
Übertragungsrisiko	T	Das tagesspezifische Risiko [engl. *Transmission Risk*], dass ein infizierter Nutzer mit seiner Positivschlüssel an andere CWA-Nutzer mitteilt und das in die Berechnung des Risikowerts eingeht.	→ Risiko → infizierter Nutzer → Positivschlüssel → CWA-Nutzer → Risikowerts
User	T	Teilweise technisch verwendetes Synonym für einen Nutzer.	→ Nutzer
Verantwortlicher (Controller)	§	Die nachfolgende Definition ist wörtlich aus der DSGVO übernommen:	

		„Verantwortlicher (ist) 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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;“ (Art 4 Nr. 7 DSGVO). Hinweis: Die Verantwortliche Stelle der Corona Warn App wird das Robert Koch Institut sein.	
Verarbeitung	§	Die nachfolgende Definition ist wörtlich aus der DSGVO übernommen: „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. 7 DSGVO).	

Verification Server	→	Englisches Synonym für Verification Server	
Verifikation	T	Bestätigung eines positiven Testergebnisses entweder automatisch durch die CWA (wenn dieses nach Testregistrierung durch Einlesen eines eindeutigen QR-Codes von der CWA abgerufen und Ihnen als CWA-Nutzer angezeigt wird) oder manuell durch Eingabe einer teleTAN, so dass die zufälligen Geräteschlüssel (Zufallscodes) der letzten bis zu 14 Tage als Positivkennungen freigegeben und auf den CWA Server hochgeladen werden können.	→ CWA → QR-Codes → CWA-Nutzer → teleTAN → Zufallscodes → Positivkennungen → CWA Server
Verification Server (Verification Server)	T	Verification Server: Software-Service, der beweist, dass ein Nutzer an der Kontaktverfolgung teilnimmt und bereit ist, seine Positivschlüssel einzureichen, vorausgesetzt er wurde von einer Labor wirklich positiv getestet.	→ Positivschlüssel
Vertrauliche Daten	§	Vertrauliche Daten umfassen Authentifizierungsdaten, sicherheitskritische Daten, persönliche Daten und vertrauliche Geschäftsdaten. • Zu den Authentifizierungsdaten gehören beispielsweise Kennwörter, Passphrasen, Zertifikate, Token und andere Anmeldeinformationen. • Zu den sicherheitskritischen Daten gehören beispielsweise kryptografische Schlüssel (außer öffentlichen Schlüsseln), Sitzungskennungen und	→ personenbezogene Daten

		Sicherheitskonfigurationseinstellungen. • Persönliche Daten oder personenbezogene Daten. • Vertrauliche Geschäftsdaten umfassen alle als vertraulich deklarierten Geschäftsdaten wie Finanzergebnisse, Verkaufszahlen, geistiges Eigentum und andere Informationen, die für Wettbewerber nützlich sind oder bei denen eine unbeabsichtigte Offenlegung einem Unternehmen schaden könnte.	
Warnung	→	Risiko-Benachrichtigung.	→ Risiko-Benachrichtigung
Wechselnde Entfernungs-schlüssel	T	Die Wechselnden Entfernungsschlüssel werden im Expositionsbenachrichtigungswerkzeug auf Basis der Tagesschlüssel berechnet. Sie werden als Sendeschlüssel und Empfangsschlüssel zwischen den mobilen Endgeräten über die Bluetooth Low Energy Schnittstelle ausgetauscht.	→ Expositionsbenachricht-igungswerkzeug → Sendeschlüssel → Empfangsschlüssel → mobilen Endgeräte → Bluetooth Low Energy
Zertifikat	→	Im dargestellten Verfahren geht es um die X509 Zertifikate, die zur Identifikation von Daten auf dem Objektstore verwendet werden.	→ X509 Zertifikate → Objektstore
Zufallscode	T	Die CWA verwendet zwei Arten von Zufallscodes, einen zufälligen Geräteschlüssel oder Tagesschlüssel, der täglich neu erzeugt wird, und eine kurzlebige zufällige Bluetooth-ID oder wechselnden Entfernungsschlüssel, die mehrfach pro Stunde kryptografisch aus dem zufälligen Geräteschlüssel abgeleitet und	→ CWA → Tagesschlüssel → Bluetooth-ID → wechselnden Entfernungsschlüssel → mobiles Endgerät → Zufallscode → infizierter Nutzer → Positivkennung → CWA Server → CWA-Nutzern

		zwischen benachbarten mobilen Endgeräten ausgetauscht wird. Beide Zufallscodes lassen sich ohne Zusatzwissen nicht einer bestimmten Person zuordnen und werden automatisch gelöscht, wenn sie 14 Tage alt sind. Ein infizierter Nutzer kann seine zufälligen Geräteschlüssel der letzten bis zu 14 Tage freiwillig als Positivkennungen auf den CWA Server hochladen und dadurch anderen CWA-Nutzern eine Risiko-Überprüfung ermöglichen.	→ Risiko-Überprüfung
Zweck	§	Als Zweck wird umgangssprachlich der Beweggrund einer zielgerichteten Tätigkeit oder eines Verhaltens verstanden und in diesem Dokument so verwendet. In Art. 5 (1) DSGVO wird die Verarbeitung personenbezogener Daten eng mit dem Zweck der Verarbeitung verknüpft. Sie sind nach den Prinzipien der Zweckbindung und der Speicherbegrenzung (u.w.) zu behandeln. Sie dürfen nur „*in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;*“ (Art 5 (1) e DSGVO) Die einfachste und wirksamste Art, dem nachzukommen ist die Löschung der Daten Art diese Daten.	

4.2 Abkürzungsverzeichnis

Begriff	Art	Beschreibung
AEM	T	Associated Encrypted Metadata
BLE	→	Bluetooth Low Energy
BWE	→	Bewertungseinstellungen
CDN	→	Content Delivery Network, CDN-Magenta
CDN-Magenta	T	Content Delivery Network
CWA	→	CWA
DSGVO	§	Datenschutzgrundverordnung
EGS	→	Eigenschüssel
ENF	→	Expositionsbenachrichtigungswerk
EPS	→	Empfangsschlüssel
FAS	→	Positivschlüssel
FVF	→	Fehlender Verdachtsfall
HKDF	T	Hash Key Derivation Function
IVF	→	Irrtümlicher Verdachtsfall
KOS	→	Kontaktschlüssel
LIS	→	Laboratory Information System
RKI	→	Robert Koch-Institut
RPI	→	Rolling-Proximity-Identifier
SES	→	Sendeschlüssel
TAN	T	Transaktionsnummer

5 Vorbemerkung

Mit diesem DSFA-Bericht werden die Ergebnisse zur Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO (DSFA) für die Verarbeitungsvorgänge im Rahmen des Verfahrens „Corona-Warn-App“ (CWA) in dem unter Ziffer 9 beschriebenen Umfang dokumentiert.

Die besondere Herausforderung der vorliegenden DSFA ergibt sich aus dem engen zeitlichen Rahmen, der dynamischen Architektur und der agilen Entwicklung der CWA, wodurch im Projektverlauf laufend Risikobetrachtungen in Architekturentscheidungen eingeflossen sind, die bis zuletzt zu Änderungen geführt haben, die in die vorliegende DSFA aufgenommen wurden. Die Änderungen wurden von den verschiedenen Workstreams des Projektes, dem behördlichen Datenschutzbeauftragten des Robert Koch-Institut (RKI), den externen juristischen Beratern der Projektbeteiligten und vom BMG diskutiert und Lösungen entwickelt. Das BfDI stand hierbei dem RKI beratend zur Seite. Insgesamt ist damit die Risikobetrachtung im Sinne der DSGVO als laufender Prozess, der auf ständige Verbesserung angelegt ist, bei der Entwicklung der CWA umgesetzt worden.

Geleitet vom Wunsch nach ständiger Verbesserung der Sicherheit der Verarbeitung sind Ergänzungen und auch eine öffentliche Diskussion der DSFA gewünscht. Zielgruppe dieses DSFA-Berichts sind technische und juristische Experten, politische Entscheidungsträger und Datenschutzaufsichtsbehörden des Bundes und der Länder sowie Interessengruppen und sonstige Stakeholder. Es wird der Anspruch höchstmöglicher Transparenz und Nachvollziehbarkeit verfolgt und versucht, dies in dem vorliegenden Bericht umzusetzen, der mögliche datenschutzrelevante Folgen identifiziert und bewertet.

Im vorgeschalteten Dokument zu den Designentscheidungen (Anlage 1) werden verschiedene von fachkundigen Interessensverbänden und Organisationen (u. a. FiFF, CCC, EDSA) veröffentlichte Anforderungskataloge für Tracing-Apps aufgeführt und mit Bezügen zu Fundstellen im DSFA-Bericht versehen, um dem Leser zu ermöglichen, nachzuvollziehen, inwieweit die Anforderungen umgesetzt wurden.

Methodisch gibt es keine Vorgaben zur Durchführung einer DSFA. Für die vorliegend durchzuführende und zu dokumentierende DSFA wird ein hoher Grad an Flexibilität benötigt, um spezielle Risikoszenarien in einer hohen Granularität entwickeln und abbilden zu können. Ebenso muss das Tool für die Risiko-Analyse die verschiedenen Risikoquellen (Angreifer) in Beziehung zu einem Risiko setzen und explizit dafür Eintrittswahrscheinlichkeiten, Schadenshöhen und Maßnahmen abbilden können. Auch die Betrachtung der Auswirkungen für verschiedene Betroffenengruppen muss möglich sein und in Beziehung zu einer konkreten Bedrohung gebracht werden können.

Bei der Durchführung der DSFA wurden die vorhandenen und dem DSFA-Team bekannten Veröffentlichungen zu einer möglichen deutschen Corona-Tracing-App umfassend berücksichtigt, wobei besonders die „Datenschutz-Folgenabschätzung für die Corona-App“

des FifF[2] hervorzuheben ist. Zudem wurden die Stellungnahmen und Forderungen von europäischen Datenschutzaufsichtsbehörden und Datenschutzgremien berücksichtigt[3]. Die durchgeführte Risikoanalyse wurde auf Grundlage einer Risiko-Matrix der Telekom geplant und dokumentiert, die sich ebenfalls an anerkannten Standards orientiert.

Organisatorisch wurde sichergestellt, dass es bei der Durchführung der DSFA zu keinem Interessenkonflikt kommt und die Unabhängigkeit der Kontroll- und Prüfungsaufgabe gewahrt bleibt, indem externe Stellen mit der Durchführung dieses Prozesses beauftragt wurden und der behördliche Datenschutzbeauftragte des RKI nicht unmittelbar in die Durchführung der DSFA eingebunden war.

Seitens des Auftraggebers wurde Wert darauf gelegt, die nachfolgend genannten offiziellen Akteure eng in den Entwicklungsprozess einzubinden, um bei unterschiedlichen Auffassungen über die Anwendung von Datenschutzvorschriften schnell zu konsensfähigen Lösungen zu gelangen und vertrauensschädigende Datenschutzbedenken und Verzögerungen zu vermeiden. Der BfDI als zuständige Aufsichtsbehörde war dabei in beratender Funktion eingebunden.

---

[2] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), Datenschutz-Folgenabschätzung für die Corona App, Version 1.6, abrufbar unter: https://www.fiff.de/dsfa-corona.

[3] *Datenschutzkonferenz*, Kurzpapier Nr. 5 zur Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, Stand: 17.12.2018, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf"h (abgerufen am 11.06.2020) und Kurzpapier Nr. 18 zum Risiko für die Rechte und Freiheiten natürlicher Personen, Stand: 26.04.2018, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (abgerufen am 11.06.2020); *Artikel-29-Datenschutzgruppe*, WP 248 Rev. 01, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, angenommen am 4. April 2017, zuletzt überarbeitet und angenommen am 4. Oktober 2017, abrufbar unter: tps://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (abgerufen am 11.06.2020)(abgerufen am 11.06.2020) und Kurzpapier Nr. 18 zum Risiko für die Rechte und Freiheiten natürlicher Personen, Stand: 26.04.2018, abrufbar unter Hps://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (abgerufen am 11.06.2020); Art*ikel-29-Datenschutzgruppe, WP* 248 Rev. 01, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, angenommen am 4. April 2017, zuletzt überarbeitet und angenommen am 4. Oktober 2017, abrufbar unter: HYH://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (abgerufen am 11.06.2020).

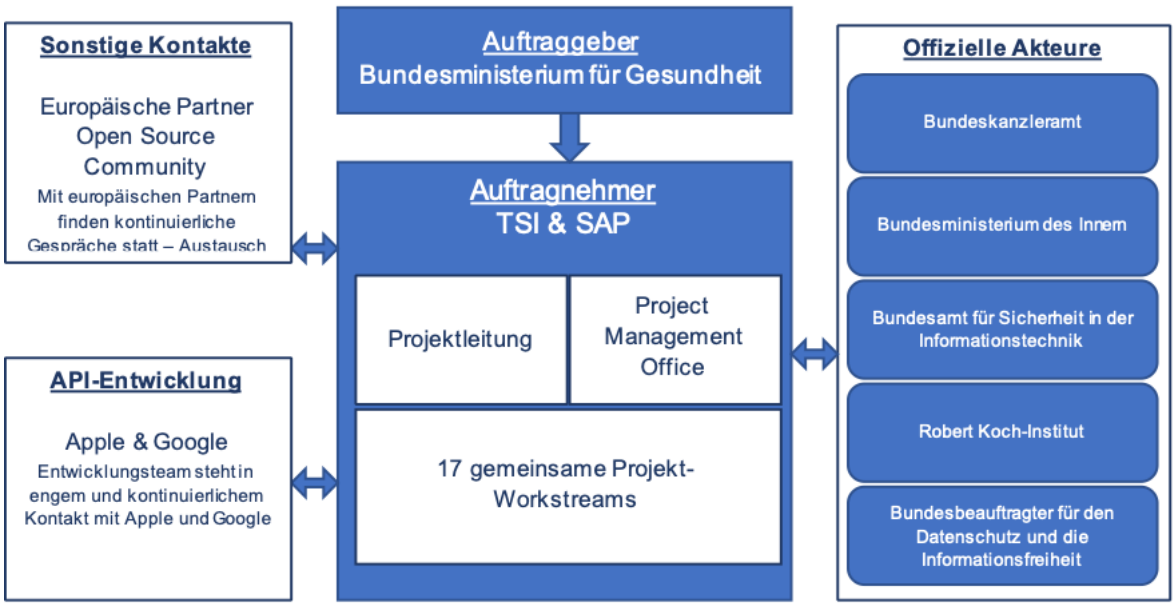


Abbildung 1: Übersicht über die Projektbeteiligten

6 Stammdaten der Organisationen

6.1 Rolle des Verantwortlichen

Die sich in der Entwicklung befindliche CWA und die CWA App werden nach ihrer Fertigstellung durch das Robert Koch-Institut (RKI) betrieben bzw. herausgegeben. Das RKI ist mithin Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO für die mit dem Betrieb der CWA einhergehende Verarbeitung der personenbezogenen Daten der Nutzer.

6.2 Name und Kontaktdaten des Verantwortlichen

Name/ Bezeichnung der datenverarbeitenden Stelle	Robert Koch-Institut
Straße/ Hausnummer	Nordufer 20
PLZ/ Ort	13353 Berlin
Telefon	030 18754-0
Telefax	030 18754 2328

E-Mail-Adresse	coronawarnapp@rki.de
Internet-Adresse	www.rki.de

Leitung	Prof. Dr. Lothar H. Weiler (Präsident)

Datenschutzbeauftragter	Dr. Jörg Lekschas
E-Mail-Adresse	datenschutz@rki.de

6.3 DSFA-Team

6.3.1 Rolle

Die DSFA wurde durch ein Team mit interdisziplinären Kompetenzen durchgeführt, dessen Mitglieder einerseits die verschiedenen Aspekte der benötigten Fachkenntnisse abdecken, andererseits aber auch Bewertungen und Entscheidungen über Maßnahmen zur Risikominimierung sowie Bewertungen über deren Auswirkungen auf die Zweckerreichung der CWA treffen können.

6.3.2 Zusammensetzung und Vorgehensplanung

Im Abstimmungstermin zwischen RKI und BfDI am 12.05.2020 wurde seitens Telekom/SAP der Vorschlag unterbreitet, dass die DSFA im Auftrag des RKI von der Telekom/SAP für das RKI durchgeführt wird. Hierzu gibt es im Datenschutz-Workstream parallele Arbeitsstränge, DSK und DSFA, welche Hand in Hand arbeiten. Diesem Vorschlag wurde seitens des RKI zugestimmt.

Beratend zur Seite standen dem Telekom/SAP-Team die Kanzlei Schürmann Rosenthal Dreyer Rechtsanwälte PartG mbB (SRD), mit der in den folgenden Tagen verschiedene Abstimmungen erfolgten: 1. Abstimmung mit dem BfDI erfolgt durch Schürmann Rosenthal Dreyer, 2. Methodik und Beispiel wurden von dem Telekom/SAP-Team vorgestellt, in einen gemeinsamen Datenraum zur Prüfung eingestellt und mit den Beteiligten abgestimmt. Im Anschluss wurde die Projektleitung mit der Dokumentation der DSFA für die CWA für das RKI beauftragt. Die DSFA wurde regelmäßig im Workstream Datenschutz abgestimmt. Der Workstream Datenschutz besteht seit dem 12.05.2020. Von Anfang an fanden regelmäßige Beratungen zwischen dem behördlichen Datenschutzbeauftragten des Auftraggebers (RKI), der Kanzlei Schürmann Rosenthal Dreyer und den weiteren Projektbeteiligten statt. Das BFDI stand hierbei dem RKI beratend zur Seite. Es wurde ein agiles Team unter Beteiligung der SAP, der Telekom (von Seiten der Entwickler) sowie der Rechtsanwaltskanzlei SRD

zusammengestellt. Der DSB des RKI steht dem DSFA-Team beratend zur Seite, wobei eine regelmäßige Einbindung des DSB in die Durchführung der DSFA nicht erfolgt ist, um die Unabhängigkeit bei der Prüfung der Ergebnisse der DSFA zu wahren.

Die Zusammensetzung im Einzelnen:

Vollständiger Name und Institution	**Qualifikation**	**Rolle bei der Durchführung der DSFA**
Harzendorf, Kerstin T-Systems MMS GmbH	Volljuristin	Erstellung Entwurf DSFA-Bericht, Erstellung Risikoanalyse-Matrix
Koch, Susanne T-Systems MMS GmbH	Volljuristin	Vorbereitung und Review/ Erfassung von Risiken, Clusterung, Maßnahmen
Jaen Pallares, Jordi T-Systems MMS GmbH	IT Security Architekt	Technische Bewertung/Threat Modelling
Duscha, Falko T-Systems MMS GmbH	Engineer/Consultant	Technische Bewertung/Threat Modelling
Dr. Gudymenko, Ivan T-Systems MMS GmbH	IT Security and Blockchain Architect	Technische Bewertung/Threat Modelling
Rosenthal, Simone Schürmann Rosenthal Dreyer Rechtsanwaelte	Rechtsanwältin	Rechtliche Beratung des RKI, Überarbeitung und Erstellung DSFA-Bericht (V 1.0)
Schürmann, Kathrin Schürmann Rosenthal Dreyer Rechtsanwaelte	Rechtsanwältin	Rechtliche Beratung des RKI, Überarbeitung und Erstellung DSFA-Bericht (V 1.0)
von der Heide, Roman Schürmann Rosenthal Dreyer Rechtsanwaelte	Rechtsanwalt	Rechtliche Beratung des RKI, Überarbeitung und Erstellung DSFA-Bericht (V 1.0)
Schieler, Charlotte Schürmann Rosenthal Dreyer Rechtsanwaelte	Rechtsanwältin	Überarbeitung und Erstellung DSFA-Bericht (V 1.0)

In Terminen am 03.06.2020, 04.06.2020 und 11.06.2020 erfolgte ein Review der Risikobewertung durch den Workstream Datenschutz, in Erweiterung um folgende Beteiligte:

Schweigkoffer, Rainer	Datenschutzexperte	Datenschutz- und Technikberatung (Entwicklung) (Gesamtprojekt)
Bruckmeier, Thorsten	Datenschutzexperte	Datenschutz- und Technikberatung (Entwicklung) (Gesamtprojekt)
Lissfeld, Dirk	Datenschutzexperte	Datenschutz- und Technikberatung (Telekom-Infrastruktur) (Gesamtprojekt)
Wagner, Frank	Datenschutzexperte	Unterstützung aus Sicht der Projektleitung

7 Notwendigkeit der DSFA

Art. 35 Abs. 1 DSGVO regelt die Pflicht zur Durchführung einer DSFA, soweit aufgrund des Umfangs, Kontexts oder Zwecks der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der von der Datenverarbeitung betroffenen Personen besteht.

Zur weiteren Konkretisierung der gesetzlichen Anforderungen haben die Datenschutzaufsichtsbehörden gemäß Art. 35 Abs. 4 DSGVO Listen erstellt und veröffentlicht, in denen Datenverarbeitungsvorgänge benannt werden, für die jedenfalls eine DSFA durchzuführen ist („Muss-Listen“).

Das Verfahren der CWA unterfällt der „Muss-Liste“ des BfDI[4] (dort die Verarbeitungstätigkeiten Nr. 4 a., 5, 7 c. und d. sowie 8).

Auch nach der Auffassung des Europäischen Datenschutzausschusses (EDSA) muss im Fall einer Corona-Tracing-App eine DSFA durchgeführt werden, weil „die Verarbeitung als mit einem hohen Risiko (Gesundheitsdaten, voraussichtliche flächendeckende Einführung, systematische Überwachung, Einsatz neuer technologischer Lösungen) behaftet eingestuft wird.“[5]

[4] BfDI - Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO für Verarbeitungstätigkeiten öffentlicher Stellen des Bundes.

[5] EDSA – Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhangmit dem Ausbruch von COVID-19 -Leitlinien, Rn. 39, S. 10 m.w.N.

Aufgrund des engen Zusammenhangs mit dem Verfahren der CWA App geht das DSFA-Team vorsorglich davon aus, dass auch hinsichtlich des Verfahrens der Verifikations-Hotline eine DSFA durchzuführen ist. Die Verifikations-Hotline wirkt sich wesentlich auf die Zweckerreichung der CWA App aus und ist somit Bestandteil des Gesamtprozesses.

8 Beschreibung der geplanten Verarbeitungsvorgänge (Prüfgegenstand)

Gegenstand dieser DSFA sind die nachfolgend beschriebenen Verarbeitungsvorgänge im Zusammenhang mit der Nutzung der CWA App durch einen Nutzer.

8.1 Kontext

Die CWA App ist eine mobile Applikation für Smartphones, die im Auftrag der Bundesregierung von der Deutschen Telekom AG und der SAP SE entwickelt und durch das RKI herausgegeben werden wird. Das RKI soll auch als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO für die mit dem Betrieb des Gesamtsystems der CWA einhergehende Verarbeitung der personenbezogenen Daten der Nutzer der CWA App fungieren.

Die CWA App nutzt das von Apple und Google entwickelte Expositionsbenachrichtungswerkzeug (ENF) für „Privacy-Preserving Contact Tracing“, das Bestandteil der Betriebssysteme Android (ab Version 6) und iOS (ab Version 13.5) ist und es Smartphones erlaubt, wechselnde zufallsgenerierte Kennnummern (sogenannte RPIs) zur Kontaktnachverfolgung per Bluetooth Low Energy (BLE) im Hintergrund auszutauschen, ohne dass die Akkulaufzeit des Smartphones merklich darunter leiden soll.

Die CWA App soll dazu beizutragen, dass Coronavirus-Infektionsketten schneller erkannt und somit unterbrochen werden können. Um dieses Ziel zu erreichen soll die CWA App die Nutzer zum einen zuverlässig und schnell über Begegnungen mit anderen infizierten Nutzern informieren und so vor einer möglichen Ansteckung mit dem Coronavirus warnen. Zum anderen sollen die Nutzer in nahezu Echtzeit über ein (positives) Testergebnis informiert werden, so dass sie sich freiwillig isolieren, andere Nutzer warnen und weitere aus epidemiologischer Sicht gebotene Maßnahmen ergreifen können.

Die CWA App und das ENF sind zentrale Komponenten des Gesamtsystems der CWA. Weitere Komponenten der CWA sind der CWA Server, der Verifikationsserver und weitere Systeme. Die Funktionen der datenschutzrechtlich relevanten Komponenten der CWA werden nachfolgend erläutert.

Der Verifikations-Hotline kommt insoweit eine der CWA App dienende Funktion zu. Sie erlaubt es infizierten Nutzern ihr Testergebnis zu teilen, wenn eine Testregistrierung nicht möglich ist.

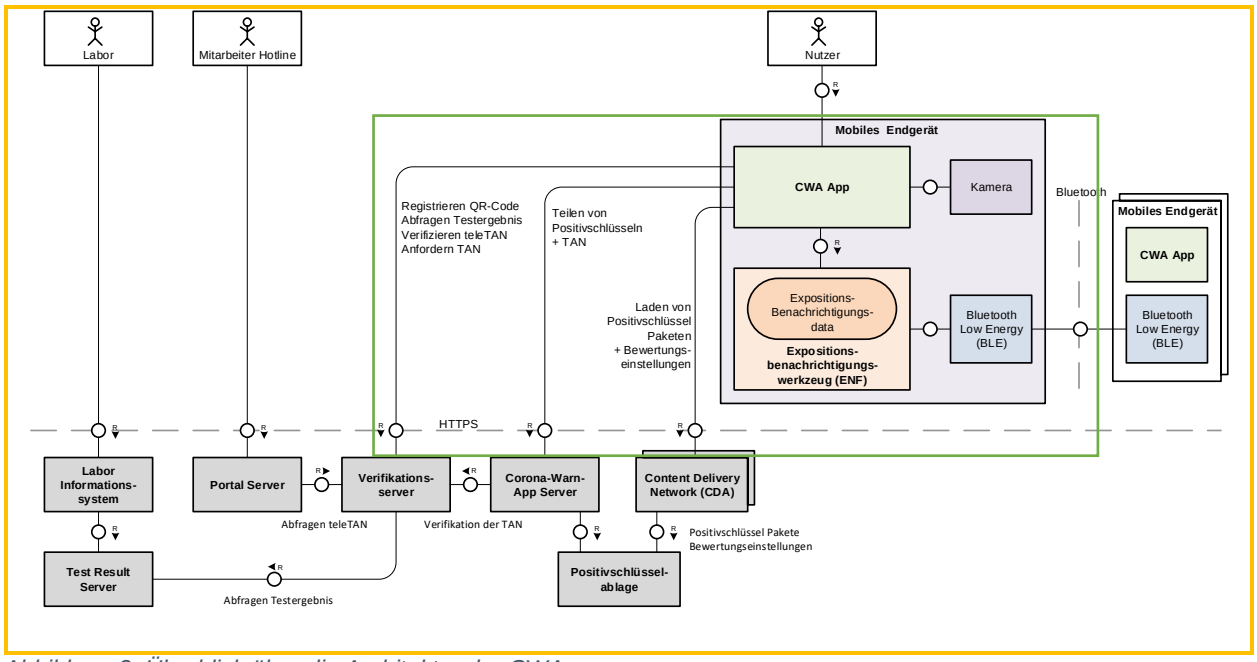


Abbildung 2: Überblick über die Architektur der CWA

8.2 Zweck der Datenverarbeitung

Die Datenverarbeitungsvorgänge in Zusammenhang mit dem Betrieb der CWA dienen folgenden Zwecken:

(1) Der Nutzer soll durch die CWA App automatisch anhand der erfassten Kennungen anderer App-Nutzer unter Verwendung des von Apple und Google entwickelten COVID-19-Kontaktprotokolls ohne Identifizierung einzelner Personen darüber informiert werden, dass er sich in der Nähe eines mit dem Coronavirus infizierten anderen App-Nutzers aufgehalten hat und wegen des Zeitpunkts (Datum), der Dauer und des Abstands zum infizierten App-Nutzer ein möglicherweise erhöhtes Infektionsrisiko besteht. Unter Berücksichtigung der räumlichen Nähe zu infizierten App-Nutzern innerhalb eines epidemiologisch relevanten Zeitraums werden hierbei dem App-Nutzer auf Basis der aktuellen Empfehlungen des RKI Informationen zu seinem Infektionsrisiko und Empfehlungen zu Gesundheits- und Infektionsschutzmaßnahmen bereitgestellt, um Infektionsketten zu unterbrechen.
(Anwendungsphase 1 und Anwendungsphase 2)

(2) Soweit der Nutzer es wünscht, soll er im Nachgang zu einem bei ihm durchgeführten Coronavirus-Test möglichst schnell und direkt über sein Testergebnis durch die CWA App informiert werden, so dass der CWA App-Nutzer im Fall eines positiven Testergebnisses ohne Zeitverlust Maßnahmen zur eigenen Gesundheitsfürsorge und zur Reduzierung des Ansteckungsrisikos für andere Personen ergreifen kann und somit Infektionsketten so früh wie möglich unterbrochen werden können. Hierzu kann der Nutzer unter anderem sein positiven Testergebnis innerhalb der CWA verfügbar machen.
(Anwendungsphase 3)

(3) Soweit der Nutzer es wünscht, kann er Information über ein positives Testergebnis und damit im Zusammenhang stehende weitere freiwillige Angaben (ab Version 1.1) der CWA verfügbar machen, so dass diese im vorausgegangenen Kontaktfall das Risiko ermitteln und andere App-Nutzer darüber informieren kann, dass sie sich in unmittelbarer Nähe zu einer Person aufgehalten haben, die nachweislich Träger des Coronavirus ist.
(Anwendungsphase 4)

Folgende „benachbarte“[6] Zwecke werden nicht im Rahmen der CWA verfolgt:

- Nachverfolgung der geographischen Verbreitung des Coronavirus,
- Echtzeit-Warnungen von/vor Corona-positiv getesteten Personen in spontanen Begegnungen,
- Überwachung von infizierten Nutzern (z. B. Einhaltung von Quarantäneauflagen),
- Ausbau von flächendeckenden Überwachungsstrukturen,
- Erstellung von Prognosen für die epidemiologische Verbreitung (z. B. Verbreitung und Verlauf von COVID-19-Erkrankungen),
- App-basierte Behandlung von an COVID-19-Erkrankten.

Falls Daten, Prozesse oder sonstige Mittel der CWA für diese Zwecke (doch) genutzt werden sollen, muss eine entsprechende DSFA durchgeführt bzw. die vorliegende DSFA um eine Betrachtung der jeweiligen benachbarten Zwecke erweitert werden.

8.3 Ablauf aus Sicht des Nutzers

8.3.1 Download und Installation der CWA App

Die CWA App wird in den App-Stores von Google (Play Store) und Apple (App Store) für Nutzer ab 16 Jahren bereitgestellt. Die Altersbeschränkung wird bei der Einreichung der CWA App eingestellt und später auch in den App-Stores angezeigt. Wenn sich ein Nutzer für das Laden der CWA App entscheidet, werden seine Zugriffsdaten (einschließlich der verwendeten IP-Adresse) und weitere Daten (z. B. Login-Daten) vom Betreiber des jeweiligen App-Stores verarbeitet. Nach Abschluss des Downloads wird die CWA App automatisch auf dem Smartphone installiert.

Für das Laden der CWA-App benötigt der Nutzer ein persönliches Nutzerkonto bei dem jeweiligen App-Store, der den jeweils gültigen Datenschutzbestimmungen und

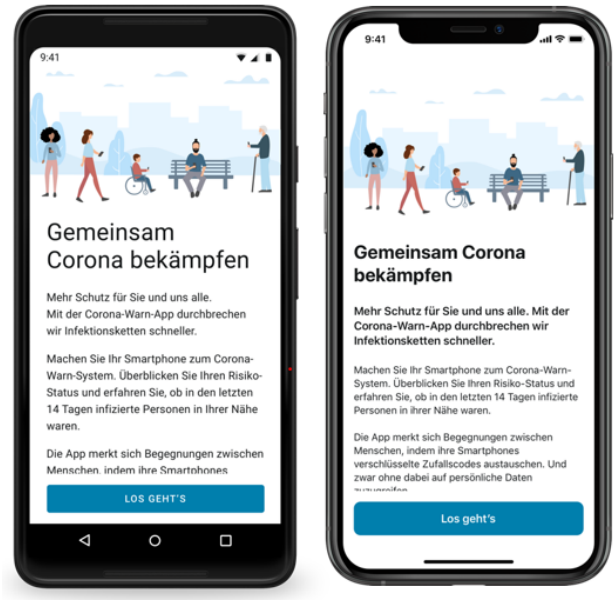
[6] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), Datenschutz-Folgenabschätzung für die Corona App, Version 1.6, 4.4, S. 32 ff., abrufbar unter: https://www.fiff.de/dsfa-corona.

Nutzungsbedingungen des jeweiligen Betreibers unterliegt. Auf der CWA App-Store-Beschreibungsseite der CWA App kann der Nutzer vor dem Laden der CWA App die Datenschutzerklärung und die Nutzungsbedingungen der CWA App aufrufen.

8.3.2 Initialer Start der CWA App

Die CWA App fragt bei jedem Start die eingestellte Systemsprache ab, um dem Nutzer die Benutzeroberfläche der CWA App in der Systemsprache anzuzeigen. Wenn die Benutzeroberfläche der CWA App nicht in der Systemsprache angeboten wird, wird die englische Sprachfassung verwendet. Zunächst wird die CWA App in deutscher und englischer Sprache angeboten. Weitere Sprachen (Türkisch, Arabisch und Russisch) sind bereits geplant und sollen zeitnah verfügbar sein.

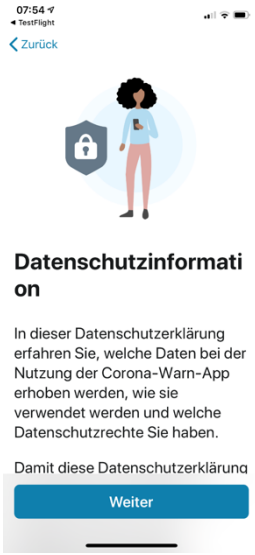
Unmittelbar nach dem initialen Start der CWA App erhält der Nutzer einmalig eine Einführung in die CWA App. Diese Einführung besteht aus den folgenden Schritten:



Schritt 1:

Auf dem ersten Bildschirm, der nach dem initialen Start der CWA App angezeigt wird, werden die Zwecke und die Funktionsweise der CWA App vorgestellt. Durch Antippen des Buttons „Los geht's“ gelangt der Nutzer zu Schritt 2.

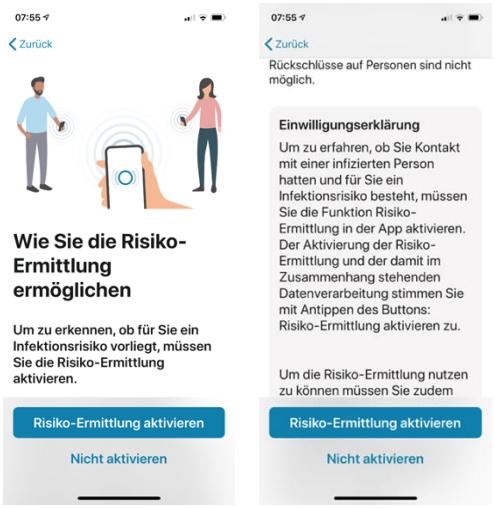
Abbildung 3: Schritt 1 der Einführung (links Android, rechts iOS)



Schritt 2:

Anzeige der Datenschutzerklärung der CWA App. Nach Antippen des Buttons „Weiter“ wird der Nutzer zur Aktivierung der Risikoermittlung weitergeleitet.

Abbildung 4: Anzeige der Datenschutzerklärung (Beispiel-Screenshot iOS)



Schritt 3:

Dem Nutzer wird erklärt, wie die Risiko-Ermittlung und Protokollierung der Begegnungen funktioniert. Durch Antippen des Buttons „Risikoermittlung aktivieren“ willigt der Nutzer in die Aktivierung der Risikoermittlung ein.

Abbildung 5: Aktivierung der Risikoermittlung (Beispiel-Screenshot iOS)

Schritt 3a:

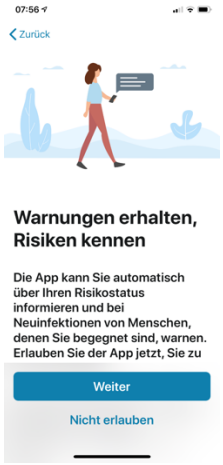
Nutzer-Dialog des Betriebssystems zur Aktivierung des ENF.

Abbildung 6: Nutzer-Dialog des Betriebssystems (Beispiel-Screenshot iOS)

Schritt 4:

Anzeige von empfohlenen Maßnahmen für den Fall, dass der Nutzer positiv getestet wird.

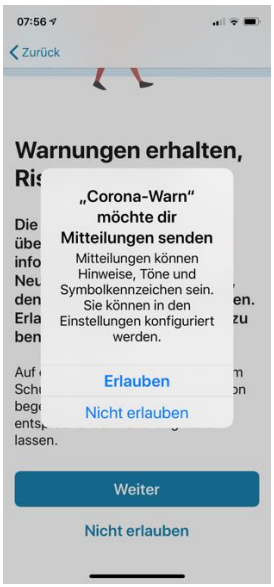
Abbildung 7: Anzeige von empfohlenen Maßnahmen (Beispiel-Screenshot iOS)



Schritt 5:

Beschreibung, zu welchen Zwecken die CWA App lokale Benachrichtigungen sendet.

Abbildung 8: Beschreibung der Zwecke (Beispiel-Screenshot iOS)



Schritt 5a (nur iOS):

Nutzer-Dialog des Betriebssystems zum Erlauben von Mitteilungen.

Abbildung 9: Nutzer-Dialog (nur iOS)

8.3.3 Home-Bildschirm

Der Home-Bildschirm wird nach dem Abschluss der Einführung und bei jedem weiteren Start der CWA App angezeigt. Dort werden der aktuelle Status der Risiko-Ermittlung (aktiv/inaktiv), der für den Nutzer ermittelte Risikostatus (z. B. „niedriges Risiko“) sowie die für den Nutzer

aktuell verfügbaren weiteren Funktionen (z. B. Testregistrierung, Testergebnis teilen, Einstellungen) und Inhalte (z. B. Glossar) angezeigt.

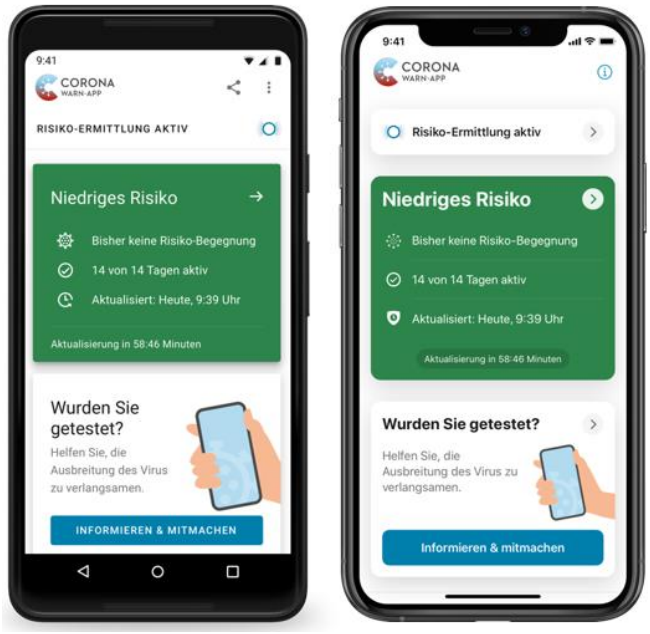


Abbildung 10: Home-Bildschirm bei "Niedrigem Risiko" (links Android, rechts iOS)

8.3.4 Risiko-Ermittlung

Der Nutzer erreicht den Hauptbildschirm der Risiko-Ermittlung über den Risikoermittlungs-Status im Kopf des Home-Bildschirms und über die Funktion „Einstellungen“. Die zentrale Bedeutung der Funktion „Risiko-Ermittlung“ wird erläutert und lässt sich vom Nutzer aktivieren bzw. deaktivieren. Im Falle einer Störung der Risiko-Ermittlung (z. B. weil der Nutzer die Bluetooth-Funktion seines Smartphones deaktiviert hat) wird dem Nutzer der Grund dieser Beeinträchtigung angezeigt und ein Lösungsweg vorgeschlagen.

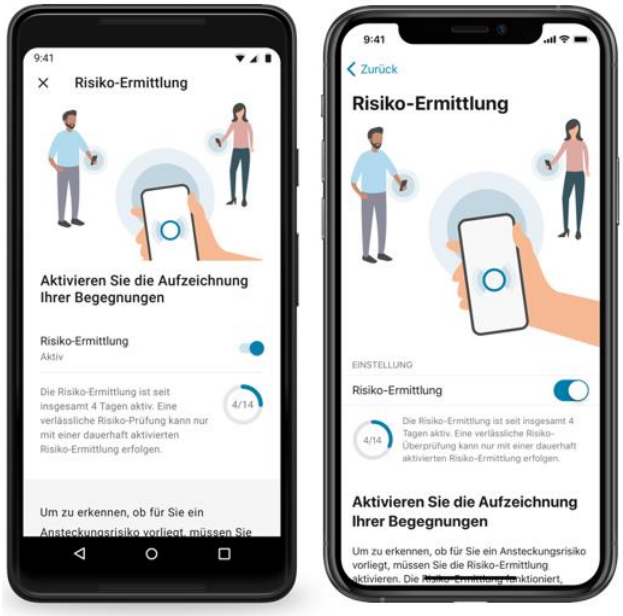


Abbildung 11: Bildschirm der Risiko-Ermittlung (links Android, rechts iOS)

8.3.5 Risikodetails und Risikostufen

Der Bildschirm „Risikodetails“ wird über Antippen des Pfeils bei der Anzeige des Risikostatus auf dem Home-Bildschirm aufgerufen. Die Detailanzeige wiederholt die Informationen der Risiko-Anzeige im Kopfbereich des Home-Bildschirms. Der Inhaltsbereich zeigt dem Nutzer Verhaltensempfehlungen entsprechend dem für ihn ermittelten Risikostatus an. Zudem wird erklärt, wie und wann der Risikostatus ermittelt wurde, etwa durch Angabe der Anzahl der Risiko-Begegnungen und den Zeitpunkt der letzten Aktualisierung des Risikostatus.

Der Risikostatus wird einer der folgenden Stufen zugeordnet:

(1) Unbekanntes Risiko
(2) Niedriges Risiko
(3) Erhöhtes Risiko

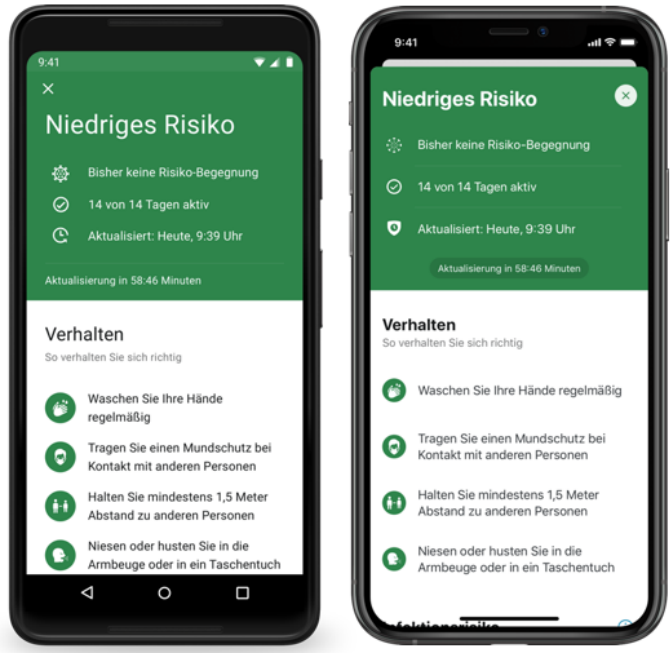


Abbildung 12: Anzeige der Risikodetails bei "niedrigem Risiko" (links Android, rechts iOS)

Im Fall eines niedrigen Risikos ist der Bildschirm teilweise grün und im Fall eines erhöhten Risikos rot hinterlegt.

8.3.6 Test registrieren

Im Fall eines durchgeführten Tests kann der Nutzer über die CWA App den digitalen Testinformationsprozess starten und sich so über den Status des Tests bzw. das Testergebnis in der CWA App informieren.

Ist das Labor an die Systeme zum Testergebnisabruf angeschlossen, wird bei der Durchführung des Tests der Nutzer seitens der testdurchführenden Stelle gefragt, ob er sein Testergebnis über die CWA App erhalten will und mit einer entsprechenden Übermittlung des Testergebnisses an die Serverinfrastruktur (Test Result Server) der CWA einverstanden ist. Sofern der Nutzer einwilligt, wird die Einwilligung auf dem Proben-Formular notiert und dem Nutzer in einem Begleitdokument (Probenbegleitschein) der QR-Code bereitgestellt, den er benötigt, um den Testergebnisabruf in der CWA App zu aktivieren. In diesem Fall kann dann die Zuordnung der Proben sowie der Testergebnisse durch den QR-Code erfolgen (der eine Kennzahl enthält), wenn der Nutzer in den weiteren Verarbeitungsprozess einwilligt.

Liegt eine Einwilligung vor, kann der Nutzer den QR-Code in der CWA App mit der Kamera seines Smartphones scannen. Die CWA App liest dann die GUID aus dem QR-Code aus.

Der Prozess zum Abruf eines Testergebnisses erfolgt über eine zyklische Abfrage von Statusänderungen durch die CWA App, die sich auf das Vorliegen eines Testergebnisses beziehen. Sofern ein Testergebnis vorliegt, wird dieses gelesen und auf dem Home-Bildschirm angezeigt. Über die lokale Benachrichtigungsfunktion wird der Nutzer über das Vorliegen des Testergebnisses informiert. Die Benachrichtigung selbst enthält keine Information über das konkrete Ergebnis des Tests. Erst nach dem Öffnen der CWA App wird dem Nutzer das Testergebnis auf dem Home-Bildschirm der CWA App einmalig angezeigt.

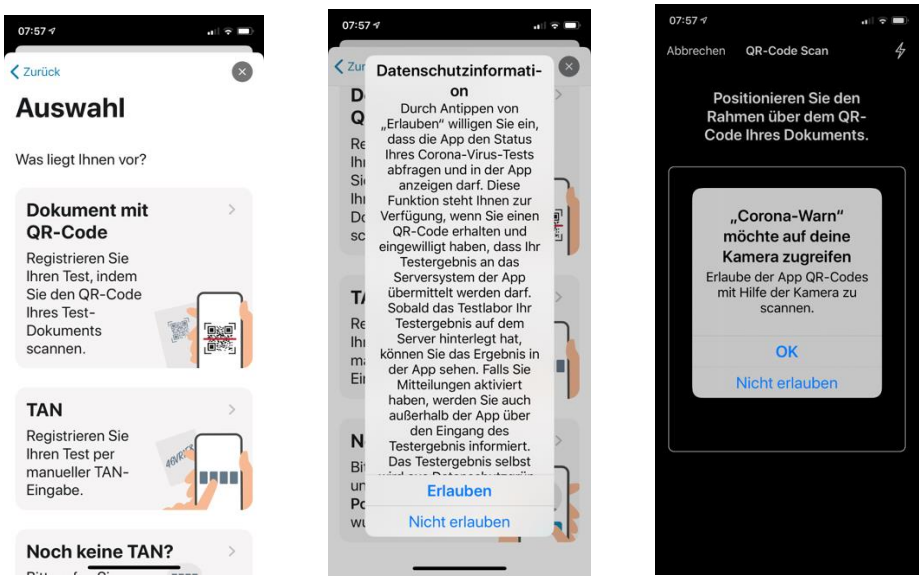


Abbildung 13: Test-Registrierung, QR-Code Verfahren (Beispiel-Screenshot iOS)

8.3.7 Verifikations-Hotline

Die Verifikations-Hotline steht Nutzern der CWA App zur Verfügung, welche die Funktion der Kontaktverfolgung der CWA App genutzt haben, denen der Testergebnisabruf jedoch nicht zur Verfügung steht. Die Ergebnisabfrage ist nicht möglich, wenn kein QR-Code mit dem Testergebnis verknüpft ist. Das ist dann der Fall, wenn das Labor oder der testende Arzt nicht an die Systeme zur Bereitstellung der Testergebnisse angeschlossen, der QR-Code des Labors oder des Nutzers aufgrund von Beschädigungen nicht lesbar ist oder kein QR-Code an Labor oder Nutzer ausgegeben wurde.

In diesem Fall kann sich der Nutzer an die Verifikations-Hotline wenden. Dem anrufenden Nutzer werden durch einen Mitarbeiter der Verifikations-Hotline gemäß einem abgestimmten Skript Plausibilitätsfragen gestellt, um die Gefahr eines Missbrauchs der Verifikations-Hotline zu verringern. Wenn der Mitarbeiter der Verifikations-Hotline die Antworten für schlüssig hält und den Anrufer somit als einen infizierten Nutzer verifiziert, fragt er ihn nach seiner Telefonnummer. Der anrufende Nutzer gibt seine Telefonnummer fernmündlich durch, der Verifikations-Hotline Mitarbeiter notiert sich die Telefonnummer schriftlich. Danach beendet der Mitarbeiter der Verifikations-Hotline das Gespräch, um über eine Weboberfläche bei dem Portalserver eine teleTAN abzufragen. Die teleTAN wird dem infizierten Nutzer sodann im Rahmen eines Rückrufs mündlich mitgeteilt. Durch den Rückruf soll die Authentizität des Anrufers weiter erhöht und die Gefahr eines Missbrauchs der Verifikations-Hotline verringert werden.

Die teleTAN hat eine Gültigkeit von einer Stunde. Innerhalb dieses Zeitraums kann der infizierte Nutzer die teleTAN in der CWA App eingeben. Die durch den Mitarbeiter der Verifikations-Hotline notierten Kontaktdaten des Nutzers werden spätestens nach einer Stunde vernichtet.

8.3.8 Testergebnis teilen

Wenn der Nutzer positiv auf das Coronavirus getestet wurde, kann er sein Testergebnis mit anderen Nutzern teilen und diese so über eine mögliche Ansteckung informieren. Die anderen Nutzer, die mit dem (infizierten) Nutzer in Kontakt waren, erfahren dabei nicht, welcher ihrer Kontakte das Testergebnis geteilt hat.

Abbildung 14: Test-Ergebnis teilen (Beispiel-Screenshot iOS)

8.3.9 Sonstige Funktionen

Neben den oben beschriebenen Hauptfunktionen umfasst die CWA App folgende weitere Funktionen:

8.3.9.1 CWA teilen

Über den Home-Bildschirm kann der Nutzer die CWA App mit anderen Personen „teilen“. Das eigentliche Teilen findet außerhalb der CWA App über die hierfür vorgesehene Schnittstelle des Betriebssystems statt. Die CWA App erhält somit keinen Zugriff die Kontakte des Nutzers.

8.3.9.2 App Informationen

Über den Home-Bildschirm kann der Nutzer den Bereich „App Informationen“ aufrufen. In diesem Bereich werden die gesetzlichen Pflichtinformationen (Datenschutzerklärung, Impressum) sowie weitere rechtliche Informationen (z. B. Open-Source-Lizenzhinweise) angezeigt. Zudem kann der Nutzer hier auf die „Häufige Fragen“-Seite zugreifen.

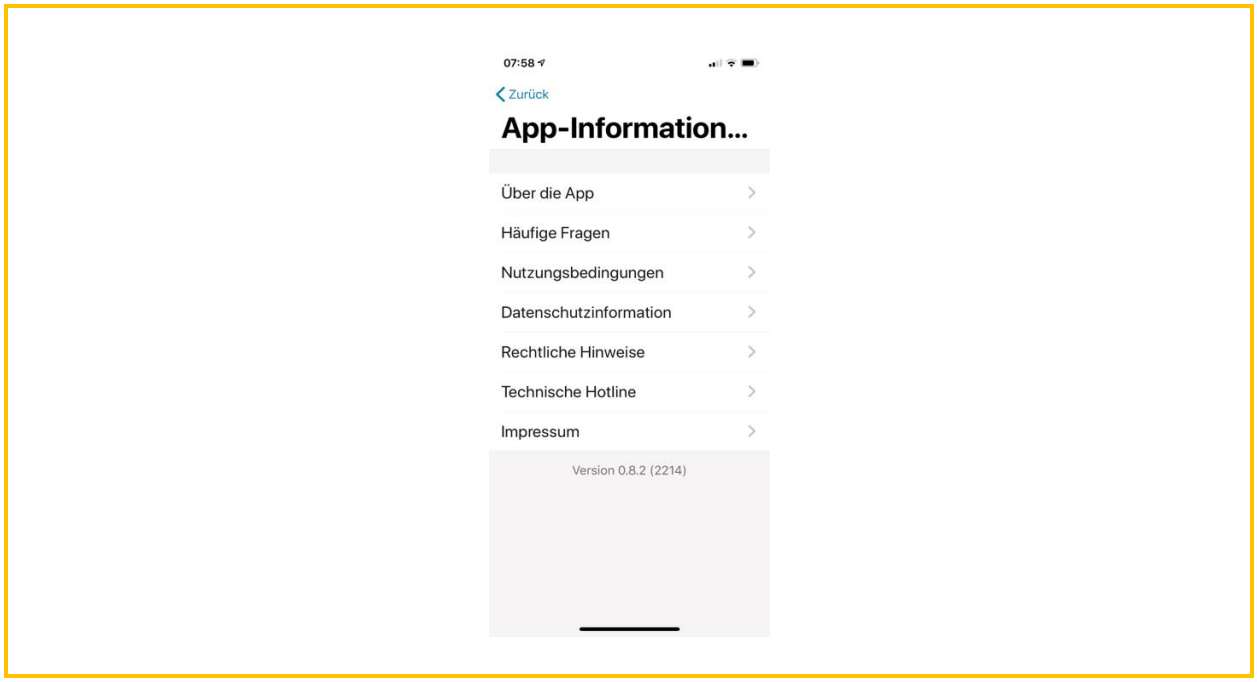


Abbildung 15: App-Information (Beispiel-Screenshot iOS)

8.3.9.3 Einstellungen

Über den Home-Bildschirm kann der Nutzer den Bereich „Einstellungen“ aufrufen. In diesem Bereich befinden sich alle Konfigurationsmöglichkeiten der CWA App, die vom Nutzer eigenständig vorgenommen werden können, etwa welche Mitteilungen die CWA App dem Nutzer zusenden darf. Zudem wird eine Funktion zum Zurückzusetzen der CWA App bereitgestellt.

8.3.9.4 Glossar

Über den Home-Bildschirm kann der Nutzer den Bereich „Glossar“ aufrufen. In diesem Bereich werden Anwenderhinweise sowie Erläuterungen zu wichtigen in der CWA App verwendeten (Fach-)Begriffen in einfacher Sprache erklärt.

8.4 Systemarchitektur

Für die technische Umsetzung der CWA wurde von den Auftragnehmern T-Systems International GmbH und SAP Deutschland SE & CO. KG eine spezielle Systemarchitektur konzipiert, die die Anforderungen von Datenschutz und Datensicherheit besonders berücksichtigt. Das System ist so konzipiert, dass eine Identifizierung einzelner Nutzer durch die an der Datenverarbeitung beteiligten Stellen und andere Nutzer ausgeschlossen werden kann. Die für die datenschutzrechtliche Betrachtung maßgeblichen Komponenten der Architektur werden nachfolgend beschrieben.

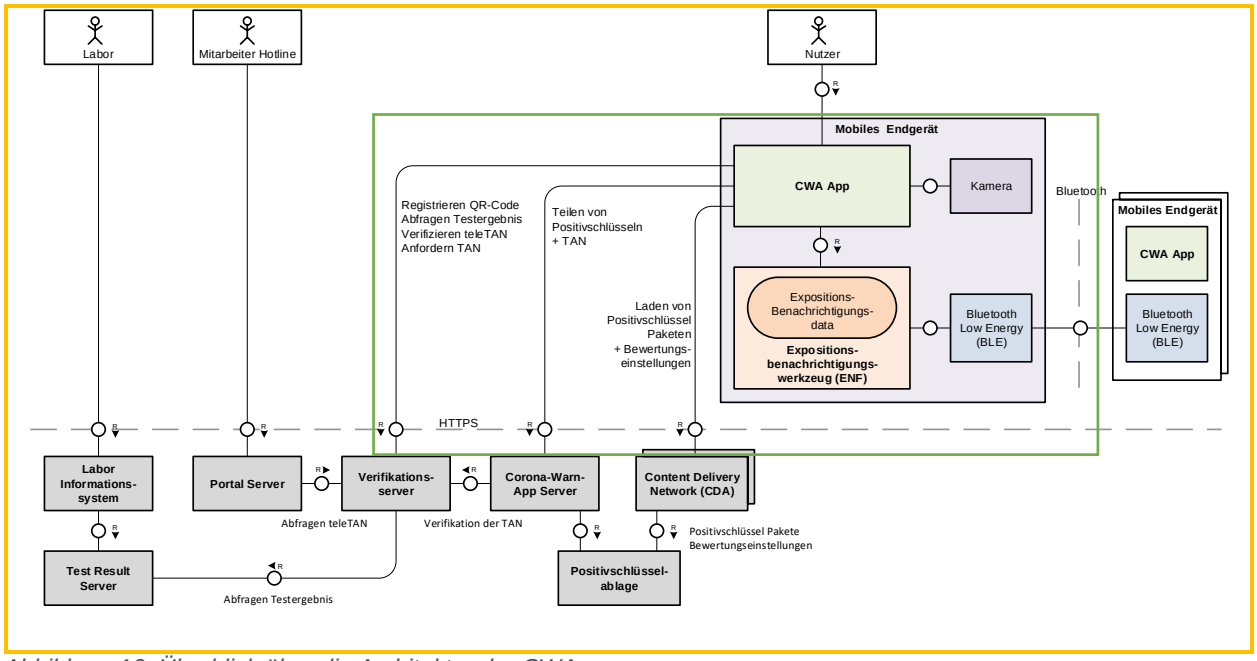


Abbildung 16: Überblick über die Architektur der CWA

8.4.1 Smartphone (Mobiles Endgerät)

Das Smartphone (einschließlich seines Betriebssystems) stellt die für den Betrieb der CWA App notwendigen Funktionalitäten und Konnektivitäten bereit. Für den Betrieb der CWA App werden insbesondere benötigt:

Internetkommunikation:

Die CWA App benötigt eine Internetverbindung, um auf die Server der CWA (CWS Server, CDN-Magenta und Verifikationsserver) zugreifen zu können.

Kamera:

Die CWA App benötigt Zugriff auf die Kamera des Smartphones, um den QR-Code im Rahmen der Testregistrierung zu scannen.

Expositionsbenachrichtigungswerkzeug:

Das ist ein Bluetooth-Low-Energy-Dienst. Er wurde von Apple und Google vor dem Hintergrund der Corona-Pandemie entwickelt, um Apps die Annäherungserkennung zwischen Geräten zur Berechnung eines Ansteckungsrisikos zu ermöglichen. Zurzeit erlauben Apple und Google nur einer App pro Land die Nutzung des ENF, wobei die CWA App von einer Gesundheitsbehörde angeboten werden muss.

8.4.2 CWA Server

Der CWA Server wird für die Funktion „Testergebnis teilen“ benötigt. Wenn der Nutzer sein (positives) Testergebnis in der CWA App mit anderen Nutzern teilt, stellt seine Instanz der CWA App eine verschlüsselte Verbindung zum CWA Server her. Über diese Verbindung werden dann die für die Warnung seiner Kontakte notwendigen Kennungen (Positivschlüssel) von der CWA App an den CWA Server übermittelt.

8.4.3 CDN-Magenta (Content Delivery Network)

Das Serversystem CDN-Magenta wird ebenfalls für die Funktion „Testergebnis teilen“ sowie für die Funktion „Risiko-Ermittlung“ benötigt.

Das CDN-Magenta stellt der CWA App eine Liste mit den Positivschlüsseln aller Nutzer, die in der CWA App ihr Testergebnis geteilt haben, zum Download über eine verschlüsselte Verbindung bereit. Die Liste mit den Positivschlüsseln wird von der CWA App zyklisch abgefragt (auch im Hintergrundbetrieb). Die Nutzer können auch manuell eine Aktualisierung der Bewertung des Ansteckungsrisikos anstoßen.

Daneben stellt das CDN-Magenta der CWA App die aktuellen Bewertungseinstellungen (BWE) zur Verfügung. Die BWE beinhalten die Konfigurationseinstellung für die Analyse und die Risikobewertung der Kontakte, deren Ergebnis die Höhe des Ansteckungsrisikos ist. Der BWE wird vom RKI konfiguriert. Es können auf diese Weise neue epidemiologische Erkenntnisse in die Risikoermittlung einfließen. Details siehe unter Ziffer 8.6.6 (Bewertungseinstellungen).

8.4.4 Verifikationsserver

Der Verifikationsserver dient der Validierung von positiven Testergebnissen, die über die Funktion „Testergebnis teilen“ mit anderen Nutzern der CWA App geteilt werden. Zur Echtheitsprüfung verwendet der Verifikationsserver eine TAN. Die TAN ist eine einmal verwendbare Transaktionsnummer, die beim Abruf des Testergebnisses automatisch generiert und dann in der CWA App abgelegt wird.

Sofern der Nutzer das Testergebnisses nicht in der CWA App erhalten hat, kann der Nutzer eine sogenannte teleTAN über die Verifikations-Hotline der CWA erhalten. Die teleTAN kann

der Nutzer dann in der CWA App eingeben. Der Verifikationsserver prüft sodann die Gültigkeit der teleTAN. Ist die teleTAN gültig, wird eine „normale“ TAN in der CWA App abgelegt.

8.4.5 Portalserver

Der Portalserver stellt dem Mitarbeiter der Verifikations-Hotline eine Funktion zur Abfrage der teleTANs zur Verfügung. Über ein Web-Interface, das mit dem Portalserver verbunden ist, kann der Mitarbeiter eine teleTAN generieren. Der Mitarbeiter muss sich einmal pro Arbeitssitzung durch eine Zwei-Faktor-Authentifizierung (Benutzername + Passwort + Code per SMS) an der Weboberfläche anmelden. Der Portalserver verbindet sich mit dem Verifikationsserver, der die einstündig gültige teleTAN generiert. Sodann wird die teleTAN wird im Klartext an den Portalserver zurückgegeben und von dort über das Web-Interface dem Mitarbeiter der Verifikations-Hotline zur Verfügung gestellt. Zudem wird ein Hashwert der teleTAN gebildet und auf dem Verifikationsserver gespeichert,

8.4.6 Test Result Server

Der Test Result Server stellt die Datenbank bereit, in welche die Labore die Testergebnisse der Nutzer eintragen können. Die Labore greifen über die Software Lab Client auf den Test Result Server zu.

8.5 Datenflüsse und Prozesse

Nachfolgend wird dargestellt, in welchen Anwendungsphasen durch welche Akteure welche Daten verarbeitet und übertragen werden. Dabei werden vier Anwendungsphasen unterschieden, die sich auch überschneiden können:

- Anwendungsphase 1: Risiko-Ermittlung (Risiko-Ermittlung ist aktiv, kein Kontaktfall)
- Anwendungsphase 2: Kontaktfall (Risiko-Ermittlung ist aktiv, Kontaktfall)
- Anwendungsphase 3: Test registrieren (Risiko-Ermittlung ist aktiv oder inaktiv, Nutzer hat QR-Code erhalten)
- Anwendungsphase 4: Testergebnis teilen (Risiko-Ermittlung ist aktiv oder inaktiv, Nutzer hat ein positives Testergebnis), evtl. nach Verifikations-Hotline (Risiko-Ermittlung ist aktiv oder inaktiv, automatisierte Testabfrage ist nicht möglich)

Abschließend wird zudem die Phase der Deinstallation der CWA App betrachtet.

Die Darstellung erfolgt aus der Perspektive eines Nutzers der CWA App.

8.5.1 Anwendungsphase 1: Risiko-Ermittlung

In der ersten Anwendungsphase werden RPIs zwischen dem Smartphone des Nutzers und den Smartphones anderer Nutzer der CWA App per BLE im Rahmen der Kontaktprotokollierung des ENF ausgetauscht (Schritt 1).

Zudem lädt die CWA App des Nutzers regelmäßig die Liste mit den Positivschlüsseln vom CDN-Magenta über das Internet (Schritt 2). Anschließend werden die empfangenen RPIs mit den heruntergeladenen Positivschlüsseln gematcht (Schritt 3).

8.5.1.1 Schritt 1: Kontaktprotokollierung

Der Austausch von RPIs im Rahmen der Kontaktprotokollierung findet unter folgenden Voraussetzungen statt:

- Der Nutzer hat die Funktion „Risiko-Ermittlung“ aktiviert
- Der Nutzer hat das Expositionsbenachrichtigungswerkzeug aktiviert
- Der Nutzer hat die Bluetooth-Schnittstelle seines Smartphones aktiviert

Der nachfolgend dargestellten Datenflüsse und Prozesse hinsichtlich Schritt 1 finden außerhalb der CWA App, nämlich im Expositionsbenachrichtigungswerkzeug statt.

Für die Kontaktprotokollierung verwendet das Expositionsbenachrichtigungswerkzeug zwei verschiedene Datenstrukturen:

- Tagesschlüssel (Temporary Exposure Keys)
- RPIs (Rolling-Proximity-Identifier)

Der Tagesschlüssel ist ein Zufallswert, der einmal täglich generiert wird und als Tagesschlüssel fungiert.

Aus dem Tagesschlüssel wird alle 10 bis 20 Minuten ein neuer RPI abgeleitet.

Der jeweils zuletzt abgeleitete RPI wird vom Smartphone mittels BLE alle fünf Minuten für zwei Sekunden versendet.

Gleichzeitig empfängt das Smartphone die auf diese Weise von anderen Smartphones ausgesendeten RPIs.

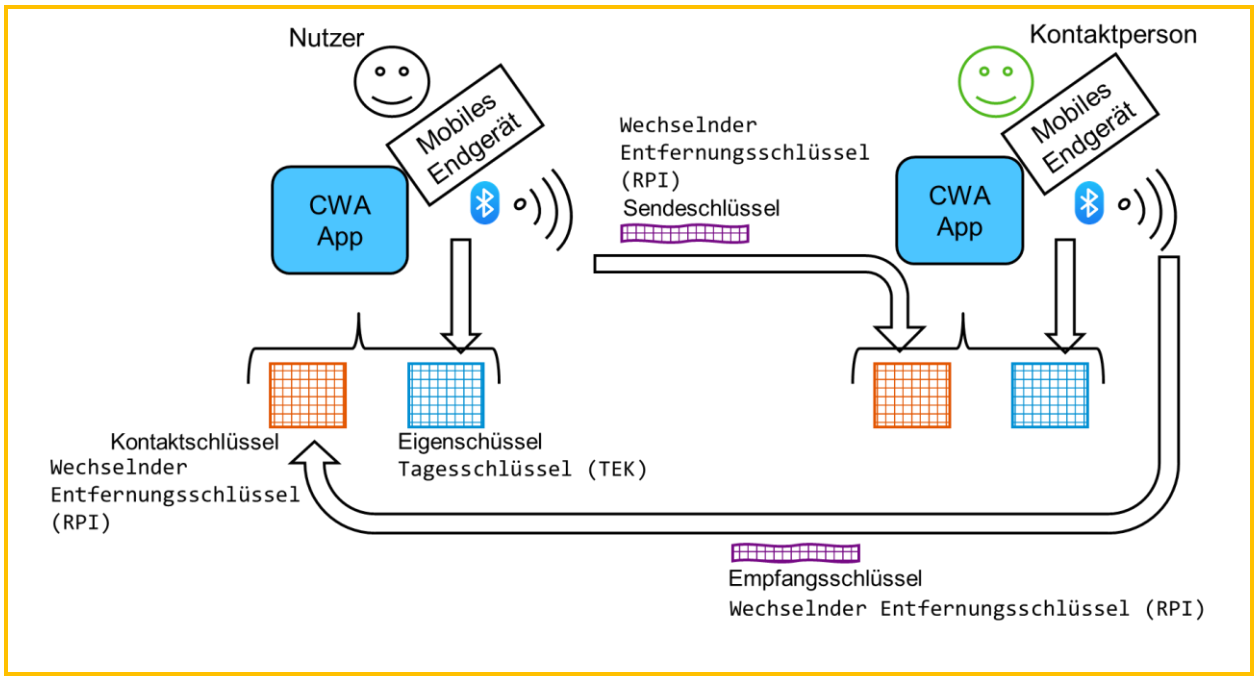


Abbildung 17: Austausch von RPIs

Diese vom Smartphone empfangenen RPIs werden im Kontaktprotokoll des Expositionsbenachrichtigungswerkzeugs über einen Zeitraum von zwei Wochen gespeichert und anschließend gelöscht. Zusammen mit den RPIs werden auch diesbezügliche Metadaten im Kontaktprotokoll gespeichert. Die gespeicherten Metadaten umfassen Angaben zum Datum des Kontakts, zur Kontaktdauer und zum Dämpfungswert (Signalstärke) des Bluetooth-Signals. Die Kontaktdauer wird in 5-Mintutenintervallen für maximal 30 Minuten protokolliert.

8.5.1.2 Schritt 2: Download der Positivschlüssel

Der Download der Liste der Positivschlüssel findet unter folgenden Voraussetzungen statt:

- Der Nutzer hat die Funktion „Risiko-Ermittlung“ aktiviert
- Der Nutzer hat das Expositionsbenachrichtigungswerkzeug aktiviert
- Der Nutzer hat die Bluetooth-Schnittstelle seines Smartphones aktiviert
- Das Smartphone des Nutzers ist mit dem Internet verbunden

Ein Positivschlüssel ist ein Tagesschlüssel eines Nutzers, der per CWA App sein (positives) Testergebnis geteilt hat.

Die CWA App ruft in regelmäßigen Abständen und bei manueller Aktualisierung des Ansteckungsrisikos von dem CDN-Magenta eine Liste mit den Positivschlüsseln bzw. Tagesschlüssel aller Nutzer ab, die in den letzten 14 Tagen ihr Testergebnis geteilt haben.

Bei einer erneuten, späteren Ermittlung werden nur die Positivschlüssel geladen, die noch nicht in die Bewertung des Ansteckungsrisikos eingeflossen sind. Um dies zu ermöglichen, wird das Datum des letzten Downloads der Liste in der CWA App gespeichert.

Zusätzlich werden die BWE von dem CDN-Magenta geladen.

Sowohl die Liste mit den Positivschlüsseln als auch die BWE werden über eine verschlüsselte Verbindung geladen.

Die geladenen Daten werden durch den CDN-Magenta signiert. Die Signatur wird nach jedem Laden in der CWA App auf Echtheit geprüft.

8.5.1.3 Schritt 3: Matching der Positivschlüssel mit RPIs

Das Matching der Positivschlüssel mit den protokollierten RPIs findet unter folgenden Voraussetzungen statt:

- Der Nutzer hat die Funktion „Risiko-Ermittlung“ aktiviert
- Der Nutzer hat das Expositionsbenachrichtigungswerkzeug aktiviert

Die CWA App gibt die heruntergeladenen Positivschlüssel an das Expositionsbenachrichtigungswerkzeug weiter, welches diese mit den im Kontaktprotokoll gespeicherten RPIs abgleicht (Matching).

Anschließend löscht die CWA App die heruntergeladenen Positivschlüssel.

Wenn es keinen „Match“ gibt, teilt das Expositionsbenachrichtigungswerkzeug dies der CWA App mit. Die CWA App zeigt dem Nutzer in diesem Fall ein „niedriges Risiko“ an.

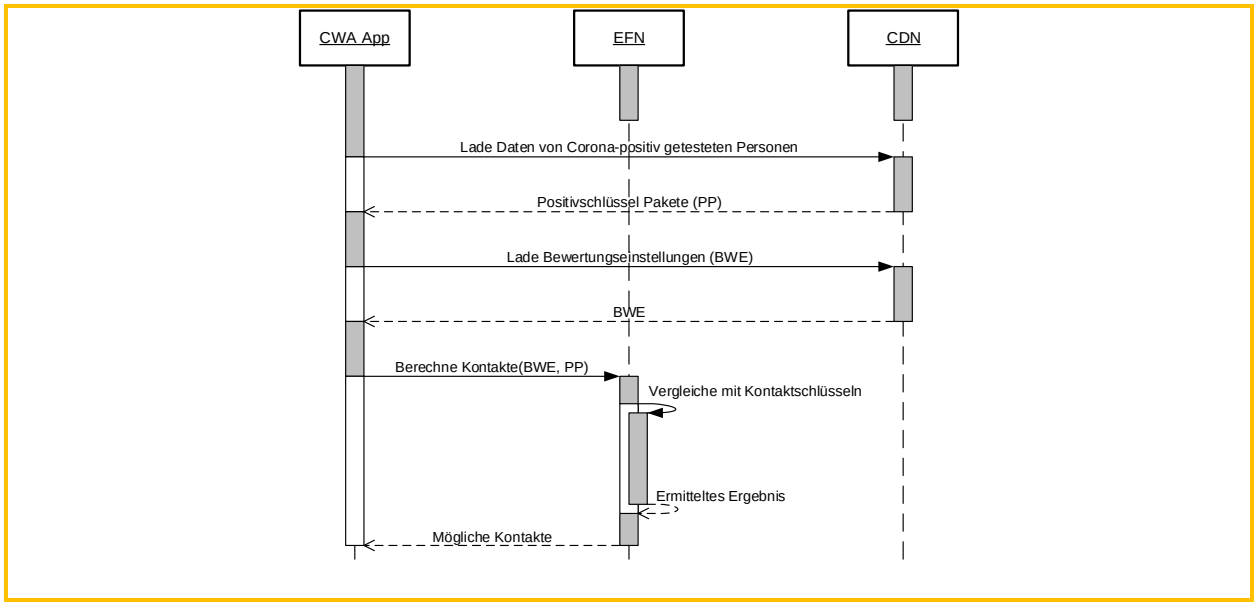


Abbildung 18: Laden der Positivschlüssel und Ermittlung möglicher Kontakte

8.5.2 Anwendungsphase 2: Kontaktfall

Wenn in Schritt 3 der Anwendungsphase 1 ein Match festgestellt wird, übergibt das Expositionsbenachrichtigungswerkzeug die zusammen mit den empfangenen RPIs im Kontaktprotokoll gespeicherten Angaben zur Kontaktdauer, das Datum und die Angabe, ob der Dämpfungswert (gemeldete Signalstärke) größer oder kleiner als 50db ist. Die betreffenden RPIs selbst werden nicht an die CWA App übergeben.

Diese Informationen werden unter Verwendung der BWE ausgewertet, um das Ansteckungsrisiko (Total Risk Score) für den Nutzer zu bewerten.

Für die Berechnung des Ansteckungsrisikos wird eine Summe aus einem Abstandsummanden, einem Faktor der vergangenen Zeit zum Kontakt, einem Faktor für die Dauer des Kontaktes und dem Übertragungs-Risiko-Faktor gebildet.

Der Abstandsfaktor wird wie folgt ermittelt:

Mit Hilfe des empfangenen Positivschlüssel und des daraus errechneten RPI werden die verschlüsselten Metadaten des empfangenen Bluetooth Signals entschlüsselt. Von der darin enthaltenen Sendesignalstärke wird die Empfangsstärke des Signals subtrahiert. Der sich ergebene Wert (Signaldämpfung) wird als Maß für die Entfernung betrachtet und als Abstandsfaktor verwendet.

TotalRiskScore = (attenuationLevelValue) * (daysSinceLastExposureLevelValue) * (durationLevelValue) * (transmissionRiskLevelValue)

Diese Berechnung des Ansteckungsrisikos findet lokal auf dem Smartphone statt, das heißt die Daten werden offline verarbeitet. Das ermittelte Infektionsrisiko wird ebenfalls ausschließlich in der CWA App gespeichert und an keine anderen Empfänger (auch nicht an das RKI, Apple, Google und sonstige Dritte) weitergegeben.

Die App zeigt dem Nutzer schließlich auf dem Home-Bildschirm der CWA App an, dass und welches Ansteckungsrisiko ermittelt worden ist. Zudem werden dem Nutzer Handlungsempfehlungen, basierend auf dem ermittelten Risikostatus, angezeigt.

8.5.3 Anwendungsphase 3: Test registrieren

Im Fall eines durchgeführten Tests auf eine Corona-Infektion kann der Nutzer über die CWA App den digitalen Testinformationsprozess starten und damit über das ermittelte Testergebnis durch die CWA App benachrichtigt werden. Dieser Test wird durch Ärzte oder Testzentren in Testlaboren durchgeführt. Von den Laboren werden die Testergebnisse auf einen zentralen Test Result Server übertragen und dort mittels eines dem Nutzer zur Verfügung gestellten QR-Code an diesen übermittelt, sofern er dem zugestimmt hat.

Die CWA App erlaubt es dem Nutzer, online das Ergebnis seines eigenen Corona-Tests abzufragen. Dazu erhält der Nutzer bei der Stelle, die den Test durchführt, z.B. beim Arzt, ein

Informationsblatt, auf dem dieses Verfahren beschrieben ist. Zu dem Informationsblatt erhält der Nutzer einen QR-Code, der mit Hilfe der CWA App eingescannt werden kann.

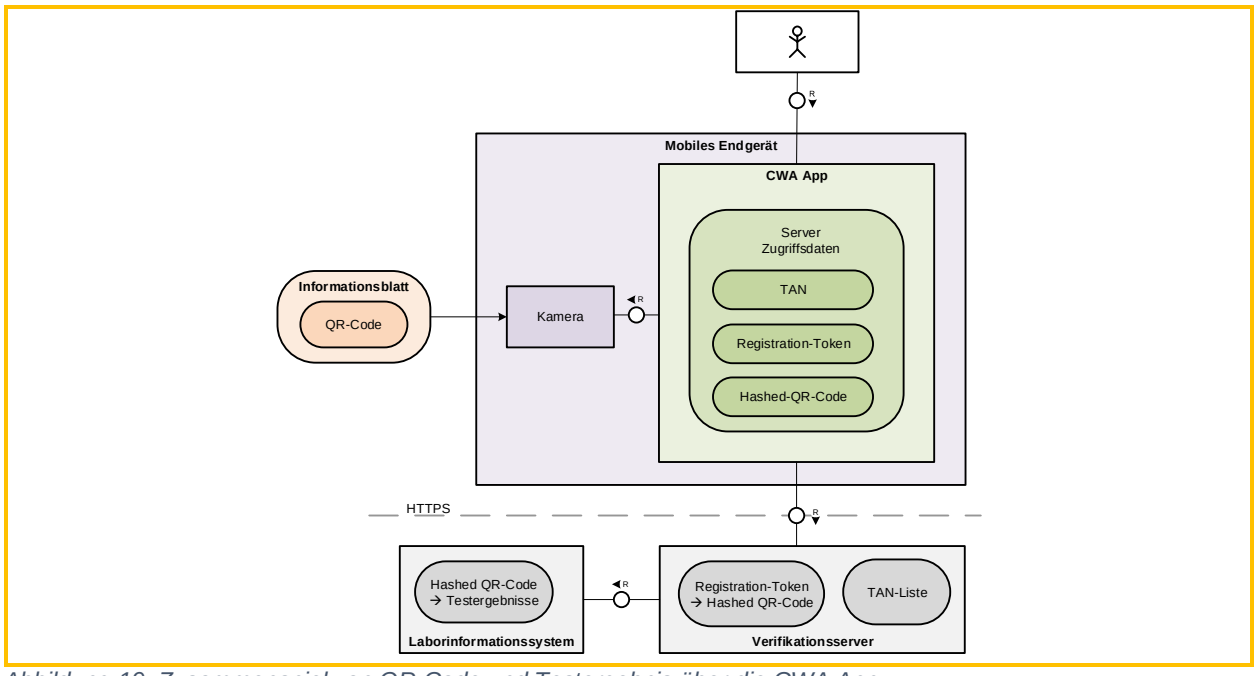


Abbildung 19: Zusammenspiel von QR-Code und Testergebnis über die CWA App

Vor dem Einscannen des QR-Codes willigt der Nutzer in die Datenverarbeitung in Zusammenhang mit dem Verfahren ein und registriert sich sodann, ohne Angabe der Person und rein unter Verwendung des QR-Codes, auf dem Verifikationsserver. Die CWA App bestimmt den Hash des QR-Codes und sendet den Hash an den Verifikationsserver. Zurück erhält die CWA App ein vom Verifikationsserver erzeugtes Registration Token, welches in der CWA App gespeichert wird. Jedes Mal, wenn der Nutzer sein Testergebnis abfragt, wird das Registration Token an den Verifikationsserver geschickt, welcher den Status des Ergebnisses ermittelt und an die CWA App zurückgibt. Der Verifikationsserver selbst ermittelt das Testergebnis durch Abfragen bei dem Test Result Server. Der Nutzer kann diesen Vorgang so oft wiederholen, bis ein endgültiges Ergebnis feststeht. Im Falle, dass das Ergebnis “positiv“ ist, kann eine TAN vom Verifikationsserver angefragt werden. Mit der Anfrage der TAN startet auch der Prozess die eigenen Eigenschlüssel anderen Nutzer zur Verfügung zu stellen. Im weiteren Verfahren können so andere Nutzer bezüglich potenzieller Kontakte mit dem Corona-positiv getesteten Nutzer gewarnt werden.

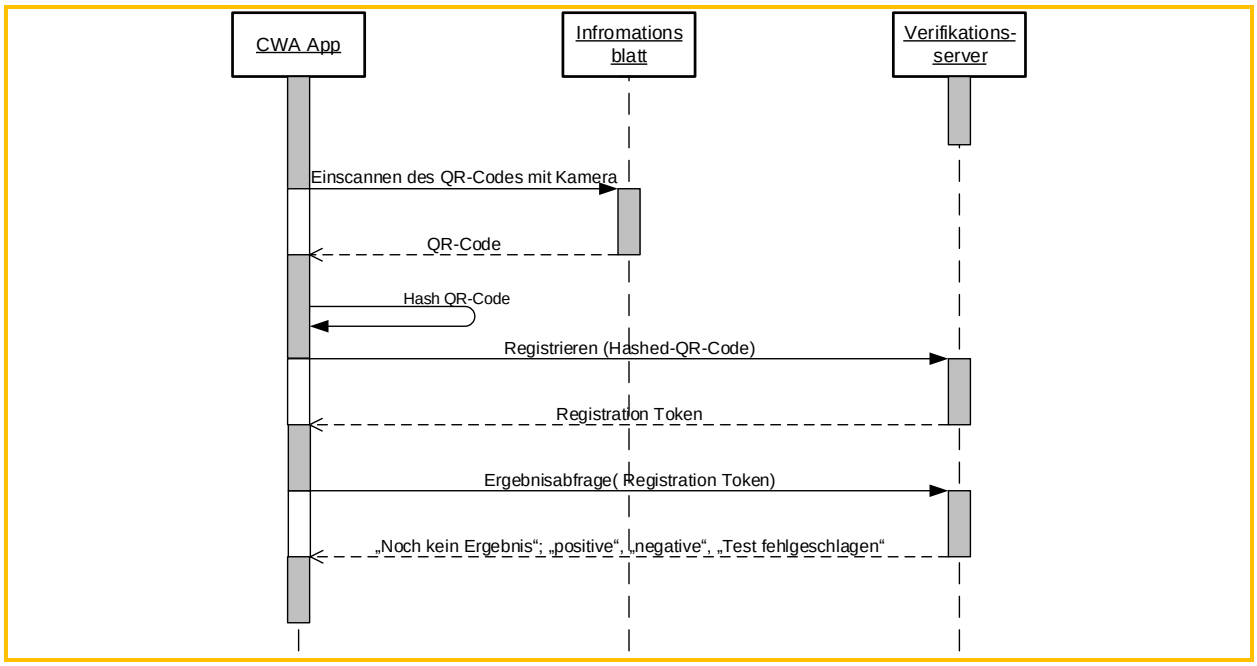


Abbildung 20: Einscannen des QR-Code, Registrierung und online Testergebnisabfrage

8.5.4 Anwendungsphase 3-4: Verifikationshotline

Die Verifikations-Hotline steht Benutzern der CWA App zur Verfügung, welche die Funktion der Kontaktverfolgung der CWA App genutzt haben, denen die Testergebnisabfrage jedoch nicht zur Verfügung steht. Die automatisierte Ergebnisabfrage ist nicht möglich, wenn kein QR-Code mit dem Testergebnis verknüpft ist. Das ist dann der Fall, wenn das Labor oder der testende Arzt nicht an die Systeme zur Bereitstellung der Testergebnisse angeschlossen, der QR-Code des Labors oder des Nutzers aufgrund von Beschädigungen nicht lesbar ist oder kein QR-Code an Labor oder Nutzer ausgegeben wurde.

Um die Gefahr der Verbreitung von falschen positiven Testergebnissen über die CWA App und die daraus folgenden falschen Empfehlungen für andere Nutzer zu verringern, werden dem anrufenden Nutzer durch einen Mitarbeiter der Verifikations-Hotline gemäß einem Skript Plausibilitätsfragen gestellt. Die Antworten der Nutzer werden nicht gespeichert. Wenn der Mitarbeiter der Verifikations-Hotline die Antworten für schlüssig hält und den Anrufer somit als einen infizierten Nutzer verifiziert, fragt er den Nutzer nach seiner Telefonnummer. Der Mitarbeiter notiert sich die Telefonnummer auf einem Zettel. Danach beendet er das Gespräch, um über ein Web-Interface bei dem Portalserver eine teleTAN abzufragen. Der Portalserver verbindet sich mit dem Verifikationsserver, der die teleTAN generiert. Der Hashwert der teleTAN wird auf dem Verifikationserver gespeichert, die teleTAN wird im Klartext an den Portal Server zurückgegeben und von dort über das Web-Interface dem Mitarbeiter der Verifikations-Hotline zur Verfügung gestellt. Die teleTAN wird dem infizierten Nutzer sodann im Rahmen eines Rückrufs mündlich mitgeteilt. Der Zettel mit der Rufnummer wird spätestens eine Stunde durch Vernichtung gelöscht.

Die teleTAN hat eine Gültigkeit von einer Stunde. Innerhalb dieses Zeitraums kann der infizierte Nutzer die teleTAN in der CWA App eingeben.

8.5.5 Anwendungsphase 4: Testergebnis teilen

Durch das teleTAN Verfahren oder durch den Erhalt eines Testergebnisses „positiv“ innerhalb der CWA App kann ein Nutzer die Einwilligung erteilen, seine Eigenschlüssel anderen Nutzern zur Verfügung zu stellen, um diese zu warnen. Technisch bedeutet dies, dass der Nutzer durch ein vorangestelltes Verfahren (teleTAN oder Abfrage über die CWA App) eine TAN erhalten darf. Der Nutzer gibt seine Einwilligung in dieses Verfahren beim zur Verfügung stellen der Eigenschlüssel.

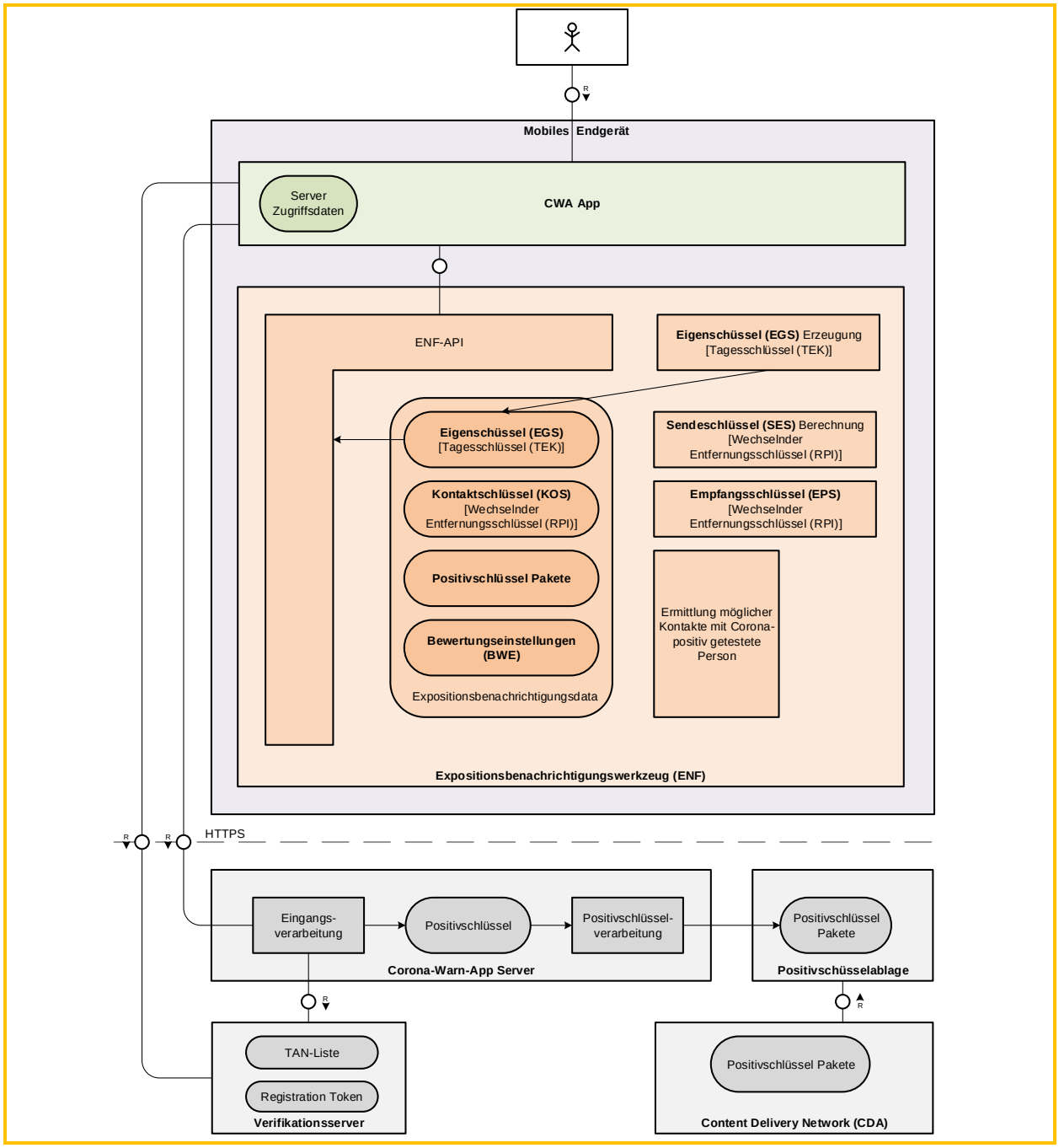


Abbildung 21: Die CWA App übergibt die TAN und die Eigenschlüssel an den CWA Server

Mit Anfrage der TAN durch die CWA App hat der Nutzer im vorangegangenen Verfahren zugestimmt, andere Personen mit Hilfe seiner Eigenschlüssel zu warnen. Die CWA App übergibt seine Eigenschlüssel, die nun Positivschlüssel genannt werden, zusammen mit der TAN an den CWA Server. Dieser überprüft die Gültigkeit der TAN mit Hilfe des Verifikationsservers und gibt dann die Verarbeitung der Positivschlüssel frei. Im weiteren Verfahren generiert der CWA Server aus vielen gesammelten Positivschlüsseln die Positivschlüssel Pakete und übergibt diese dem CDN.

Da Eigenschlüssel vom aktuellen Tag durch das Expositionsbenachrichtigungswerkzeug nicht freigegeben werden, wird der Eigenschlüssel von heute in einem separaten Schritt am nächsten Tag auf den CWA Server geladen.

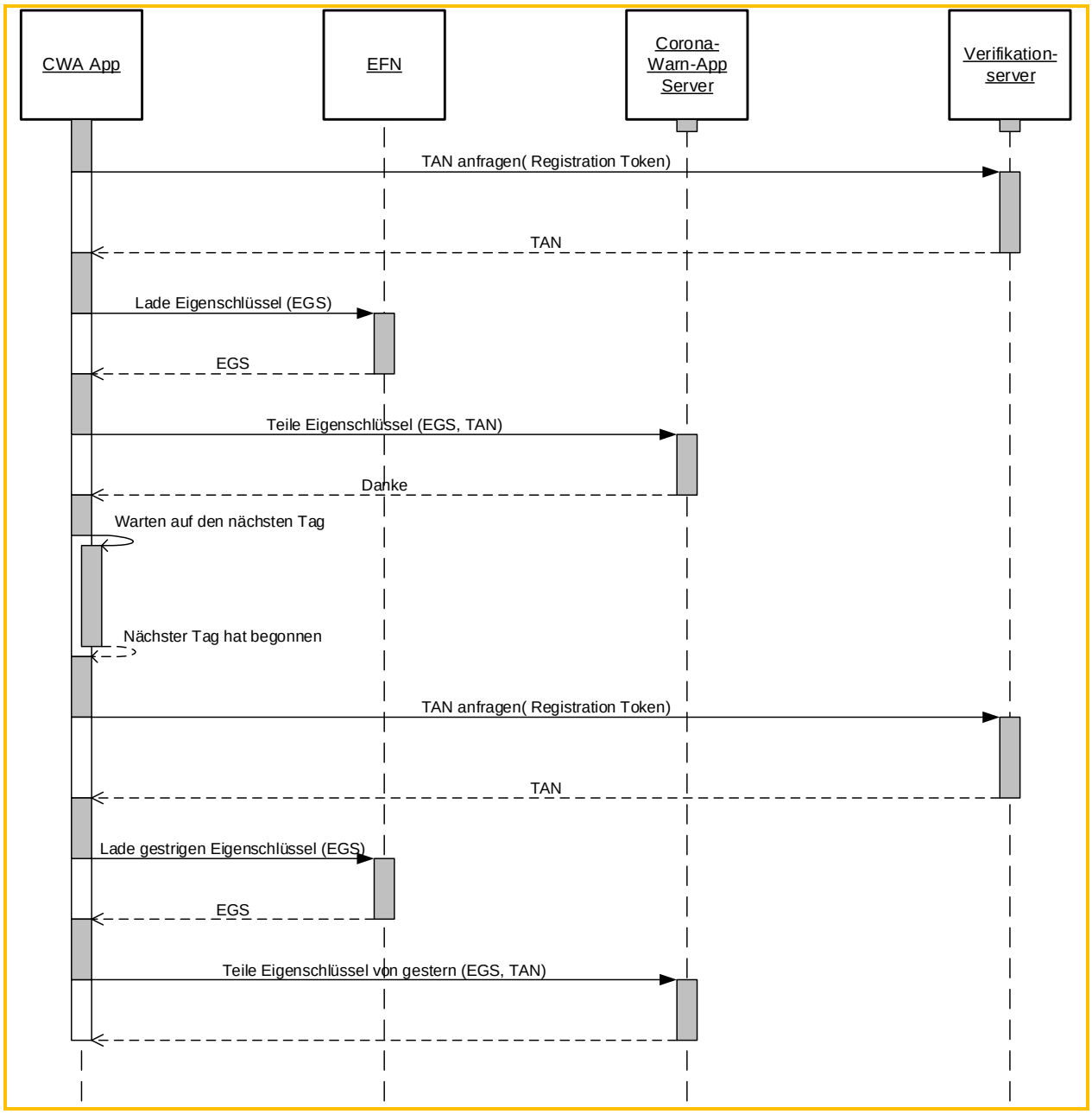


Abbildung 22: Ablauf beim Teilen der Eigenschlüssel durch hochladen auf den CWA Server

8.5.6 Deinstallation der CWA App

Der Nutzer deinstalliert die CWA App des mobilen Endgeräts. Dadurch werden sämtliche von der CWA App gespeicherten und verwalteten Daten vom Smartphone gelöscht.

Nicht gelöscht werden die Daten, die durch das Betriebssystem gespeichert und verwaltet werden. Dies sind der Verschlüsselungsschlüssel in der KeyChain sowie die Daten im Kontaktprotokoll des Expositionsbenachrichtigungswerkzeugs des jeweiligen Betriebssystems.

8.6 Kategorien von Daten

Daten aus den folgenden Kategorien werden im Rahmen der oben beschriebenen Anwendungsphasen und Prozesse verarbeitet:

- Zugriffsdaten (Anwendungsphasen 1, 3 und 4)
- Tagesschlüssel (Anwendungsphase 1 und 4)
- RPI (Anwendungsphasen 1 und 2)
- Metadaten zu RPIs (Anwendungsphasen 1 und 2)
- Positivschlüssel (Anwendungsphase 4)
- Bewertungseinstellungen (Anwendungsphase 1)
- TANs (Anwendungsphasen 3 und 4)
- Registration Token (Anwendungsphasen 3 und 4)
- QR-Code / GUID (Anwendungsphase 3)
- Risikowert (Anwendungsphase 1 und 2)
- Risikostatus (Anwendungsphasen 1 und 2)
- Name und Telefonnummer (Verifikations-Hotline) (Anwendungsphase 3-4)
- Antworten auf Plausibilitätsfragen (Verifikations-Hotline) (Anwendungsphase 3-4)

Die nachfolgenden Angaben beruhen auf den Datenfeldkatalogen des Rahmenkonzeptes und der Datenschutzkonzepte der einzelnen Komponenten.

8.6.1 Zugriffsdaten

Bei den HTTPS-Requests der CWA App auf den CWA-Server oder das CDN-Magenta fallen Zugriffsdaten an. Bei jedem Abruf von Daten vom Serversystem der CWA App wird die IP-Adresse (auf dem vorgelagerten Load Balancer) maskiert und im Weiteren nicht mehr

innerhalb des Serversystems der CWA App verarbeitet. Neben der IP-Adresse umfassen die Zugriffsdaten auch folgende Informationen:

- Datum und Uhrzeit des Abrufs (Zeitstempel)
- übertragene Datenmenge (bzw. Paketlänge)
- Meldung über erfolgreichen Abruf

8.6.2 Tagesschlüssel

Der Tagesschlüssel (Temporary Exposure Key, auch TEK oder Eigenschlüssel genannt) ist eine Datenstruktur. Es handelt sich um einen täglich neu zufällig generierten Wert, der lokal im ENF gespeichert und von diesem verwaltet wird. Nach Ablauf von 14 Tagen seit der Generierung wird ein Tagesschlüssel automatisch aus dem ENF gelöscht. Die CWA App kann nur im Rahmen der Funktion „Testergebnis teilen“ auf Tagesschlüssel (dann in der Rolle eines Positivschlüssels) zugreifen.

Der Tagesschlüssel dient als Initialwert für die Erzeugung von RPIs. Aus einem Tagesschlüssel können somit RPIs abgeleitet werden. Aus einem früheren Tagesschlüssel lassen sich jedoch keine später erzeugten Tagesschlüssel ableiten.

Bei Kenntnis des Tagesschlüssel und einer (daraus abgeleiteten) RPI können spätere (aus dem gleichen Tagesschlüssel abgeleitete) RPIs abgeleitet werden.

Ein Tagesschlüssel besteht aus vier Datenfeldern:

TransmissionRiskLevel

Dieses Datenfeld hat einen Wert zwischen 0 und 8 und bezeichnet die Höhe des Übertragungsrisiko für Kontakte des Nutzers. So kann berücksichtigt werden, dass beispielsweise ein Nutzer, der einen Test durchgeführt hat oder positiv auf eine Infektion getestet worden ist, in der Regel ein größeres Ansteckungsrisiko für seine Kontakte darstellt als ein Nutzer, der gerade einen negativen Befund erhalten hat.[7]

RollingPeriod

Dieses Datenfeld gibt die Anzahl der zeitlichen Intervalle an, zu denen der Schlüssel gültig war (ein Zeitraum entspricht 10 Minuten). Daraus kann abgeleitet werden, bis wann der Tagesschlüssel für die Erzeugung von RPIs verwendet worden ist.

---

[7] https://static.googleusercontent.com/media/www.google.com/de//covid19/exposurenotifications/pdfs/Android-Exposure-Notification-API-documentation-v1.3.2.pdf, S. 7.

RollingStartNumber

Dieses Datenfeld gibt den Zeitpunkt der ersten Benutzung des Tagesschlüssel an.

KeyData

Dieses Datenfeld enthält den eigentlichen Schlüssel, auf welchen sich die drei anderen Datenfelder beziehen.

8.6.3 RPI

Die eigene RPI (Rolling Proximity Identifier) des Nutzers wird vom ENF aus dem aktuell gültigen Tagesschlüssel abgeleitet und alle 10 bis 20 Minuten ausgetauscht. Nach Ablauf von 14 Tagen seit der Generierung wird eine RPI automatisch aus dem Kontaktprotokoll des ENF gelöscht.

Bei Kenntnis des Tagesschlüssels, aus dem eine RPI abgeleitet worden ist, können die später aus derselben Tagesschlüssel abgeleiteten RPIs berechnet werden. Ohne Kenntnis der zugrundeliegenden Tagesschlüssel kann aus einer RPI weder auf die Tagesschlüssel noch auf andere RPIs geschlossen werden.

Die eigenen RPIs des Nutzers werden vom ENF verwaltet und sind nur diesem bekannt. Die empfangenen RPIs anderer Nutzer werden im Kontaktprotokoll des ENF gespeichert und dort nach 14 Tagen gelöscht.

Die CWA App hat zu keinem Zeitpunkt Zugriff auf eigene oder fremde RPIs.

8.6.4 Metadaten zu fremden RPIs

Die vom ENF aufgezeichneten RPIs anderer Nutzer werden zusammen mit den folgenden Metadaten im Kontaktprotokoll des ENF gespeichert:

- Datum des Kontakts
- Dämpfungswert (gemeldete Signalstärke - gemessene RSSI)
- Dämpfungsbehälter (enthält z. B. die Angabe, ob Signalstärke <=50 dB oder >50 dB; es wird davon ausgegangen, dass eine Dämpfung von kleiner als 50 dB auf den epidemiologisch relevanten Abstand von unter zwei Metern schließen lässt)
- Dauer der Begegnung mit der infizierten Person (exposure) in 5er Schritten (<5/5/10/15/20/25/30/>30 Minuten)

Im Kontaktfall übergibt das ENF diese Metadaten an die CWA App, die unter Verwendung dieser Daten dann den Total Risk Score hinsichtlich dieses Kontakts berechnet.

8.6.5 Positivschlüssel

Ein Positivschlüssel ist ein “umgewidmeter” Tagesschlüssel eines Nutzers, der in der CWA App sein Testergebnis geteilt hat. Wenn ein Nutzer sein Testergebnis teilt, werden alle im ENF gespeicherten Tagesschlüssel (der letzten 14 Tage) an die CWA App übergeben und von dieser dann gebündelt an den CWA Server gesendet.

8.6.6 Bewertungseinstellungen (BWE)

Die BWE (Exposure Parameter Configuration) sind eine komplexe Datenstruktur. Diese Datenstruktur beinhaltet die Konfigurationseinstellung für die Analyse und die Risikobewertung der Kontakte, deren Ergebnis der Total Risk Score ist. Der BWE wird vom RKI verwaltet. Es können auf diese Weise neuste epidemiologische Erkenntnisse in die Risikoermittlung einfließen.

Die BWE bestehen aus vier Parameterkategorien:

Transmission Risk: Dieser Wert stellt das Übertragungsrisiko da. Er wird vom RKI vorgegeben. Es fließen hier epidemiologische Erkenntnisse über Symptomstärke, Symptomstartpunkt oder den Testzeitpunkt ein.

Duration Risk: Dieser Wert ist abhängig der summierten Aufenthaltszeit am Kontakt.

Days Risk: Dieser Wert reflektiert den zeitlichen Abstand seit dem Kontakt in Tagen.

Attenuation Risk: Dieser Risikowert ist abhängig vom Abstand zum Kontakt.

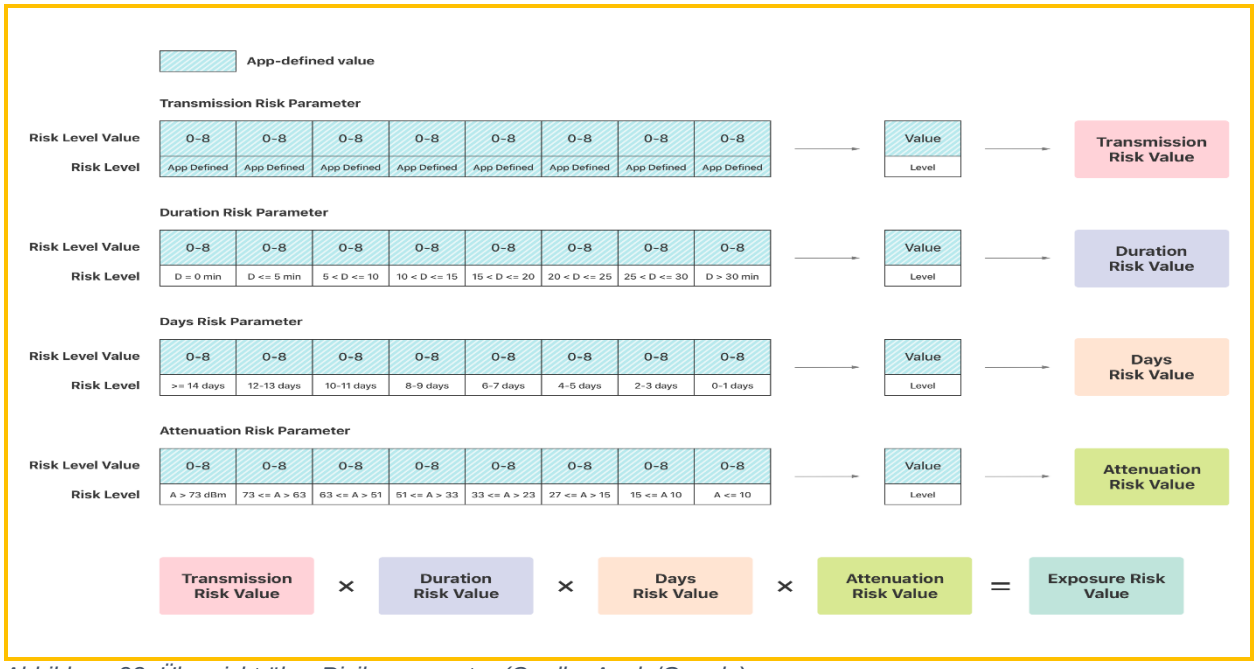


Abbildung 23: Übersicht über Risikoparameter (Quelle: Apple/Google)

8.6.7 TANs

Die TAN ist eine einmal verwendbare Transaktionsnummer, die beim Abruf des Testergebnisses automatisch generiert und dann in der CWA App abgelegt wird. Nach der Einwilligung des Nutzers in das Teilen seines Testergebnisses werden die TAN und die Tagesschlüssel der letzten 14 Tage an den CWA Server übermittelt. Dieser überprüft die Gültigkeit der TAN mit Hilfe des Verifikationsservers und gibt dann die Verarbeitung der Positivschlüssel frei.

8.6.8 Registration Token

Der Registration Token wird nach Auslesen der in einem QR-Code enthaltenen GUID vom Verifikationsserver erstellt und an die CWA App übermittelt. Der Registration Token erschwert als zusätzlicher Schritt eine Identifizierung des Nutzers durch natürliche Personen und ermöglicht gleichzeitig die technische Zuordenbarkeit zur Kommunikation mit dem Verifikationsserver, um ein Testergebnis abzufragen.

8.6.9 QR-Code / GUID

Der QR-Code wird einer Person bei Durchführung eines Corona Tests mit Abnahme der Probe auf einem Probenbegleitschein aufgedruckt übergeben. Er dient der Kennung für einen Corona Test. Der QR-Code enthält eine GUID, welche der Nutzer mit seiner CWA App über die Kamerafunktion seines Smartphones scannen kann. Die CWA App übermittelt dann einen Hashwert der GUID an den Verifikationsserver und erhält dafür vom Server einen Registration Token, der für die Abfrage des Testergebnisses notwendig ist.

8.6.10 Risikowert (Total Risk Score)

Der Risikowert gibt die Höhe des Ansteckungsrisikos des Nutzers in Bezug auf einen Kontakt (exposure) an einem Tag an. Der Risikowert berücksichtigt daher auch mehrere Kontakte an einem Tag mit der gleichen Person.

Sofern es im Rahmen der Anwendungsphase 1 einen Match gibt, übergibt das EFN die im Kontaktprotokoll gespeicherten Angaben zur Kontaktdauer, das Datum und die Angabe, ob der Dämpfungswert (gemeldete Signalstärke) größer oder kleiner als 50db ist, an die CWA App. Die zugehörigen RPIs werden nicht an die CWA App übergeben.

Diese Informationen werden unter Verwendung der aktuellen BWE ausgewertet, um das Infektionsrisiko (Total Risk Score) für den Nutzer zu bewerten. Dabei kommt folgende Formel zur Anwendung:

Für die Berechnung des Total Risk Score wird eine Summe aus einem Abstandsummanden, einem Faktor der vergangenen Zeit zum Kontakt, einem Faktor der Dauer des Kontaktes und dem Übertragungs-Risiko-Faktor gebildet.

Der Abstandsfaktor wird wie folgt ermittelt:

Mit Hilfe des empfangenen Positivschlüssel und des daraus errechneten RPI werden die verschlüsselten Metadaten des empfangenen Bluetooth Signals entschlüsselt. Von der darin enthaltenen Sendesignalstärke wird die Empfangsstärke des Signals subtrahiert. Der sich ergebene Wert (Signaldämpfung) wird als Maß für die Entfernung betrachtet und als Abstandsfaktor verwendet.

TotalRiskScore = (attenuationLevelValue) * (daysSinceLastExposureLevelValue) * (durationLevelValue) * (transmissionRiskLevelValue)

Diese Berechnung des Total Risk Score findet lokal auf dem Smartphone statt, das heißt die Daten werden offline verarbeitet. Das ermittelte Infektionsrisiko wird ebenfalls ausschließlich in der CWA App gespeichert und an keine anderen Empfänger (auch nicht an das RKI, Apple, Google und sonstige Dritte) weitergegeben.

Die App zeigt dem Nutzer schließlich auf dem Homescreen der CWA App an, dass und welches Infektionsrisiko ermittelt worden ist. Zudem werden dem Nutzer Handlungsempfehlungen, basierend auf dem ermittelten Infektionsrisiko, angezeigt.

Bei einer erneuten, späteren Ermittlung des Ansteckungsrisikos werden nur die aktuellen Diagnoseschlüssel vom CDN geladen, die noch nicht in alte Bewertungen eingeflossen sind. Um das zu gewährleisten, wird das Datum des letzten Downloads in der CWA gespeichert.

8.6.11 Risikostatus

Der Risikostatus wird von der Risiko-Ermittlung berechnet und erlaubt es dem RKI, dem Nutzer entsprechend der vermittelten Risikostufe Informationen und Handlungsempfehlungen zu geben. Der Risikostatus wird in drei Stufen angegeben:

- Unbekanntes Risiko
- Niedriges Risiko
- Erhöhtes Risiko

8.6.12 Name und Telefonnummer (Verifikations-Hotline)

Im Rahmen der Verifikations-Hotline werden Telefonnummer und ggfs. Name des anrufenden Benutzers erfragt und notiert. Die Zettel, auf denen Name und Telefonnummer notiert sind, werden regelmäßig, das heißt spätestens nach einer Stunde, durch Vernichtung im Reißwolf gelöscht.

8.6.13 Antworten auf Plausibilitätsfragen (Verifikations-Hotline)

Im Rahmen der Verifikations-Hotline stellen Mitarbeiter den Anrufern Plausibilisierungsfragen, um die Gefahr eines Missbrauchs der CWA App zu verringern. Wenn der Mitarbeiter die Antworten für plausibel hält, ruft er den Anrufer unter der angegebenen Telefonnummer zurück und teilt dem Anrufer eine teleTAN mit.

8.7 Löschung der Daten

Alle in der CWA gespeicherten Daten werden gelöscht, sobald sie für die Funktionen der CWA nicht mehr benötigt werden:

8.7.1 Löschung der Daten der Anwendungsphase 1: Risiko-Ermittlung und Anwendungsphase 2: Kontaktfall

Die Löschung der im Rahmen der Anwendungsphasen 1 und 2 durch die CWA App verarbeiteten Datenkategorien richtet sich nach den Angaben in der Datenschutzerklärung der CWA App nach nachfolgend genannten Fristen, wobei aus Gründen der Einfachsprachlichkeit teilweise “untechnische” oder zusammenfassende Kategorienbezeichnungen verwendet werden:

“Die Liste der Zufalls-IDs [Positivschlüssel, Anm. d. Autoren] von Nutzern, die ein positives Testergebnis geteilt haben, wird in der App unverzüglich und im Übrigen im Kontaktprotokoll des Smartphones nach 14 Tagen automatisch gelöscht.

Auf die Löschung der Begegnungsdaten [Metadaten zu fremden RPIs, Anm. d. Autoren] im Kontaktprotokoll Ihres Smartphones (einschließlich Ihrer eigenen Zufalls-IDs [Eigenschlüssel, Anm. d. Autoren]) und die Begegnungsdaten auf anderen Smartphones [RPIs und Metadaten des Nutzers, Anm. d. Autoren] hat das RKI keinen Einfluss, da diese Funktion von Apple bzw. Google bereitgestellt werden. Die Löschung richtet sich nach den Festlegungen von Apple bzw. Google. Zurzeit werden die Daten nach 14 Tagen automatisch gelöscht. Zudem können Sie im Rahmen der von Apple und Google bereitgestellten Funktionalitäten in den Systemeinstellungen Ihres Geräts gegebenenfalls eine manuelle Löschung anstoßen.

Der in der App angezeigte Risikowert [Risikostatus, Anm. d. Autoren] wird gelöscht, sobald ein neuer Risikowert ermittelt worden ist. Ein neuer Risikowert wird in der Regel ermittelt, nachdem die App eine neue Liste mit Zufalls-IDs [Positivschlüsseln, Anm. d. Autoren] erhalten hat.”

8.7.2 Löschung der Daten der Anwendungsphase 3: Test registrieren

Die Löschung der im Rahmen der Anwendungsphase 3 durch die CWA App verarbeiteten Datenkategorien richtet sich nach den Angaben in der Datenschutzerklärung der CWA App nach folgenden genannten Fristen, wobei auch hier aus Gründen der Einfachsprachlichkeit abweichende Kategorienbezeichnungen verwendet werden:

“Die gehashte Kennzahl [GUID, Anm. d. Autoren] wird auf dem Serversystem der CWA App nach 21 Tagen gelöscht.

Die gehashte Kennzahl und das Testergebnis in der Testergebnis-Datenbank [Test Result Server, Anm. d. Autoren] werden im Fall eines negativen Testergebnisses unmittelbar nach dem Abruf des Testergebnisses und im Fall eines positiven Testergebnissen unmittelbar nach dem Löschen der auf Serversystem gespeicherten Kopie der TAN gelöscht (s.u.).

Das Token, das auf dem Serversystem gespeichert ist [Kopie des Registration Token, Anm. d. Autoren], wird nach 21 Tagen gelöscht.

Das Token, das in der CWA App gespeichert ist [Registration Token, Anm. d. Autoren], wird nach Löschung der CWA App vom Smartphone oder nach Ausführung der Funktion ‘Testergebnis teilen’ gelöscht.”

8.7.3 Löschung der Daten der Anwendungsphase 4: Testergebnis teilen

Die Löschung der im Rahmen der Anwendungsphase 4 durch die CWA App verarbeiteten Datenkategorien richtet sich nach den Angaben in der Datenschutzerklärung der CWA App nach nachfolgend genannten Fristen, wobei auch hier aus Gründen der Einfachsprachlichkeit abweichende Kategorienbezeichnungen verwendet werden:

“Die in der App geteilten eigenen Zufalls IDs [Positivschlüssel, Anm. d. Autoren] werden nach 14 Tagen vom Serversystem gelöscht.

Die Kopie der TAN, die auf dem Serversystem gespeichert ist, wird nach 21 Tagen gelöscht.

Die TAN, die in der App gespeichert ist, wird nach Teilen des Testergebnisses gelöscht.

Die TeleTAN, die in der App gespeichert ist, wird nach Teilen des Testergebnisses gelöscht.

Die TeleTAN, die auf dem Serversystem gespeichert ist, wird nach 21 Tagen gelöscht.

Die TeleTAN, die dem Mitarbeiter der Hotline übermittelt wird, wird dort direkt nach der telefonischen Weitergabe an Sie gelöscht.

Das Token, das auf dem Serversystem gespeichert ist [Kopie des Registration Token, Anm. d. Autoren], wird nach 21 Tagen gelöscht.

Das Token, das in der App gespeichert ist [Registration Token, Anm. d. Autoren], wird nach Teilen des Testergebnisses gelöscht.”

8.7.4 Löschung der Zugriffsdaten

Zur Löschung von Zugriffsdaten siehe unter Ziffer 10.1.1.

8.8 An der Datenverarbeitung beteiligte Akteure

Nachfolgend werden die Akteure beschrieben und datenschutzrechtlich eingeordnet, die unmittelbar Einfluss auf die Verarbeitung personenbezogener Daten im Rahmen der CWA nehmen können.

8.8.1 Betroffene Personen

Betroffene Personen der Datenverarbeitung im Rahmen der CWA sind die Nutzer der CWA App.

8.8.2 Verantwortlicher

Das RKI ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO für die mit dem Betrieb der CWA einhergehende Verarbeitung von personenbezogenen Daten der Nutzer.

8.8.3 Mögliche weitere Verantwortliche

Soweit personenbezogenen Daten nur lokal auf dem Smartphone oder nur im P2P-Verfahren zwischen zwei Smartphones verarbeitet werden, kommen als weitere eigenständige Verantwortliche oder zumindest faktische “Datenherren” zum einen die Unternehmen Apple und Google als Anbieter des NF sowie zum anderen die Nutzer der CWA App in Betracht. Eine gemeinsame Mittel- und Zweckfestlegung im Sinne von Art. 26 DSGVO durch diese Stellen (soweit diese als Verantwortliche anzusehen sind) und das RKI ist derzeit nicht ersichtlich, sollte jedoch fortlaufend kritisch geprüft werden.

Für eine eigene Verantwortlichkeit von Apple und Google spricht, 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. Soweit es sich für Google und Apple um die durch das ENF verarbeiteten Daten um

personenbezogene Daten handelt, können sie als die für die Verarbeitung (gemeinsame) Verantwortliche angesehen werden.[8]

Auch der Nutzer selbst hat es in der Hand, ob und wie lange seine personenbezogenen Daten und die von anderen Nutzern der CWA App lokal auf seinem Smartphone verarbeitet werden. Insbesondere kann der Nutzer einen wesentlichen Teil der Datenverarbeitung jederzeit beenden, etwa durch Deaktivierung des ENF oder die Deinstallation der CWA App. In letzterem Fall wäre die Herstellung eines Personenbezugs von bisher übermittelten eigenen Daten für das RKI, Apple, Google oder andere Nutzer nicht mehr möglich.

8.8.4 Auftragsverarbeiter

Das RKI bedient sich für den Betrieb eines Teils der CWA nachfolgender Dienstleister, die personenbezogene Daten der Nutzer im Auftrag des RKI verarbeiten. Die Datenverarbeitung durch diese Dienstleister erfolgt jeweils auf Grundlage eines schriftlichen Auftragsverarbeitungsvertrags nach Art. 28 Abs. 3 DSGVO.

8.8.4.1 SAP Deutschland SE & Co. KG

Die SAP Deutschland SE & Co. KG (im Folgenden „SAP“) hat im Auftrag der Bundesregierung zusammen mit der T-Systems International GmbH die CWA entwickelt. Im Rahmen des laufenden Betriebs übernimmt SAP notwendige Leistungen zur Weiterentwicklung der CWA App sowie Support- und Pflegeleistungen (sogenannter 3rd-Level-Support). Davon umfasst sind insbesondere Leistungen zur Fehlerbehebung innerhalb der CWA App, Funktionsverbesserungen, Codeänderungen und -optimierungen, Stabilisierungsmaßnahmen und Migrationen. Personenbezogene Daten von Nutzern der CWA App werden dabei im Regelfall nicht verarbeitet, eine Zugriffsmöglichkeit kann im Rahmen des zu leistenden Supports aber auch nicht gänzlich ausgeschlossen werden.

8.8.4.2 T-Systems International GmbH

Die T-Systems International GmbH (im Folgenden „T-Systems) hat zusammen mit SAP die CWA entwickelt. T-Systems übernimmt den Applikationsbetrieb als Auftragsverarbeiter, wobei die CWA App in Containern in Kubernetes-Clustern der Open Telekom Cloud (OTC) läuft. In diesem Zusammenhang verarbeitet T-Systems die über die CWA App erzeugten technischen Zugriffsdaten sowie die über den Portalserver und die über die Schnittstelle zu den Laboren (Lab Server) sowie das Content Delivery Network (CDN-Magenta) erzeugten Daten. Außerdem ist T-Systems für den sogenannten 1st- und 2nd-Level-Support zuständig. Hierzu

[8] In diese Richtung auch die *Artikel-29-Datenschutzgruppe*, Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten, S. 14.

gehören insbesondere die Anwendungsüberwachung, die Ticketerstellung, Problemlösung, die Ursachenanalyse und Problembehandlung sowie der Betrieb und die Verwaltung der technischen Infrastruktur. Schließlich ist T-Systems für die technische Hotline und die Verifikationshotline zuständig, bei der gegebenenfalls nach erfolgter Verifikation von Anrufern eine teleTAN generiert und übermittelt wird.

T-Systems unterhält mit schriftlicher Genehmigung des RKI (Art. 28 Abs. 2 S.1 DSGVO) Unterauftragsverhältnisse mit folgenden Dienstleistern, die ebenfalls mit personenbezogenen Daten der Nutzer in Berührung kommen können:

- Deutsche Telekom Regional Solutions & Products GmbH (1st & 1,5 Level Support für OTC)
- IT Services Hungary (Operation, 1st and 2nd Level Support für OTC)
- Deutsche Telekom IT GmbH (User support MyWorkplace für OTC)
- Axivas Deutschland GmbH (Service Desk für OTC)
- Deutsche Telekom Individual Solutions & Products GmbH (DC Hardware disposal and replace für OTC)
- Axivas Deutschland GmbH (Call-center Leistung für Hotline)
- Deutsche Telekom Technik GmbH (für das Content Delivery Network (CDN) über das der Gemeinschaft die Positivschlüssel zum Download zur Verfügung gestellt werden).

8.9 Begleitdokumente zur Beschreibung der geplanten Verarbeitungsvorgänge (Prüfgegenstand)

Die folgenden Begleitdokumente enthalten weitergehende Beschreibungen des Prüfgegenstands in sachlicher Hinsicht und sind insoweit Bestandteile dieses DSFA-Berichts. Etwaige rechtliche Wertungen in den Begleitdokumenten sind nicht Bestandteil dieses DSFA-Berichts.

Nr.	Bezeichnung des Dokuments	Stand/ Version
1	Datenschutzkonzept der CWA der Bundesrepublik Deutschland (Rahmendokument)	1.1
2	Datenschutzkonzept der CWA der Bundesrepublik Deutschland – Verifikation und Testergebnis	1.1
3	Datenschutzkonzept der CWA der Bundesrepublik Deutschland – CWA App	1.1
4	Datenschutzkonzept der CWA der Bundesrepublik Deutschland – CWA Server	1.1
5	Datenschutzkonzept der CWA der Bundesrepublik Deutschland - Verifikations-Hotline	1.1
6	Designentscheidungen der CWA der Bundesrepublik Deutschland	1.2
7	Technisch-Organisatorische Maßnahmen	1.1

9 Einholung des Standpunktes der betroffenen Personen

Gemäß Art. 35 Abs. 9 DSGVO kann der Verantwortliche die Standpunkte der betroffenen Personen einholen, um deren Sichtweisen in Erfahrung zu bringen und somit möglicher Kritik frühzeitig zu begegnen und dadurch die Akzeptanz des geplanten Verfahrens zu fördern zu.

Da die betroffenen Personen alle potenziellen Nutzer der CWA App sind und daher ein sehr breites Spektrum der Bevölkerung umfassen, wurden die Standpunkte der betroffenen Personen durch die Auswertung verschiedener Quellen eingeholt:

- Individuelles und öffentliches Feedback auf die Veröffentlichung von Quellcodes und Dokumenten (Datenschutzkonzepte usw.) auf der GitHub-Projektseite,
- Medienberichterstattung über die CWA,
- Fachveröffentlichungen,
- Stellungnahmen von Datenschutzbehörden und Datenschutzgremien (z. B. Europäischer Datenschutzausschuss)[9] und
- Stellungnahmen von Verbänden und Interessensgruppen[10].

Den geäußerten Standpunkten wurde bei der Entwicklung der CWA, soweit aus Sicht der Stakeholder zweckmäßig und möglich, Rechnung getragen.

10 Datenschutzrechtliche Bewertung

Nachfolgend werden einzelne Aspekte der Verarbeitungsvorgänge im Rahmen der CWA aus datenschutzrechtlicher Sicht bewertet, sodass die datenschutzrechtlichen Anforderungen identifiziert sowie die geplanten Maßnahmen und Ergebnisse der Risikoanalyse einer datenschutzrechtlichen Beurteilung zugänglich gemacht werden können.

[9] EDSA, Guidelines 04/2020 on the use of location data and contacttracing tools in the context of the COVID-19 outbreak, European Data Protection Board (abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf, zuletzt abgerufen am 14.06.2020).

[10] Offener Brief des Chaos Computer Clubs (CCC) vom 24.04.2020 an Bundesminister Spahn, abrufbar unter https://www.ccc.de/system/uploads/300/original/Offener_Brief_Corona_App_BMG.pdf (abgerufen am 14.06.2020); Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), Datenschutz-Folgenabschätzung für die Corona App, Version 1.6, abrufbar unter: https://www.fiff.de/dsfa-corona.

10.1 Kategorien von personenbezogenen Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Dass im Rahmen der CWA personenbezogene Daten durch das RKI als Verantwortlichen verarbeitet werden, steht außer Frage. Die Frage, in welchem konkreten Umfang personenbezogene Daten der Nutzer durch das RKI verarbeitet werden, ist hingegen schwierig zu beantworten. Denn ein Teil der Datenverarbeitung findet nur lokal bzw. „offline" auf dem Smartphone des Nutzers statt und dies teilweise auch nur innerhalb des ENF, also außerhalb der CWA App.

10.1.1 Personenbezogene Daten

Nachfolgend wird angenommen, dass personenbezogene Daten durch das RKI in folgenden Fällen verarbeitet werden:

- In Form von **Zugriffsdaten** beim Download von Positivschlüsseln und BWE (Anwendungsphase 1), bei der Testregistrierung (Anwendungsphase 3) und beim Teilen eines Testergebnisses (Anwendungsphase 4),
- In Form von **Positivschlüsseln** und eindeutigen Kennungen (**Registration Token**, **TAN**) beim Teilen eines Testergebnisses (Anwendungsphase 4) und
- In Form eindeutiger Kennungen (**GUID**) beim Registrieren eines Tests,

jedoch jeweils nur solange, wie die vom Nutzer für die Übermittlung dieser Daten verwendete IP-Adresse auf dem CWA Server bzw. CDN-Magenta gespeichert ist.

Unabhängig davon, ob es sich bei den Positivschlüsseln und anderen eindeutigen Kennungen und Informationen (auch in Form von einzelnen Zugriffsdaten) für das RKI für sich genommen um personenbezogene Daten des Nutzers handelt, folgt der Personenbezug dieser Daten jedenfalls aus ihrer – wenn auch nur kurzzeitigen – Verbindung mit der IP-Adresse, die für die Übermittlung dieser Daten an das RKI verwendet wird. Denn bei IP-Adressen handelt es für den Anbieter eines Online-Dienstes um ein personenbezogenes Datum, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, mit Hilfe der zuständigen Behörde und dem Internetzugangsanbieter, die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen.[11] Das RKI hat die rechtliche Möglichkeit, sich beispielsweise im Fall von Cyberattacken an die zuständige Behörde zu wenden, um die fraglichen Informationen zu erlangen bzw. die Strafverfolgung einzuleiten und infolge auch die an sich anonymen Daten dem Verwender der IP-Adresse zuzuordnen. 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.

[11] EuGH, Urteil vom 19.10.2016 – C-582/14 (Breyer/Deutschland).

Da 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, besteht der oben beschriebene Personenbezug in Verbindung mit einer IP-Adresse für das RKI jedoch nur für eine „technische Sekunde“.

10.1.2 Lokale Datenverarbeitung auf dem Smartphone

Der Austausch von RPIs zwischen Smartphones per BLE, die Kontaktprotokollierung im Kontaktprotokoll, die Erzeugung von Tagesschlüsseln und RPIs sowie die Ermittlung des Risikos für den Nutzer finden nur lokal bzw. „offline“ auf dem Smartphone, d. h. ohne die unmittelbare Mitwirkung oder Kenntnis des RKI statt.

Der konkrete Ablauf dieser lokalen Datenverarbeitung liegt außerhalb des faktischen Einflussbereichs des RKI. Dies gilt sowohl für die von der CWA App auf technischer Ebene selbst verarbeiteten Daten als auch für die betriebssystemseitige Datenverarbeitung „hinter“ der Schnittstelle des ENF.

Die unmittelbarsten Einflussmöglichkeit hinsichtlich des Ablaufs der lokalen Datenverarbeitung durch die CWA App und das ENF haben einerseits der Nutzer, etwa durch die Änderung von Systemeinstellungen des Smartphones oder das manuelle Löschen des Kontaktprotokolls, und andererseits Apple bzw. Google, die als Hersteller des Betriebssystems die Möglichkeit zur nachträglichen Änderung des ENF haben und insoweit auf technischer Ebene prinzipiell auch zur Verknüpfung der dort verarbeiteten Tagesschlüssel und RPIs mit einer geräte- (z. B. Werbe-ID) oder nutzerspezifischen Kennung (z. B. Apple-ID oder Google-Konto) haben. Da die CWA App keine Tracking- oder Nutzungsanalyse-Funktionalitäten beinhaltet, kann das RKI jedoch nicht die durch die CWA App verarbeiteten Kennungen und Risikoinformationen mit einem Nutzungsprofil verknüpfen, welches möglicherweise Rückschlüsse auf die Person des Nutzers ermöglichen würde. Für das RKI sind die nur lokal in der CWA App verarbeiteten Daten des Nutzers somit faktisch anonym.

Das RKI legt durch die Programmierung und das Verbreiten der CWA App jedoch die Mittel und Zwecke der lokalen Datenverarbeitung durch die CWA App fest. Fraglich ist daher, ob und, falls ja, in welchem Umfang diese Zweck-Mittel-Festlegung hinsichtlich der lokalen Datenverarbeitung trotz ihrer faktischen Anonymität für das RKI eine Verantwortlichkeit des RKI im Sinne von Art. 4 Nr. 7 DSGVO begründet.

Für die Bewertung des Personenbezugs kommt es nach der Rechtsprechung des EuGH auf die relative Bestimmbarkeit für den (eventuell) Verantwortlichen an, d. h. der (eventuell) Verantwortliche muss bei der Bewertung seiner möglichen Verantwortlichkeit nur die Mittel berücksichtigen, die er selbst oder eine andere Person nach allgemeinem Ermessen wahrscheinlich nutzen werden. Es ist somit zwar nicht Bedingung, dass alle für die Herstellung des Personenbezugs notwendigen Informationen oder Mittel für das RKI selbst verfügbar sind oder eingesetzt werden, d. h. das RKI muss sich das abstrakt verfügbare Drittwissen und die für Dritte zur Verfügung stehenden Mittel prinzipiell zurechnen lassen. Dies allerdings nur, soweit das Wissen und die Mittel durch das RKI vernünftigerweise eingesetzt werden (können). Mit der Rechtsprechung des EuGH wird man nach allgemeinem Ermessen davon

ausgehen müssen, dass Verantwortliche (insbesondere, wenn es sich um eine öffentliche Stelle handelt) grundsätzlich keine rechtswidrigen Mittel einsetzen, um die Anonymität aufzuheben.[12] Wenn man davon ausgeht, dass das RKI vernünftigerweise keine Maßnahmen ergreifen kann oder wird, um die Anonymität eines Nutzers aufzuheben, wären die lokal verarbeiteten Daten vor diesem Hintergrund auch dann als anonym für das RKI anzusehen, wenn sie im Einzelfall vom Nutzer oder einem Dritten (z. B. Apple/Google) einer Person zugeordnet werden können. Es erscheint daher vertretbar, eine datenschutzrechtliche Verantwortlichkeit des RKI für die lokale Verarbeitung durch die CWA App sowie das ENF – die eine Verarbeitung von personenbezogenen Daten voraussetzt – zu verneinen.

Der BfDI hat im Rahmen seiner projektbegleitenden Beratung erhebliche datenschutzrechtliche Bedenken an einer solchen Sichtweise geäußert. Das RKI hat sich daher entschieden, vorsorglich von seiner datenschutzrechtlichen Verantwortlichkeit für die oben beschriebene lokale Datenverarbeitung durch die CWA App auszugehen. Damit soll auch der Eindruck vermieden werden, dass sich das RKI als Anbieter der CWA App nicht für den Schutz der lokal verarbeiteten Daten zuständig fühlt.[13]

10.1.3 Gesundheitsdaten

Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Art. 4 Nr. 15 DSGVO), wobei auch Informationen über Krankheitsrisiken einer Person als Gesundheitsdaten gelten (vgl. Erwägungsgrund 35). Daher wäre beispielsweise auch die Angabe, dass der Nutzer einen bestimmten Risikostatus oder sich hat testen lassen hat, als Gesundheitsdatum einzustufen. Denn aus diesen Informationen geht hervor, dass eine erhöhte Wahrscheinlichkeit einer COVID-19-Erkrankung des Nutzers besteht.

Bei den Tagesschlüsseln des Nutzers handelt es sich um personenbezogene Daten, aber vor ihrer Umwidmung zu Positivschlüsseln (noch) nicht um Gesundheitsdaten. Da zum Verarbeitungszeitpunkt noch nicht bekannt ist, ob eine solche Umwidmung stattfinden wird, könnten die Tagesschlüssel allenfalls vorsorglich als Gesundheitsdaten betrachtet werden. Dies erscheint jedoch nicht sachgerecht. Denn die CWA App wird voraussichtlich ganz

[12] Vgl. zusammenfassend und m.w.N. bei Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 4 Nr. 1 Rn. 61 und 64.

[13] Vgl. ähnlich bei *Kühling/Schildbach*, in: Corona-Apps – Daten- und Grundrechtsschutz in Krisenzeiten (NJW 2020, 1545 (1549), die jedoch erst mit dem Absetzen einer Infektionsmeldung von einem Personenbezug für das RKI ausgehen: „Es erschiene teleologisch wenig überzeugend, gerade das RKI, das über die Mittel und Zwecke der Datenverarbeitung entscheidet und das notwendige zentrale Element herstellt, aus dem Anwendungsbereich des Datenschutzrechts zu entlassen. Daher spricht vieles für die Anwendbarkeit der datenschutzrechtlichen Regelungen. Das gilt allerdings nicht bereits mit dem Zeitpunkt des Beginns der CWA App-Nutzung, sondern erst mit dem Absetzen einer Infektionsmeldung. Letztlich verbleibt gerade in dieser zentralen Frage jedoch eine erhebliche Rechtsunsicherheit."

überwiegend von nicht infizierten – also gesunden – Personen verwendet werden. Daher lässt die Existenz von Tagesschlüsseln keinen Rückschluss auf einen bestimmten Gesundheitszustand oder ein bestimmtes Erkrankungsrisiko des Nutzers zu. Der Tagesschlüssel erlaubt nur den Rückschluss, dass der Träger dieses Pseudonyms ein Nutzer der CWA App ist. Zudem hat es allein der Nutzer in der Hand, ob eine Umwidmung seiner Tagesschlüssel zu Positivschlüsseln erfolgt, nämlich indem er ausdrücklich bestätigt und einwilligt, dass sein Testergebnis mit den anderen Nutzern geteilt wird.

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; sofern man (vorsorglich) davon ausgeht, dass auch die anschließende lokale Verarbeitung der heruntergeladenen Positivschlüssel durch die CWA App im Verantwortungsbereich des RKI erfolgt, handelt es sich für das RKI auch bei den lokal durch die CWA App verarbeiteten Kopien der Positivschlüssel anderer Nutzer um Gesundheitsdaten. Gleiches gilt für die lokal durch die CWA App ermittelten Ergebnisse der Risiko-Ermittlung, sofern und sobald ein Kontaktfall festgestellt worden ist.

Die Kennungen TAN, teleTAN, GUID und das Registration Token sind Gesundheitsdaten, da sie nur im Fall einer Testregistrierung oder eines positiven Testergebnisses verarbeitet werden. Aus der Existenz dieser Kennungen lässt sich deshalb ableiten, dass für den Nutzer entweder ein erhöhtes Risiko einer Coronavirus-Infektion und somit einer COVID-19-Erkrankung besteht oder er bereits infiziert ist.

Dies legt den Schluss nahe, dass es sich auch bei den im Rahmen des Verifikationshotline Prozesses verarbeiteten Daten um Gesundheitsdaten handelt. Denn es ist davon auszugehen, dass sich alle in Zusammenhang mit dem Verifikations-Hotline Prozess verarbeiteten personenbezogenen Daten auf einen infizierten Nutzer beziehen.

10.2 Rechtsgrundlagen

Eine Datenverarbeitung ist nur dann rechtmäßig ist, wenn eine wirksame Einwilligung oder ein anderer Zulässigkeitstatbestand legitimierend eingreift. Die Zulässigkeitstatbestände ergeben sich in erster Linie aus Art. 6 DSGVO und, soweit besondere Kategorien von personenbezogenen Daten, etwa Gesundheitsdaten, verarbeitet werden, aus Art. 9 DSGVO.

10.2.1 Geplante Rechtsgrundlage - Einwilligung

Zentrale Rechtsgrundlage für die Verarbeitung personenbezogener Daten in Zusammenhang mit dem Betrieb der CWA App ist die Einwilligung (gem. Art. 4 Nr. 7 DSGVO, Art. 6 Abs. 1 lit. a DSGVO). Da in weiten Teilen der CWA App besondere Kategorien personenbezogener Daten verarbeitet werden, insbesondere Gesundheitsdaten, gelten insoweit ergänzend die Anforderungen von Art. 9 Abs. 2 lit. a DSGVO. Für die Verarbeitung in den unterschiedlichen

Anwendungsphasen der CWA App werden jeweils separate Einwilligungen eingeholt. Die Einwilligungen sollen, soweit möglich und sachgerecht, in der CWA App eingeholt werden. Sofern die Einholung der Einwilligung in der CWA App nicht sachgerecht erscheint, wird sie in Zusammenhang mit der jeweiligen Verarbeitung eingeholt, etwa telefonisch im Rahmen der Verifikations-Hotline.

Das RKI begründet die Entscheidung für Einwilligungen als Rechtsgrundlage damit, dass die Schaffung einer spezialgesetzlichen Rechtsgrundlage von der Bundesregierung zurzeit nicht geplant ist.

10.2.2 Weitere mögliche Rechtsgrundlagen

10.2.2.1 § 3 BDSG

Soweit keine besonderen Kategorien personenbezogener Daten in der CWA App verarbeitet werden, käme auch § 3 BDSG als Rechtsgrundlage der Verarbeitung in Betracht. Demnach ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe erforderlich ist. Fragliche wäre, ob der Betrieb der CWA App als eine solche Aufgabe des RKI qualifiziert werden kann. Aus Gründen der höheren Transparenz hat sich das RKI jedoch auch in diesen Fällen für den Rückgriff auf die Einwilligung als Rechtsgrundlage entschieden.

10.2.2.2 § 4 Abs. 3 S. 4 IfSG

Das IfSG stellt dem RKI mit § 4 Abs. 3 S. 4 IfSG eine spezialgesetzliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten zum Zwecke der Kontaktpersonennachverfolgung zur Seite, soweit dies zur Abwendung von Gefahren von Dritten, den Betroffenen und der Verhinderung der Weiterverbreitung von schwerwiegenden übertragbaren Krankheiten erforderlich ist. Fraglich ist, ob diese Regelung dem grundgesetzlichen Bestimmtheitsgrundsatz genügt, Art. 20 GG. Zugleich ist der Anwendungsbereich der Regelung ausdrücklich auf die Zusammenarbeit des RKI mit internationalen Organisationen beschränkt (§ 4 Abs. 3 S. 4 Hs. 2 IfSG). Es ist zudem unklar, ob auch die Verarbeitung besonderer Kategorien personenbezogener Daten erfasst wäre. § 4 Abs. 3 S. 4 IfSG wurde daher im Rahmen des Betriebs der CWA App nicht herangezogen.

10.2.2.3 § 22 BDSG

Als Rechtsgrundlage der Verarbeitung, auch besonderer Kategorien von personenbezogenen Daten, kommt in Zusammenhang mit der CWA App neben der Einwilligung zudem § 22 Abs. 1 Nr. 1 lit. c und d sowie Nr. 2 lit. b BDSG in Betracht.

Bevor diese Normen als Rechtsgrundlage nutzbar gemacht werden können, stellt sich jedoch auch die Frage der Europarechtskonformität dieser Regelungen. Kritisch wird vor allem betrachtet, dass die Regelungen die Formulierung der Öffnungsklauseln aus Art. 9 Abs. 2 g und i DSGVO im Wesentlichen wiederholen, ohne dabei konkretere Vorgaben zu enthalten. Dies verstoße gegen die Systematik der Öffnungsklauseln, die eine spezifische Umsetzung verlange.[14]

Ebenfalls in Zusammenhang mit der hohen Abstraktion der Formulierung der Rechtsgrundlagen in § 22 BDSG steht der Vorwurf der fehlenden Vereinbarkeit mit dem Bestimmtheitsgebot des Art. 20 GG. Da § 22 BDSG die Verarbeitung von den besonders schützenswerten besonderen Kategorien personenbezogener Daten legitimiert, wäre eine möglichst konkreter Tatbestand der Norm erforderlich. Diesem Anspruch werden die Rechtsgrundlagen in § 22 BDSG nicht gerecht.

Auch unter Berücksichtigung der nachfolgend identifizierten Schwächen der Einwilligung als Rechtsgrundlage, ist diese aufgrund der mit ihr verbundenen höheren Transparenz gegenüber den Benutzern und der Warnfunktion im Ergebnis datenschutzfreundlicher und daher gegenüber einer der Rechtsgrundlagen nach § 22 BDSG vorzugswürdig.

10.2.2.4 Spezialgesetz

Teilweise wurde politisch und in der Öffentlichkeit für den Betrieb der CWA App die Schaffung einer spezialgesetzlichen Grundlage verlangt. Ein solches Gesetz könnte unter Nutzung der Öffnungsklauseln der DSGVO detaillierte Regeln für den Betrieb einer CWA vorsehen. Bestimmte rechtliche Unsicherheiten in Zusammenhang mit dem Betrieb der CWA, die auch in diesem DSFA Bericht aufgezeigt werden, könnten gegebenenfalls durch ein solches Gesetz aufgelöst werden. Allerdings könnte das Gesetz durch detaillierte Vorgaben den Eindruck erwecken, es gäbe eine gesetzliche Vorgabe oder wenigstens ein Gebot zur Nutzung der CWA App. Das Prinzip der freiwilligen Nutzung der CWA App wäre dann schwer zu begründen. Die Bundesregierung hat sich daher für eine einwilligungsbasierte CWA App entschieden.

10.2.3 Eignung der Einwilligung als Rechtsgrundlage

Die Wirksamkeitsvoraussetzungen einer Einwilligung ergeben sich aus Art. 4 Nr. 7 DSGVO in Verbindung mit Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DSGVO sowie Art. 7 DSGVO. Entscheidende Bedingungen einer wirksamen Einwilligung sind neben der Informiertheit, die Zweckbestimmtheit und die Freiwilligkeit.

[14] vgl. nur Frenzel, Paal/Pauly, § 22 Rn. 2; *Rose*, Taeger/Gabel, § 22 Rn. 8.

Von verschiedener Seite wurden Zweifel am Vorliegen der Wirksamkeitsvoraussetzungen der Einwilligung für die Datenverarbeitung im Rahmen der CWA geäußert[15].

10.2.3.1 Zweckbestimmtheit der Einwilligung

Die Einwilligungen in die Datenverarbeitung der verschiedenen Anwendungsphasen der CWA App sollen jeweils für die Nutzung einer bestimmten Funktion eingeholt werden:

- für die Risiko-Ermittlung,
- für die Testregistrierung und
- für das Teilen eines Testergebnisses.

Ausreichend bestimmt ist der Zweck einer Einwilligung, wenn „aus der Perspektive eines objektiven Empfängers der Einwilligung erkennbar ist, ob eine bestimmte Verarbeitung von der bestätigenden Handlung gedeckt ist“[16].

Da die oben genannten Funktionen bzw. Zwecke klar abgrenzbar und aus der Sicht eines Nutzers, der sich bewusst für die Installation der CWA App entscheidet, naheliegend und einleuchtend sind, ist nicht anzunehmen, dass der Zweck der Einwilligung nicht ausreichend bestimmt werden kann. Die Einwilligungserteilung kann durch eine eindeutige bestätigende Handlung erfolgen, nämlich durch Antippen eines entsprechenden Buttons.

Anforderungen:

Das RKI muss gewährleisten, dass die Einwilligungserklärung sprachlich und optisch transparent ist (vgl. Art. 12 Abs. 1 DSGVO) und die visuelle und textliche Gestaltung des Bestätigungsbuttons keinen Zweifel am Bestätigungswillen des Nutzers zulässt.

Im Rahmen der Verifikations-Hotline wird die Einwilligung gegebenenfalls fernmündlich eingeholt. In diesem Fall ist auf die verständliche mündliche Erläuterung der Datenverarbeitung Wert zu legen sowie eine eindeutige bestätigende Aussage des Nutzers einzuholen.

---

[15] Der EDSA empfiehlt in seinen Guidelines 04/2020 on the use of location data and contacttracing tools in the context of the COVID-19 outbreak, European Data Protection Board (abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (abgerufen am 14.06.2020) wenn möglich, die Nutzung einer gesetzlichen Rechtsgrundlage, da es an der Freiwilligkeit fehlen könne. Vgl auch netzpolitik.org, EU Abgeordnete hinterfragen Contact Tracing, (abrufbar unter: https://netzpolitik.org/2020/eu-abgeordnete-hinterfragen-contact-tracing/ (abgerufen am 14.06.2020).

[16] *Klement* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, DSGVO Art. 7, Rn. 68.

10.2.3.2 Informiertheit der Einwilligung

Die Informiertheit der Einwilligung erfordert, dass im Wissen um alle entscheidungsrelevanten Informationen die Risiken und Vorteile der Einwilligung von der betroffenen Person abgeschätzt und in einer selbstbestimmten Entscheidung münden können. Der Nutzer muss also in der Lage sein, die ihm vorgelegte Einwilligungserklärung (ggf. einschließlich der zugehörigen Datenschutzhinweise) inhaltlich vollumfänglich zu erfassen.

Der Nutzer muss insbesondere darüber in Kenntnis gesetzt werden, welche Arten von Daten zu welchem Zweck verarbeitet werden, wer die verantwortliche datenverarbeitende Stelle ist und wie diese zu erreichen ist sowie an welche Dritten die Daten im Falle der Übermittlung weitergegeben werden, wobei der Detailgrad in einen angemessenen Verhältnis zur Bedeutung des Geschäfts und dem Kontext der Einwilligung zu halten ist.[17]

Im Fall der CWA App ist nicht ersichtlich, dass diese Information dem Nutzer im Vorfeld einer Einwilligungserteilung nicht zuverlässig vermittelt werden könnten. Zu beachten ist, dass eine Einwilligung, die sich auf die Verarbeitung von Gesundheitsdaten bezieht, dies ausdrücklich benennen muss. Sofern die Risikoanalyse ergibt, dass das Risiko einer Identifizierung für den Nutzer aufgrund des konzeptionsbedingten Datenschutzes der CWA nur gering ist, bedarf es aus Sicht des DSFA-Teams insoweit keiner besonderen Risikohinweise.

Anforderungen:

Das RKI muss gewährleisten, dass der Nutzer vor der Erteilung einer Einwilligung in der CWA App in transparenter Form mindestens erfährt, welche Arten von Daten (z. B. Positivschlüssel) zu welchem Zweck (also für welche Funktion der CWA App) verarbeitet werden, dass das RKI der Verantwortliche ist und wie das RKI kontaktiert werden kann. Die letzten beiden Anforderungen dürften erfüllt sein, soweit die CWA App eine ordnungsgemäße Datenschutzerklärung und die Pflichtangaben gemäß § 5 TMG (Impressum) enthält.

Bei der Datenverarbeitung in Zusammenhang mit der Verifikations-Hotline wird die Einwilligung mündlich eingeholt. Die infizierten Nutzer werden gemäß dem Skript darüber informiert, dass ihnen Fragen zur Plausibilisierung ihres Testergebnisses gestellt werden und ihre Telefonnummer zum Zweck des Rückrufs aufgeschrieben und anschließend zeitnah durch Vernichtung gelöscht werden.

[17] Kühling/Buchner/Buchner/Kühling, 2. Aufl. 2018, DS-GVO Art. 7 Rn. 59.

10.2.3.3 Freiwilligkeit der Einwilligung

Von verschiedenen Seiten und in der öffentlichen Diskussion[18] wird die Ungeeignetheit der Einwilligung als Rechtsgrundlage für die Datenverarbeitung im Rahmen der CWA insbesondere damit begründet, dass es an der Freiwilligkeit fehlen könnte.

Das Freiwilligkeitsprinzip gliedert sich neben dem Unterprinzip „Informiertheit“ auch in das Prinzip „Freiheit von Zwang“.[19] Wenn die Einwilligung des Nutzers in die Datenverarbeitung informiert und ohne Zwang erteilt wird, ist sie freiwillig. Ohne Zwang ist die Einwilligung, wenn der Nutzer in der Lage sein, die Einwilligung zu verweigern oder zurückzuziehen, ohne dadurch Nachteile zu erleiden oder dies zu befürchten (vgl. DSGVO-Erwägungsgrund 42).

Der Freiwilligkeit könnten im Fall der CWA fehlen, als dass zwischen dem Nutzer und dem RKI als Verantwortlichen ein Über- und Unterordnungsverhältnis besteht (vgl. Erwägungsgrund 43). Denn als Bundesoberbehörde repräsentiert das RKI ein staatliches Organ. Allein daraus kann jedoch nicht grundsätzlich auf die fehlende Freiwilligkeit geschlossen werden.[20]

Die Freiwilligkeit fehlt erst, wenn in Anbetracht aller Umstände des Einzelfalls nicht anzunehmen ist, dass die Einwilligung freiwillig gegeben würde. Besaß der Betroffene keine

---

[18] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), Datenschutz-Folgenabschätzung für die Corona App, Version 1.6, abrufbar unter: https://www.fiff.de/dsfa-corona, S. 53; EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, p. 7; Kühling/Schildbach: Corona-Apps – Daten- und Grundrechtsschutz in Krisenzeiten, NJW 2020, 1545, S. 1547; statt vieler zudem Verweis auf den folgenden Presseartikel: Krempl, Corona-Tracing-Apps: Freiwilligkeit bedeutet nicht Freiwilligkeit abrufbar auf (abgerufen am 14.05.2020) mit Verweis auf die Online-Konferenz der Stiftung Datenschutz mit Frederick Richter (Stiftung Datenschutz), Chris Boos (IT-Unternehmer, Investor und Mitglied im Digitalrat der Bundesregierung), Ulrich Kelber (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit), Ninja Marnau (Senior Researcher am CISPA Helmholtz- Zentrum für Informationssicherheit), Jens Redmer (Director Business Development Google EMEA) und Sarah Spiekermann-Hoff (Professorin für Wirtschaftsinformatik und Institutsleiterin des Lehrstuhls für Wirtschaftsinformatik und Gesellschaft an der Wirtschaftsuniversität Wien). https://www.heise.de/newsticker/meldung/Corona-Tracing-Apps-Freiwilligkeit-bedeutet-nicht-Freiwilligkeit-4713114.html (abgerufen am 14.05.2020) mit Verweis auf die Online-Konferenz der Stiftung Datenschutz mit Frederick Richter (Stiftung Datenschutz), Chris Boos (IT-Unternehmer, Investor und Mitglied im Digitalrat der Bundesregierung), Ulrich Kelber (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit), Ninja Marnau (Senior Researcher am CISPA Helmholtz-Zentrum für Informationssicherheit), Jens Redmer (Director Business Development Google EMEA) und Sarah Spiekermann-Hoff (Professorin für Wirtschaftsinformatik und Institutsleiterin des Lehrstuhls für Wirtschaftsinformatik und Gesellschaft an der Wirtschaftsuniversität Wien).

[19] *Heckmann/Paschke* in Ehmann/Selmayr, DSGVO Kommentar, 2. Aufl. 2018, DS-GVO Art. 7, Rn. 48.

[20] So aber Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), Datenschutz-Folgenabschätzung für die Corona App, Version 1.6, abrufbar unter: https://www.fiff.de/dsfa-corona, S. 54.

echte Wahl, da er anderenfalls Nachteile zu befürchten hatte, stellt die Einwilligung keine gültige Grundlage für die Datenverarbeitung dar.

Dies könnte der Fall sein, wenn gesetzliche Vorgaben zur Nutzung der CWA App gemacht werden oder seitens einer Behörde ein bestimmter Verbreitungsgrad der CWA App zur Bedingung beispielsweise für Lockerungsmaßnahmen oder Zutrittsvoraussetzungen gemacht würde. Derartige Planungen sind derzeit jedoch nicht bekannt und seitens des RKI auch nicht geplant. Auch gibt es keine gesetzliche vorgesehene Normierung, die eine Nutzung der CWA App voraussetzt oder dazu verpflichtet. Zudem ist nicht offen ersichtlich und auch nicht öffentlich einsehbar, wer Nutzer der CWA ist und wer nicht. Das ist von außen nicht erkennbar. Auch ist es der Art der Datenverarbeitung nicht immanent, dass der Verantwortliche oder Dritte über dieses Wissen verfügen. Dadurch ist es zusätzlich erschwert von der Nutzung der CWA Vorteile abhängig zu machen, da deren Nutzung dem Einzelnen nicht angesehen und somit nachgewiesen werden kann.

Beispielsweise wird angeführt, dass die Freiwilligkeit eine echte Wahlmöglichkeit für den Betroffenen voraussetzt, da nur so die Schutzwirkung der Einwilligung erfüllt werden könne.[21]

Dieses unechte Wahlrecht kann sich daraus ergeben, dass sich einzelne Personen einem gesellschaftlichen Druck ausgesetzt sehen die CWA App zu nutzen. Wenn nämlich beispielsweise Familienmitglieder, Freunde und Arbeitskollegen die CWA App nutzen und sich herausstellt, eine Person aus ihrem Kreis tut dies nicht, dann kann dies zu einem moralischen Vorwurf und sozialem Druck führen, sodass der Betroffene die CWA App schließlich trotz innerer Ablehnung nutzt, um sich dem Druck zu entziehen. Dies könnte insbesondere auch dann eintreten, wenn von der Nutzung der CWA App von staatlicher Seite Lockerungsmaßnahmen abhängig gemacht würden, denn dann hänge es tatsächlich von der einzelnen Person ab, ob auch seine Familie, Freunde und Arbeitskollegen von weiterer Lockerungsmaßnahmen profitieren. Hier käme dann neben einem sozialen Druck auch ein staatlicher Druck zu tragen. Insofern stellt das FIfF in Ihrem Entwurf für die Datenschutz-Folgenabschätzung für die Corona-App dar, dass „der Freiwilligkeit der Einwilligung […] insoweit ein erwartbares belastendes Verwaltungshandeln gegenüber“ steht und sich dieses belastende Verwaltungshandeln „nicht gegen die einzelne Bürgerïn richtet, sondern im Form allgemeiner Freiheitsbeschränkungen unterschiedslos alle Bürgerïnnen betrifft“.

Zudem könnten auch private Einrichtungen eine Installation und Nutzung der CWA zur Voraussetzung Ihres Angebots machen (wie bspw. einem Restaurantbesuch). Zwar wäre ein Betroffener dann nicht verpflichtet das Angebot wahrzunehmen, jedoch mittelbar einem Zwang ausgesetzt die CWA gleichwohl zu nutzen, um von dem Angebot nicht ausgeschlossen zu werden. 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

[21] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), Datenschutz-Folgenabschätzung für die Corona App, Version 1.6, abrufbar unter: https://www.fiff.de/dsfa-corona, S. 54 mit weiterem Verweis auf Article 29 Data Protection Working Party 2018, S. 5.

kaufschwache Personen handelt. Daher erscheint es derzeit nicht nur aus wirtschaftlichen, sondern auch aus sozialen und Reputationsgründen unwahrscheinlich, dass private Einrichtungen die faktische Ausgrenzung eines erheblichen (und in der Regel überdurchschnittlich schutzbedürftigen) Teils der Bevölkerung betreiben werden.

Ferner wäre es einem Nutzer, der die CWA App nur aufgrund eines sozialen Zwangs nutzt, möglich, die CWA App auf einem (alten) Smartphone oder nur temporär zu installieren oder zu aktivieren, um im Fall einer privaten „Kontrolle“ die Nutzung der CWA App zu belegen.

Dem kann jedoch entgegengebracht werden, dass die Nutzung der CWA nicht überprüfbar ist, ohne dass der Nutzer die CWA App vorzeigt. Weder dem Verantwortlichen noch Dritten ist es von außen möglich einzusehen, ob die CWA App auf einem Smartphone installiert und vollumfänglich genutzt wird. Eine solche Veröffentlichung von Daten ist nicht vorgesehen und geplant. Auch gibt es keine Pläne oder gesetzliche Normierungen, die bspw. die Ausweitung von staatlichen Lockerungsmaßnahmen von der Nutzung der CWA App abhängig machen. Insoweit ist deshalb zurzeit nicht davon auszugehen, dass sich ein spürbarer gesamtgesellschaftlicher Druck zur Nutzung der CWA aufbaut.

Gleichwohl sind diesbezügliche Bedenken ernst zu nehmen.

Zu dem Ergebnis der grundsätzlichen Zulässigkeit auf der Basis der Freiwilligkeit kommt auch der EDSA.

Anforderung:

Das RKI sollte fortwährend beobachten, ob Anzeichen für einen „sozialen Zwang“ zur Nutzung der CWA-App bestehen und ggf. gegensteuernde Maßnahmen ergreifen.

Diese Erwägungen lassen sich auf die Einwilligung für die Verarbeitung der personenbezogenen Daten in Zusammenhang mit der Verifikations-Hotline übertragen.

10.2.3.4 Einwilligungen von Minderjährigen

Eine Nutzung der CWA App durch Nutzer unter 16 Jahren ist nicht vorgesehen. Die CWA App kann im Rahmen der vom Betriebssystem vorgesehenen Kinderschutzmaßnahmen auf Smartphones von Kindern verboten werden. Die CWA App erhebt keine Daten zum Alter des Nutzers, eine spezifische Einwilligung für Minderjährige ist deshalb nicht vorgesehen. Aus diesem Grund kann nicht ausgeschlossen werden, dass sich Jugendliche unter 16 Jahren entgegen dieser Vorgabe die CWA App trotzdem herunterladen und nutzen, ohne dass eine Einwilligung eines Erziehungsberechtigten vorliegt.

Das RKI hat faktisch keine Möglichkeit, dies zu verhindern. Es kann nur gezielt in der Veröffentlichungsphase und auch nach Veröffentlichung der CWA App darauf hinwirken, dass in der Öffentlichkeit ein Bewusstsein über diese Altersgrenzen herrscht, um einer Nutzung durch unter 16-jährige Personen ohne Zustimmung der Erziehungsberechtigten entgegenzuwirken.

Ein Verstoß gegen die Altersbeschränkung führt allerdings nicht zwangsläufig zur Unwirksamkeit der Einwilligung. Unwirksam wäre die Einwilligung im Fall von unter 16-jährigen Personen nur bei fehlender Einsichtsfähigkeit in die Reichweite der erteilten Einwilligung. Die Regelung des Art. 8 DSGVO, wonach die Wirksamkeit von Einwilligungen von unter 16-jährigen Personen nach Art. 8 DSGVO eine Einbeziehung der gesetzlichen Vertreter erfordert, steht dem nicht entgegen, da der Anwendungsbereich dieser Vorschrift nicht eröffnet ist. Art. 8 DSGVO findet nur auf "Dienste der Informationsgesellschaft" Anwendung. Die Definition des Begriffs „Dienst der Informationsgesellschaft" in Art. 4 Nr. 25 DSGVO verweist auf die Richtlinie (EU) 2015/1535. Danach ist ein Dienst der Informationsgesellschaft jede

- in der Regel gegen Entgelt
- elektronisch
- im Fernabsatz und
- auf individuellen Abruf eines Empfängers
- erbrachte Dienstleistung.

Die CWA App ist kein solcher Dienst, da mit ihr bzw. einer öffentlichen Corona-Tracing-App keine kommerziellen Interessen verfolgt und jedenfalls die Nutzung in der Regel ohne Zahlung eines Entgelts möglich ist. Denn eine Tracing-App, deren Nutzung nur gegen Entgelt möglich ist, dürfte ein erhebliches Verbreitungshindernis darstellen.

10.2.3.5 Datenverarbeitung in Zusammenhang mit der Verifikationshotline

Die Frage der datenschutzrechtlichen Relevanz der Vorgänge in Zusammenhang mit der Verifikationshotline ist differenziert zu betrachten.

Jedenfalls das Erfragen und Niederschreiben der Telefonnummer und ggfs. des Namens des anrufenden Nutzers durch den Mitarbeiter der Verifikations-Hotline fällt in den Anwendungsbereich des Datenschutzrechts. Name und Telefonnummer stellen personenbezogene Daten dar, Art. 4 Nr. 1 DSGVO. Das Erfragen und Niederschreiben ist auch eine Verarbeitung, Art. 4 Nr. 2 DSGVO. Gem. Art. 2 Nr. 1 unterfallen nichtautomatisierte Verarbeitungen allerdings nur dann der DSGVO, wenn die Daten in einem Dateisystem gem. Art. 4 Nr. 6 DSGVO gespeichert werden oder gespeichert werden sollen. Die Frage, ob das Aufschreiben von Name und Telefonnummer auf einen Zettel durch den Mitarbeiter sowie der anschließende Rückruf hierunter fällt ist mit Unsicherheit verbunden, kann jedoch dahinstehen. Denn gem. § 1 Abs. 8 BDSG ist die DSGVO für die Verarbeitung personenbezogener Daten durch öffentliche Stellen entsprechend anzuwenden, auch wenn der Anwendungsbereich der DSGVO aus anderen Gründen nicht eröffnet ist[22]. Da es sich bei dem RKI um eine öffentliche Stelle handelt und jedenfalls eine Datenverarbeitung vorliegt, sind

[22] *Ernst*, Paal/Pauly, § 1 BDSG Rn. 18; *Klar*, Kühling/Buchner, § 1 BDSG Rn. 34.

daher unabhängig hiervon die Vorgaben der DSGVO einzuhalten. Auch die Vorgaben des BDSG gelten unmittelbar, § 1 Abs. 1 Nr. 1 BDSG.

Anders könnte es sich jedoch hinsichtlich der Wahrnehmung des Namens des anrufenden Benutzers zu Beginn des Telefonats verhalten. Nach allgemeiner Ansicht setzt das Erheben von Daten im Sinne von Art. 4 Nr. 2 DSGVO ein aktives Tun voraus[23]. Daran fehlt es hier jedoch.

Die sich anschließende Beantwortung der Plausibilitätsfragen ist differenziert zu betrachten, soweit bei der Formulierung der Fragen darauf geachtet wird, dass keine für den Mitarbeiter der Verifikation-Hotline selbst personenbeziehbaren Daten erfragt werden. Insbesondere Details zu Anlass und Ablauf der ärztlichen Untersuchung sowie zum behandelnden Arzt stellen keine personenbezogenen Daten dar. Denn entsprechend den insoweit übertragbaren Erwägungen aus den Urteilen des EuGH[24] ist zwar nicht erforderlich, „dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden." Entscheidend ist in diesen Fällen jedoch, ob die Person über Mittel verfügt, „die vernünftigerweise eingesetzt werden könnten, um mit Hilfe Dritter […] die betreffende Person […] bestimmen zu lassen." Um mit Hilfe dieser Angaben den anrufenden Nutzer zu identifizieren, wäre eine Zusammenführung der Angaben mit Daten des behandelnden Arztes oder der sozialrechtlichen Leistungsträger erforderlich. Dem DSFA Team ist ein solcher Anspruch des RKI oder der sonstigen am Betrieb der CWA App beteiligten Akteure indes nicht bekannt, sodass insoweit davon ausgegangen werden kann, dass es sich bei den in Zusammenhang mit der Plausibilisierung erfragten Angaben nicht unbedingt um personenbezogene Daten handeln muss. Diese Bewertung wird jedoch durch die Abfrage der Telefonnummer zum Zwecke des Rückrufs obsolet, da jedenfalls darin die Verarbeitung eines personenbezogenen Datums zu sehen ist.

Daher ist auch in Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen der Verifikations-Hotline die Einwilligung als Rechtsgrundlage im vorab dargelegten Umfang als Rechtsgrundlage einzuholen.

10.3 Betroffenenrechte

Jede Verarbeitung personenbezogener Daten verlangt von dem Verantwortlichen die Gewährleistung der Betroffenenrechte auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGV), Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie die Gewährleistung der Mitteilungspflichten (Art. 19 DSGVO) und der Datenübertragbarkeit (Art. 20 DSGVO). Wenn die Verarbeitung auf Grundlage einer Einwilligung erfolgt, muss zudem die Widerruflichkeit der Einwilligung sichergestellt werden. Ausnahmen hiervon sind nur unter engen gesetzlichen Voraussetzungen möglich.

[23] vgl. nur *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann. Art. 4 Nr. 2, Rn. 15.
[24] EuGH, Urt. v. 19.10.2016, Rs. Breyer, C-582/14, Rn. 42 ff.

10.3.1 Widerruf von Einwilligungen

Gemäß Art. 7 Abs. 3 DSGVO muss eine wirksame Einwilligung jederzeit mit Wirkung für die Zukunft widerruflich sein. Gemäß Art. 17 Abs. 1 lit. b DSGVO sind die auf Grundlage der Einwilligung verarbeiteten personenbezogenen Daten dann grundsätzlich zu löschen. Zu den Einzelheiten wird auf die oben benannten Datenschutzkonzepte verwiesen.

Zum Widerruf der Einwilligung in die Risiko-Ermittlung können Nutzer die Funktion über den Schieberegler innerhalb der CWA App deaktivieren oder die CWA App löschen.

Zum Widerruf der Einwilligung zur Verarbeitung personenbezogener Daten in Zusammenhang mit der Funktion „Test registrieren“ können Nutzer die Testregistrierung in der CWA App löschen. Das Token zum Abruf des Testergebnisses wird dann von Gerät des Nutzers gelöscht. Weder das RKI noch das Labor können die übermittelten Daten dann der CWA App oder dem Smartphone des Nutzers zuordnen.

Zum Widerruf der Einwilligung in die Datenverarbeitung für die Funktion „Testergebnis teilen“ muss der Nutzer die CWA App löschen. Sämtliche in der CWA App gespeicherten RPIs werden dann entfernt und können dem Smartphone des Nutzers nicht mehr zugeordnet werden. Wenn die Möglichkeit vom Betriebssystem des Smartphones eröffnet ist, können die eigenen RPIs zudem im Rahmen der Kontaktaufzeichnungs-Funktion in den Systemeinstellungen des Smartphones des Benutzers gelöscht werden.

Ein Teil der auf dem Test Result Server, dem Verification Server und dem CWA Server gespeicherten Daten wird auch im Falle des Widerrufs erst nach Ablauf der vorgesehenen Löschfristen gelöscht. Dies wird damit begründet, dass keine Möglichkeit bestünde, eine frühere Löschung ohne Identifizierung des Nutzers durchzuführen. Insbesondere verzichte die CWA App auf ein eigenes Nutzer- und Berechtigungskonzept, da ansonsten zusätzliche identifizierende Informationen des Nutzers erhoben und verarbeitet werden müssten. Dies habe zur Konsequenz, dass eine Löschung von Daten in Zusammenhang mit dem Widerruf nicht möglich sei, da eine Zuordnung der Daten zu einem Nutzer nicht möglich wäre. Die Löschung könne daher nur durch den automatisierten Prozess innerhalb der Löschfristen erfolgen.

Vorausgesetzt, dass tatsächlich keine Möglichkeit der Identifizierung des Nutzers besteht, stellt dies nach Einschätzung des DSFA Teams eine zulässige Design-Entscheidung dar. Der europäische Gesetzgeber hat in Art. 5 Abs. 1 litt. c und e DSGVO die Entscheidung getroffen, dem Verantwortlichen das Minimieren der Verarbeitung personenbezogener Daten aufzugeben. Er hat in den Artt. 11 Abs. 2 S. 2, 12 Abs. 2 S. 2 DSGVO vorgegeben, dass der Verantwortliche und die betroffene Person eine weniger effektive Wahrnehmung der Betroffenenrechte in Kauf zu nehmen haben, wenn dadurch der Fortfall der Identifikationsmöglichkeit der betroffenen Person ermöglicht wird. Die Entscheidung, einerseits die Identifikation des Nutzers auszuschließen, andererseits dadurch die Löschung der personenbezogenen Daten des Nutzers auf dem Test Result Server, dem Verification Server und dem CWA Server durch den automatischen Löschprozess vornehmen zu lassen, setzt daher diese gesetzlichen Vorgaben um.

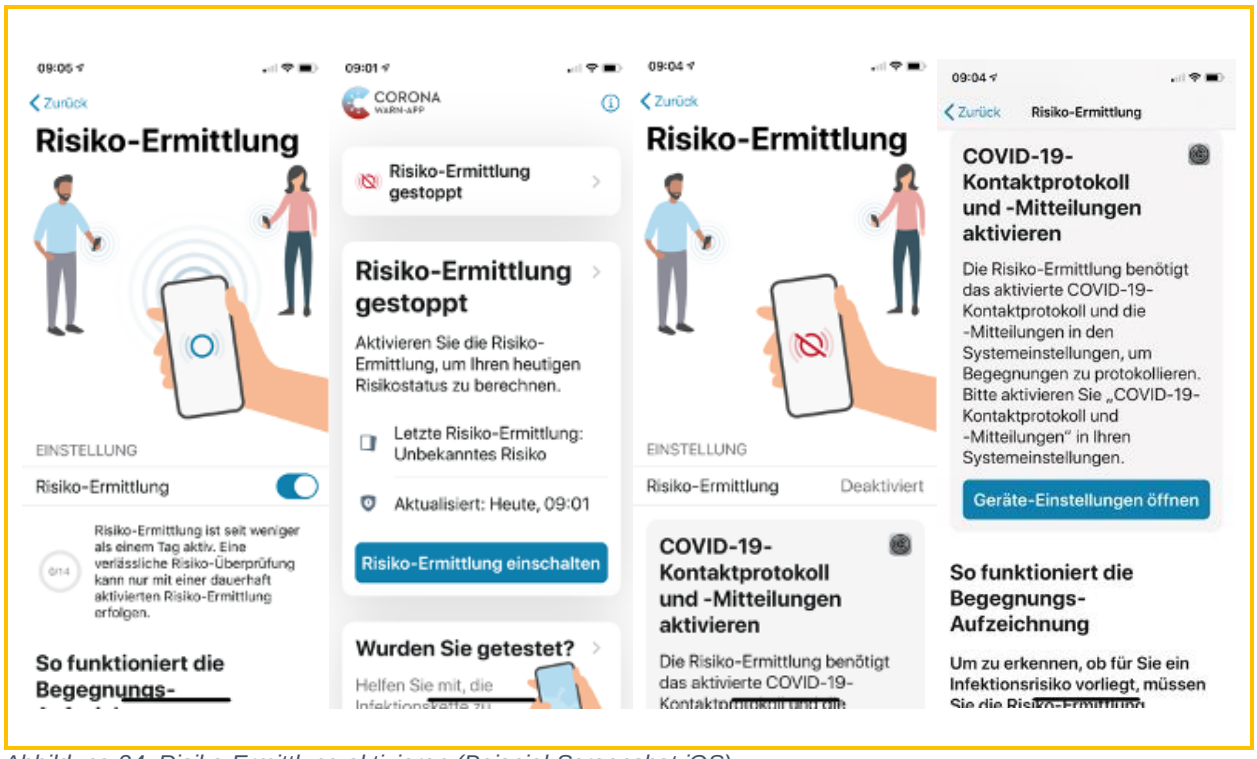


Abbildung 24: Risiko-Ermittlung aktivieren (Beispiel-Screenshot iOS)

Soweit die Verarbeitung personenbezogener Daten in Zusammenhang mit der Verifikationshotline auf Grundlage einer Einwilligung stattfindet, kann der Widerruf telefonisch erklärt werden. Da die Datenverarbeitung in Zusammenhang mit der Verifikationshotline jedoch weit überwiegend „flüchtig“ ist, also keine digitale oder physische Kopie der Daten existiert, ist der Widerruf insoweit ohnehin nur formeller Natur. Soweit eine physische Kopie der Daten besteht, kann diese ohne Weiteres durch Vernichtung gelöscht werden.

10.3.2 Gewährleistung weiterer Betroffenenrechte

Das RKI geht derzeit davon aus, dass eine Umsetzung der Betroffenenrechte nach Art. 15 ff. DSGVO nicht möglich ist. Die Identifizierung sei auch dann nicht möglich, wenn die betroffene Person zusätzliche Informationen zur Identifizierung bereitstelle. Hierauf weist der Verantwortliche Nutzer, die Anträge auf die Gewährleistung der Betroffenenrechte stellen, hin.

Der Verantwortliche kann unter den Voraussetzungen von Art. 11 Abs. 2 DSGVO in Verbindung mit Art. 12 Abs. 2 S. 2 DSGVO ausnahmsweise die Umsetzung der Betroffenenrechte verweigern. Das ist der Fall, wenn 1. der Verantwortliche dem Antragsteller keine durch ihn verarbeiteten Daten zuordnen kann, auch nicht nachdem die betroffene

Person zusätzliche Angaben zu seiner Person gemacht hat, und 2. der Verantwortliche dies nachweisen kann.[25]

Im Rahmen des Betriebs der CWA App verarbeitet das RKI ausschließlich pseudonyme Daten, für die dem Verantwortlichen die Informationen zur Zuordnung zu einer natürlichen Person fehlen. Ein Nutzer kann diese Pseudonyme gegenüber dem Verantwortlichen derzeit auch nicht auflösen. Hierzu würde eine Funktion der CWA App benötigt, die ihm die vorgenannten Pseudonyme offenbart oder dem RKI übermittelt. Die CWA App verfügt gegenwärtig über keine solche Funktion. Hierdurch wird sichergestellt, dass eine Identifikation nicht durch einen Fehler des Nutzers oder auf Grund eines Angriffs, der den Nutzer zur Identifikation bewegen soll, bewirkt werden kann.

Vorausgesetzt, dass tatsächlich keine Möglichkeit der Identifizierung des Nutzers besteht, stellt dies nach Einschätzung des DSFA Teams eine zulässige Design-Entscheidung dar. Für weitere Details zur rechtlichen Bewertung der Gewährleistung der Betroffenenrechte durch das RKI wird auf das Datenschutzkonzept der CWA der Bundesrepublik Deutschland, Version 1.1 verwiesen.

Aufgrund der nur flüchtigen Verarbeitung von personenbezogenen Daten außerhalb von Dateisystemen in Zusammenhang mit der Verifikationshotline, ergibt sich insoweit für die Betroffenenrechte kein Anwendungsfall. Soweit die Telefonnummer und der Name des Nutzers aufgeschrieben werden, müssen diese ohnehin zeitnah gelöscht werden. Dies ist auch im Falle eines Löschverlangens ohne Weiteres möglich.

Anmerkung:

Es wird empfohlen die technische Umsetzbarkeit der Betroffenenrechte in den zukünftigen Versionen der CWA App zu prüfen.

10.4 Privacy-by-Design-Maßnahmen

Für die technische Realisierung der CWA wurde eine Systemarchitektur konzipiert, die die Anforderungen von Datenschutz und Datensicherheit besonders berücksichtigt, wobei im Projektverlauf laufend Risikobetrachtungen und externe Stellungnahmen in die Architekturentscheidungen eingeflossen sind und nach Veröffentlichung weiter einfließen werden. Die daraus resultierenden Design-Maßnahmen führen zu einem konzeptionsbedingten Datenschutz der CWA.

Eine Übersicht aller Designentscheidungen kann dem Dokument Designentscheidungen (Anlage 1) entnommen werden. Insbesondere, aber nicht abschließend, wurden hierbei folgende Risiken berücksichtigt:

[25] Im Einzelnen streitig. Mit weiteren Nachweisen: *Dix*, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 12 Rn. 24.

- Risiken im Zusammenhang mit der Nutzung der ENF Schnittstelle der Betriebssysteme (Android und iOS)
    - Exakte Funktionsweise unbekannt
    - Unberechtigte Nutzung der Daten durch Apple und Google
    - überschießende Datenverarbeitung
- Risiken und Schwachstellen im Zusammenhang mit der Nutzung der BLE Technologie
    - Falsche Kontaktberechnung aufgrund von Ungenauigkeiten
    - Abfangen von Bluetooth Signalen
    - Angriffsszenarien
    - Bestehende Sicherheitslücken der Bluetooth-Technologie
- Teilen der CWA App mit Freunden/Bekannten
    - Zugriff auf Kontakdaten
- Nutzung der CWA App durch Minderjährige
- Bewegungsverfolgung
    - Vertraulichkeit der Tagesschlüssel und RPI
- Infektionsrisiko bestimmen
    - False positive/false negative
    - Sicherheit des QR-Codes
    - Sicherheit der Übermittlung der Daten zu einem positiven Test an andere Nutzer
- Risiken im Zusammenhang mit dem Hotline-Verfahren
    - Missbräuchliche Meldung von Positivbefunden
- Erkennen einer Infektion eines Nutzers durch Abfangen von Übertragungsdaten

10.5 Weitere datenschutzrechtliche Anforderungen

Bei der Entwicklung der CWA wurde versucht, die von verschiedenen fachkundigen Organisationen aufgestellten Datenschutzanforderungen an eine Corona-Tracing-App so weit wie möglich umzusetzen. Berücksichtigt wurden insbesondere folgende Dokumente:

- Europäischer Datenschutzausschuss (EDSA), Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 vom 21. April 2020[26]

[26] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_de.pdf

- Chaos Computer Club (CCC), 10 Prüfsteine für die Beurteilung von „Contact Tracing"-Apps vom 6. April 2020[27]
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FifF), Datenschutz-Folgenabschätzung (DSFA) für eine Corona-App, Version 1.6 vom 29. April 2020[28]
- Digitalcourage e.V., Einordung zur geplanten „Corona-Kontakt-Tracing-App" des RKI, Stand 4. Mai 2020[29]

Die Maßnahmen, die zur Umsetzung der in den genannten Dokumenten aufgestellten Anforderungen ergriffen worden sind, werden in dem Dokument „Designentscheidungen der CWA der Bundesrepublik Deutschland" (Anlage 1) dokumentiert.

Dieses Dokument soll dazu dienen, dass die datenschutzkritische Öffentlichkeit anhand der relevanten Anforderungen von Behörden und NGOs prüfen und bewerten kann, inwieweit ein grundrechtsschonendes Design gelungen ist. Auch werden Anregungen und Kritik gern aufgenommen.

11 Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

11.1 Notwendigkeit der Verarbeitung

Eine Datenverarbeitung ist in Bezug auf den Zweck als notwendig anzusehen, „wenn die Aufgabe sonst nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann"[30]. Dabei ist Notwendigkeit nicht auf die Datenverarbeitung in Ihrer Gesamtheit zu beziehen, „sondern auf die einzelnen konkreten Ausgestaltungsaspekte, die in der systematischen Beschreibung darzustellen sind"[31].

Die verschiedenen Verarbeitungsvorgänge im Rahmen der CWA sind notwendig, da es zurzeit keine anderen technischen Lösungen gibt, um einzelne Personen über ein sie betreffendes Infektionsrisiko in einem engen zeitlichen Zusammenhang zu informieren, Testergebnisse bekannt zu geben und andere Personen über vor einer möglichen Ansteckung kurzfristig zu warnen. Dies gilt insbesondere für den Gebrauch des ENF.

---

[27] https://www.ccc.de/de/updates/2020/contact-tracing-requirements
[28] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), Datenschutz-Folgenabschätzung für die Corona App, Version 1.6, abrufbar unter: https://www.fiff.de/dsfa-corona.
[29] https://digitalcourage.de/blog/2020/corona-app-einordnung-digitalcourage
[30] *Jandt* in Kühling/Buchner, DSGVO Kommentar 2. Aufl. 2018, DS-GVO Art. 35, Rn. 40; *Dammann* in Simitis, Bundesdatenschutzgesetz, 7. Aufl. 2011, § 14, Rn. 15.
[31] *Jandt* in Kühling/Buchner, DSGVO Kommentar 2. Aufl. 2018, DS-GVO Art. 35, Rn. 40.

Bei den Anwendungsphasen 1 (Risiko-Ermittlung) und 2 (Kontaktfall) liegt der Zweck darin, den Nutzer anhand der erfassten RPIs anderer Nutzer automatisch darüber zu informieren, dass sie sich in der Nähe eines mit Coronavirus infizierten anderen Nutzers aufgehalten haben und wegen des Zeitpunkts (Datum), der Dauer und des Abstands zum infizierten Nutzer ein möglicherweise erhöhtes Infektionsrisiko besteht. Bei Anwendungsphase 3 (Testregistrierung) wird der Zweck verfolgt, den Nutzer im Nachgang zu einem bei ihm durchgeführten Coronavirus-Test möglichst schnell über sein Testergebnis zu informieren, so dass der Nutzer im Fall eines positiven Testergebnisses ohne Zeitverlust Maßnahmen zur eigenen Gesundheitsfürsorge und zur Reduzierung des Ansteckungsrisikos für andere Personen ergreifen kann und somit Infektionsketten so früh wie möglich unterbrochen werden können. In der Anwendungsphase 4 (Testergebnis teilen) wird der Zweck verfolgt, die Information über ein positives Testergebnis für andere Nutzer verfügbar zu machen, sodass diese im Fall eines vorangegangenen Kontakts mit dem (infizierten) Nutzer gewarnt werden.

Alle vorgenannten Zwecke können nur erreicht werden, wenn die CWA App die Daten des Nutzers wie oben beschrieben verarbeitet und insbesondere das ENF nutzt. Ohne die Nutzung des ENF wäre die CWA App nicht zum Hintergrundbetrieb in der Lage und hätte somit keine Möglichkeit, zuverlässig RPIs mit anderen Smartphones auszutauschen.

Die Verarbeitung von Name, Telefonnummer sowie der Antworten auf die Plausibilitätsfragen in Zusammenhang mit der Verifikations-Hotline dient der Verringerung des Missbrauchs der CWA App. Andere mildere Mittel zur Verhinderung des Missbrauchsrisikos sind nicht ersichtlich. Die Verarbeitung ist daher notwendig.

11.2 Verhältnismäßigkeit der Verarbeitung

Die Verarbeitungsvorgänge der CWA sind verhältnismäßig, soweit sie legitimen Zwecken dienen und zur jeweiligen Zweckerreichung geeignet, erforderlich und angemessen sind.

11.2.1 Legitimer Zweck

Die Verarbeitungsvorgänge der CWA dienen legitimen Zwecken, nämlich der frühzeitigen Unterbrechung von Infektionsketten und dem Gesundheitsschutz der einzelnen Nutzer.

Der Einsatz der Verifikations-Hotline unterstützt den digitalen Prozess (QR-Code Verfahren), um einer möglichst breiten Bevölkerungsschicht die Nutzung der der CWA zu ermöglichen, insbesondere Nutzern die über keinen QR-Code verfügen oder diesen verloren haben oder soweit Labore noch nicht an die erforderliche Infrastruktur angeschlossen sind. Die Verarbeitung von Name, Telefonnummer sowie der Antworten auf die Plausibilitätsfragen dient auch einem legitimen Zweck. Ein Missbrauch der CWA App wäre geeignet, andere Nutzer erheblich in ihren Freiheitsrechten einzuschränken, wenn diese sich aufgrund eines fälschlicherweise über die CWA App gemeldeten Infektionsrisikos in die Isolation begeben. Der Missbrauch der CWA App birgt darüber hinaus die Gefahr der erheblichen Einschränkung des öffentlichen Lebens, wenn sich Nutzer, die über die CWA App eine falsche Risiko-

Benachrichtigung erhalten, andere Menschen aus ihrem Umfeld warnen, ohne das Ergebnis eines Tests abzuwarten. So ist denkbar, dass sich öffentliche Einrichtungen, wie Schulen, aufgrund einer falschen Risiko-Benachrichtigung eines Lehrers oder Schülers veranlasst sehen, vorübergehend zu schließen. Des Weiteren ist bereits das Risiko des Missbrauchs der CWA App geeignet, das Vertrauen in die Funktionsfähigkeit und Sinnhaftigkeit der CWA App zu unterminieren, was zu einer geringeren Akzeptanz sowie Nutzung der CWA App in der Bevölkerung führen kann.

11.2.2 Eignung

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. Gleichwohl ist noch unklar, wie effektiv diese Technologie bei der Verfolgung von Tracking-Zwecken ist.

An der Eignung der CWA App zum Abruf und Teilen von Testergebnissen, so dass Infektionsketten früher unterbrochen werden können, bestehen keine Zweifel.

Die Eignung der Verarbeitung von Name, Telefonnummer sowie der Antworten auf die Plausibilitätsfragen zum Zweck der Verringerung der Gefahr des Missbrauchs der CWA App ist fraglich. Wenn die Kombination aus dem Stellen von Plausibilitätsfragen und Erheben von Name und Telefonnummer sowie dem Rückruf im Einzelfall es im Einzelfall erlauben einen dolosen Nutzer zu erkennen, so sind die Maßnahmen jedenfalls nicht geeignet denselben Nutzer der CWA App daran zu hindern erneut anzurufen und zu versuchen, sich gegenüber einem anderen Mitarbeiter, unter anderen Namen und mit anderen Antworten auf die Plausibilitätsfragen Zugang zu einer teleTAN zu verschaffen. Es ist zudem nicht auszuschließen, dass es im Social Engineering erfahrenen Nutzern durch überzeugendes Auftreten auch im ersten Anruf gelingen kann, die Plausibilitätsfragen in überzeugender Weise zu beantworten Da jedoch jedenfalls im Einzelfall die Verhinderung eines Missbrauchs möglich ist, so kann die Eignung jedoch nicht generell ausgeschlossen werden. Es sind jedoch wesentlich effektivere Mittel der Missbrauchsverhinderung denkbar.

Eine vom Datenschutzbeauftragten des RKI empfohlene Alternative besteht darin, die Verifikations-Hotline nicht für Nutzer anzubieten, sondern nur für die behandelnden Ärzte zu eröffnen. Diese könnten die Verifikations-Hotline anrufen und die teleTAN erfragen, nachdem sie ein positives Testergebnis eines Nutzers vom Labor erhalten haben und die teleTAN anschließend an den jeweiligen Benutzer weitergeben. Der anrufende Arzt könnte etwa durch Abgleich der angezeigten Rufnummer mit der öffentlich bekannten Rufnummer des Arztes oder unter Verwendung einer entsprechenden Datenbank authentisiert werden. Zwar sind Angriffe auch in diesem Fall nicht vollkommen ausgeschlossen, etwa durch sog. Call ID Spoofing (also das Anzeigen einer falschen Telefonnummer). Diese Missbrauchsmöglichkeit ist jedoch wesentlich aufwendiger und kann durch entsprechende Gegenmaßnahmen seitens der Verifikations-Hotline, etwa dem Einsatz entsprechender Endgeräte, effektiv verhindert werden. Die Umsetzung dieser Maßnahme wird gegenwärtig geprüft.

11.2.3 Erforderlichkeit

Die Datenverarbeitung im Rahmen der CWA App ist für die Erfüllung der genannten Zwecke erforderlich. Gleich geeignete oder mildere Mittel sind nicht ersichtlich, insbesondere wird bereits eine konzeptionsbedingt datensparsame Systemarchitektur verfolgt. Die Nutzung von GPS- oder Mobilfunk-Metadaten wäre keine mildere Alternative, da Standortdaten verarbeitet werden müssen, die – anders als die per BLE ausgetauschten RPIs – zur Erstellung von Bewegungsprofilen verwendet werden können, die wiederum Rückschlüsse auf den Nutzer zulassen können.

Eine Kontaktnachverfolgung und Warnung von Kontakten, die dem Nutzer nicht persönlich bekannt sind, ohne den Einsatz einer App ist – auch in pseudonymer oder gar anonymer Form – zurzeit technisch nicht realisierbar.

Mit Hilfe einer App können Personen deutlich schneller über eine potentielle Infektionsgefahr informiert werden als auf „traditionelle“ Weise (z. B. telefonisch durch die Gesundheitsämter).

Durch die automatisierte und für die beteiligten Akteure faktisch anonyme Bekanntgabe von Testergebnissen in der CWA App wird die Datenverarbeitung zwischen Labor, Arztpraxis und getesteter Person auf das minimal erforderliche Maß reduziert und ein Missbrauch oder falsche Bekanntgabe von Testergebnissen deutlich unwahrscheinlicher. Die automatisierte Verarbeitung kann zudem die händische Anreicherung von analog vorhandenen Patientendaten bei den beteiligten Akteuren (Arzt, Labor, Gesundheitsamt usw.) verhindern, die ihrerseits wiederum eigene Gefahrenquellen für Fehler oder Missbrauch darstellen könnten.

Die Verarbeitung von Name, Telefonnummer sowie der Antworten auf die Plausibilitätsfragen im Rahmen der Verifikations-Hotline ist auch erforderlich. Wenn die Kombination aus dem Stellen von Plausibilitätsfragen und Erheben von Name und Telefonnummer sowie dem Rückruf es auch im Einzelfall ermöglichen kann, einen dolosen Benutzer der App zu erkennen, so sind die Maßnahmen jedenfalls nicht geeignet denselben Benutzer der CWA App daran zu hindern erneut anzurufen und zu versuchen, sich gegenüber einem anderen Mitarbeiter, unter anderem Namen und mit anderen Antworten auf die Plausibilitätsfragen Zugang zu einer teleTAN zu verschaffen. Da jedoch jedenfalls im Einzelfall die Verhinderung eines Missbrauchs möglich ist, kann die Erforderlichkeit nicht generell ausgeschlossen werden.

11.2.4 Angemessenheit

Im Ergebnis sind keine Anhaltspunkte ersichtlich, die gegen die Angemessenheit sprechen würden.

Eine Verarbeitung ist zur Erreichung eines Zweckes angemessen, wenn die konkrete Interessenabwägung im Rahmen einer Zweck-Mittel-Relation zugunsten der Verantwortlichen ausfällt. Es sind daher die Interessen der betroffenen Personen mit den Interessen des

Verantwortlichen abzuwägen. Im Fall der CWA stehen sich die Interessen des RKI als Verantwortlicher und die Interessen der Nutzer gegenüber.

Die Interessen des RKI liegen darin, im Rahmen der ihm zugewiesenen Aufgaben der Erkennung, Verhütung und Bekämpfung von Krankheiten das Gesundheitsrisiko für die Bevölkerung zu minimieren und die Gefahr von Corona-Neuansteckungen durch die Bereitstellung der verschiedenen Funktionalitäten der CWA App bereits in einem frühen Stadium zu unterbinden. Damit kommt das RKI im Rahmen seiner Aufgaben der Verwirklichung des Grundrechts auf das Leben und die körperliche Unversehrtheit nach.

Demgegenüber stehen die Interessen der Nutzer, nicht in ihren Grundrechten insbesondere auf das Recht der informationellen Selbstbestimmung eingeschränkt zu werden und beispielsweise einer Überwachung, gesellschaftlichem Druck zur Nutzung der CWA App oder rechtlichen, wirtschaftlichen oder sozialen Nachteilen infolge der Nichtnutzung der CWA App ausgesetzt zu sein. Dies insbesondere auch deswegen, weil der Nutzen von Corona-Tracing-Apps noch unbekannt ist und die Hinnahme von Grundrechtseinschränkungen somit möglicherweise umsonst gewesen ist.

Gegen die Angemessenheit der Verarbeitung zu den mit der Risiko-Ermittlung verfolgten Zwecken würde es sprechen, wenn zur Eindämmung der Corona-Pandemie eine dezentrale und somit lokale Verfolgung von infizierten Personen und ihren Kontakten – also so, wie sie schon jetzt durch die Gesundheitsämter durchgeführt wird – den größeren Nutzen verspricht. Dies würde sich für die Bevölkerung grundrechtsschonender darstellen, da nur solche Personen kontaktiert und mit dem Gesundheitsamt in Verbindung gebracht werden, bei denen ein begründeter Verdacht für eine Corona-Infektion besteht. Dies kann jedoch nicht bewertet werden, da ein gewisser Nutzen einer Corona-Tracing-App zwar wahrscheinlich, konkret aber noch nicht absehbar ist. Es darf jedoch angenommen werden, dass eine Corona-Tracing-App der lokalen Verfolgung durch die Gesundheitsämter jedenfalls bei der Nachverfolgung von Infektionsketten im Zusammenhang mit Reiseaktivitäten regelmäßig deutlich überlegen sein wird. Gleiches gilt bei sich schnell ausbreitenden Infektionswellen, nicht zuletzt wegen der häufig personell unzureichend ausgestatteten lokalen Gesundheitsbehörden,

Es besteht das Risiko, dass durch die CWA App (oder eine andere Corona-Tracing-App) eine übermäßige Datenverarbeitung ermöglicht wird, so dass auch solche Daten erfasst werden, die zur Erreichung der Zwecke der CWA App nicht geeignet oder erforderlich sind. Somit würden die Nutzer bei Verwendung der CWA App der Gefahr ausgesetzt, dass die dabei angesammelten Daten für andere Zwecke genutzt werden, die der Nutzer nicht mehr überblicken kann. Dieses Risiko, welches prinzipiell bei jeder Verwendung neuer Technologien zur Verarbeitung personenbezogener Daten besteht, kann in der Regel nur effektiv auf ein verhältnismäßiges Maß reduziert werden, indem die konkrete technische Umsetzung zu einem ausreichenden konzeptionsbedingten Datenschutz (Privacy by Design) führt, der insbesondere die Schutzziele der Datenminimierung und Zweckbindung gewährleistet. Vor diesem Hintergrund ist die CWA App unter Beachtung des Privacy-by-Design-Grundsatzes konzipiert worden (siehe Privacy-by-Design-Maßnahmen). Insbesondere wurde bewusst auf eine zentrale Speicherung von Kontakten sowie die Erfassung von einer Identifizierung einzelner Nutzer ermöglichenden Angaben sowie Standortdaten verzichtet. Die CWA App ist technisch so konzipiert, dass die personenbezogene Datenverarbeitung faktisch anonym

abläuft und sich auf ein minimales Maß beschränkt. Sofern diese Design-Maßnahmen ausreichend effektiv sind, steht allein das Risiko einer übermäßigen Datenverarbeitung der Verarbeitung im Rahmen der Funktionen der CWA App daher nicht entgegen.

Der Umstand, dass die CWA App die Konnektivitäten und das ENF von Google und Apple verwendet, stellt ein erhebliches Risiko dar, welches durch das RKI praktisch nicht beseitigt und auf technischer Ebene auch nicht reduziert werden kann. Die genaue technische Umsetzung der betriebssystem- und hardwareseitigen Funktionalitäten ist der Kontrolle des RKI entzogen. Es ist anzunehmen, dass Apple und Google durch eine Änderung des ENF auch zur Verknüpfung der dort verarbeiteten Tagesschlüssel und RPIs mit einer geräte- (z. B. Werbe-ID) oder nutzerspezifischen Kennung (z. B. Apple-ID oder Google-Konto) in der Lage sind. Derartige Risiken bestehen allerdings bei jeder Drittanbieter-App, die Schnittstellen eines Betriebssystems oder technische Komponenten des Smartphones nutzt. Allerdings haben die Nutzer durch die Verwendung eines Android- bzw. iOS-Smartphones zum Ausdruck gebracht, 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 (z. B. durch Deaktivierung der Ortungsdienste). Daher ist es nicht überzeugend, die Unverhältnismäßigkeit mit der Nutzung von Software und Hardware von Drittherstellern zu begründen.

Zugunsten der Verhältnismäßigkeit der Verarbeitungsvorgänge der CWA spricht die Freiwilligkeit der Nutzung. Damit wird auch dem Recht auf informationelle Selbstbestimmung des Einzelnen Ausdruck verliehen. Es darf und soll niemand von staatlichen Stellen dazu gezwungen werden, die CWA App zu nutzen. Es steht jedem frei, die CWA App zu nutzen oder die Nutzung abzulehnen. Entscheidet sich eine Person für die Nutzung der CWA App, so basieren die Datenverarbeitungen auf deren Einwilligungen. Vor Erteilung der Einwilligungen wird der Nutzer in der CWA App oder im Rahmen von Probenentnahmen über die Datenverarbeitung informiert. Damit liegen die Voraussetzungen für eine informierte und freiwillige Einwilligung in die Datenverarbeitung vor.

Die CWA App verfügt auch nicht über Funktionen, die eine Verwendung im Sinne eines „Immunitätsausweises“ nahelegen. Mit der CWA App kann ohne das Zutun des Nutzers nicht durch Dritte nachvollzogen werden, ob er bereits mit dem Coronavirus infiziert war oder ein erhöhtes Infektionsrisiko besteht. Allerdings kann naturgemäß nicht ausgeschlossen werden, dass versucht wird, die CWA App zu derartigen Zwecken einzusetzen, etwa indem ein Betreiber einer öffentlich zugänglichen Einrichtung (z. B. Restaurant) das Vorzeigen der CWA App oder eines „niedrigen Risikos“ zur Voraussetzung für den Einlass macht. Zwar wäre ein Betroffener dann nicht verpflichtet, das Angebot wahrzunehmen, jedoch mittelbar einem Zwang ausgesetzt die CWA gleichwohl zu nutzen, um von dem Angebot nicht ausgeschlossen zu werden. 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. Daher erscheint es derzeit nicht nur aus wirtschaftlichen, sondern auch aus sozialen und Reputationsgründen unwahrscheinlich, dass private Einrichtungen die faktische Ausgrenzung eines erheblichen (und in der Regel überdurchschnittlich schutzbedürftigen) Teils der

Bevölkerung betreiben werden. Ferner wäre es einem Nutzer, der die CWA App nur aufgrund eines sozialen Zwangs nutzt, möglich, die CWA App auf einem (alten) Smartphone oder nur temporär zu installieren.

Mit Blick auf die Zwecke der CWA App und ihrer potenziellen Bedeutung für die Unterbrechung von Infektionsketten und um das Risiko des Einzelnen für eine Infektion zu verringern wird die Datenverarbeitung im Zusammenhang mit der CWA App daher zum jetzigen Zeitpunkt insgesamt als notwendig und verhältnismäßig bewertet. Allerdings muss die Verhältnismäßigkeit fortwährend weiterbewertet werden für den Fall, dass sich die hier zugrunde gelegten Umstände ändern. Dies gilt insbesondere für die Situation, dass Sicherheitslücken oder geänderte Datenschutzpraktiken auf Seiten der Hersteller der Smartphones und Betriebssysteme bekannt werden, Anhaltspunkte für das Entstehen eines sozialen Drucks zur Nutzung der CWA App oder unvorhergesehene Häufungen von Fehlwarnungen dazu führen, dass Nutzer fälschlich annehmen, sie wären infiziert.

Die Verarbeitung von Name, Telefonnummer sowie der Antworten auf die Plausibilitätsfragen im Rahmen der Verifikations-Hotline ist ebenfalls angemessen. Mit Blick auf die oben beschriebenen erheblichen Auswirken der missbräuchlichen Nutzung der CWA App auf die Freiheiten des Einzelnen sowie die durch eine missbräuchliche Nutzung möglichen Einschränkung des öffentlichen Lebens ist die Verarbeitung der Daten des Nutzers durch den Mitarbeiter der Verifikations-Hotline auch angemessen. Dies gilt auch vor dem Hintergrund der nur eingeschränkten Eignung des gegenwärtigen Verfahrens der Verifikations-Hotline.

12 Risikoanalyse

12.1 Methodik

Grundlage und Hilfsmittel für die Planung, Durchführung und Dokumentation der Risikoanalyse im Rahmen dieser DSFA ist eine Excel-Tabelle, die 2018 im Rahmen eines Projektes zur Umsetzung eines integrierten IT-Sicherheits- und Datenschutz-/Risikomanagements im medizinischen Umfeld erstellt und seitdem weiterentwickelt wurde.

Die Excel-Tabelle ist konzipiert worden, um eine integrierte Betrachtung klassischer Datensicherheitsziele (Verfügbarkeit, Integrität, Vertraulichkeit) aus Unternehmenssicht einerseits und der Datenschutzziele andererseits, zu denen – neben Verfügbarkeit, Integrität und Vertraulichkeit – etwa auch Zweckbindung, Datenminimierung, Transparenz und Nichtverkettbarkeit gehören, zu ermöglichen. Sie ermöglicht ein systematisches Vorgehen unter Berücksichtigung verschiedener Blickwinkel (Betrachtung spezifischer Risikoquellen, Schadenspotentiale für verschiedene Betroffenengruppen) und die zeitversetzte Durchführung von Risikobewertungen durch verschiedene Projektbeteiligte sowie die flexible Anpassung an Designentscheidungen und Anforderungen von Entwicklern, externen Beratern und Aufsichtsbehörden.

Für das Gesamtprojekt wird jeweils eine Risikobewertung zum einen gemeinsam für die VT 1, 2 und 4 durchgeführt, für VT 3 sowie den Hotline-Prozess.

12.2 Risiko-Identifikation

Um zu identifizieren, wie, durch wen oder was und unter welchen Umständen, Risiken für die Rechte und Freiheiten natürlicher Personen ausgelöst werden können, wurde – dem Praxishandbuch des Forum Privatheit angelehnt[32] – in folgenden Schritten vorgegangen:

(1) Identifikation der Risikoquellen
(2) Identifikation der Bedrohungen/Risiken
(3) Zuordnung von Bedrohungen/Risiken zu Betroffenen

12.2.1 Risikoquellen

Risikoquellen sind zum einen Personen, die ein Interesse daran haben könnten, die Verarbeitungsvorgänge und die damit verarbeiteten Daten in unrechtmäßiger Weise zu verwenden. Aber auch Stellen, die eine rechtmäßige Datenverarbeitung bezwecken, können ein Risiko darstellen.

Folgende Risikoquellen für die Rechte und Freiheiten natürlicher Personen wurden identifiziert:

- CWA-Nutzer
- Skriptkiddie
- Hacker
- Cracker
- (ehemaliger) Mitarbeiter
- Wirtschaftsunternehmen mit kommerziellen Interessen (inkl. andere App-Betreiber)
- Hersteller/ Betreiber
- Versicherungen/ Arbeitgeber/ Inhaber von Hausrechten
- Krimineller
- Labormitarbeiter/Arzt
- Geheimdienst/ Regierung/Sicherheits- und Gesundheitsbehörden

Einzelheiten können dem Tabellenblatt „Angreifertyp und Motivation“ der Risiko-Matrix entnommen werden.

(In der Risiko-Matrix können die Risikoquellen nach Bedarf ausgewählt werden, somit ein bestimmtes Bedrohungsszenario für verschiedene Risikoquellen betrachtet werden.)

[32] Martin/ Friedewald/ Schiering/ Mester/ Hallinan „Die Datenschutzfolgenabschätzung nach Art. 35 DSGVO – Ein Handbuch für die Praxis“, Frauenhofer Verlag, 2020 (im Folgenden „Praxishandbuch“).

12.2.2 Bedrohungen/Risiken

Die Bedrohungen/Risiken werden, ausgehend von den Schutzzielen und den Betroffenenrechten, den folgenden Risikokategorien zugeordnet:

- Unbefugte oder unrechtmäßige Verarbeitung
- Verarbeitung wider Treu und Glauben
- Für die Betroffenen intransparente Verarbeitung
- Unbefugte Offenlegung von und Zugang zu Daten
- Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten
- Verweigerung der Betroffenenrechte
- Verwendung der Daten zu inkompatiblen Zwecken
- Verarbeitung nicht vorhergesehener Daten
- Verarbeitung nicht richtiger Daten
- Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler)
- Verarbeitung über die Speicherfrist hinaus
- Die Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung selbst liegt.

Die identifizierten Bedrohungen/Risiken speisen sich aus folgenden Quellen:

- Risikoszenarien, die von fachkundigen Organisationen identifiziert worden sind (siehe unter Ziffer 9.12)
- Risikobetrachtungen durch die Projektbeteiligten
- Ergebnisse der Workstreams
- Ergebnisse aus dem Threat Modelling für die Komponenten CWA App, CWA Server, Verifikation Server, Portal Server und Lab Server

12.2.3 Zuordnung der Risiken zu Betroffenengruppen

Um eine differenzierte Bewertung der identifizierten Bedrohungen/Risiken zu ermöglichen, werden diese den potenziellen Betroffenengruppen zugeordnet.

Vorliegend gibt es nur eine Kategorie von betroffenen Personen, nämlich Nutzer der CWA App. Die potenziellen Betroffenengruppen entsprechen daher den verschiedenen Nutzergruppen. Beispiele sind:

- Kinder
- Jugendliche
- Epidemiologische Risikogruppen (60+, Vorerkrankungen)
- Nicht-Erstsprachler
- Nutzer mit wenig „App-Erfahrung“
- Nutzer mit Sehbehinderungen

12.3 Bewertung der Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit (Wahrscheinlichkeit im Sinne der ISO 27005) ist ein Schätzer für das Eintreten eines Ereignisses, der in dieser DSFA anhand des auf dem Tabellenblatts „Eintrittswahrscheinlichkeit“ beschriebenen 4-Stufenmodells bestimmt worden ist.

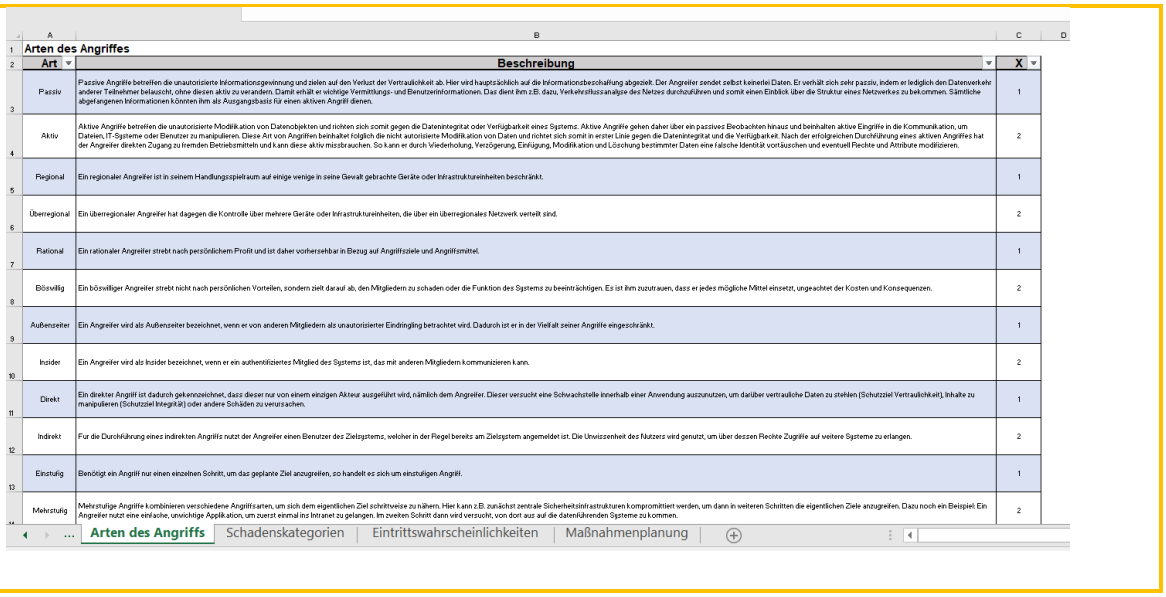
Die Wahrscheinlichkeit des Eintritts eines Ereignisses hängt von der Motivation, den Möglichkeiten und Fähigkeit sowie den Ressourcen des Angreifertyps sowie den implementierten technischen und organisatorischen Maßnahmen ab.

Schließlich kann in die Bewertung auch die öffentliche Meinung mit einfließen, etwa sollte eine sehr hohe Eintrittswahrscheinlichkeit (EW) angenommen werden, wenn davon ausgegangen wird, dass ein Innentäter beim Betrieb ohne weitere besondere Fähigkeiten das Risiko verwirklichen könnte.

Als Hilfestellung und auch zur Nachvollziehbarkeit der Grundlagen der DSFA werden in einem Tabellenblatt der Risiko-Matrix „Angreifertypen und Motive“ dargestellt. Neben den als typisch geltenden Angreifer werden im Rahmen der DSFA auch weitere Akteure betrachtet, denen Angriffszenarien zugetraut werden[33].

Die Angreifer werden Risikoquellen zugeordnet, die wiederum Bedrohungen/Risiken zugeordnet werden und somit eine differenzierte Betrachtung ermöglichen.

Auch werden die Arten von Angriffen beschrieben:



Arten des Angriffes

Art	Beschreibung	X
Passiv	Passive Angriffe betreffen die unautorisierte Informationsgewinnung und zielen auf den Verlust der Vertraulichkeit ab. Hier wird hauptsächlich auf die Informationsbeschaffung abgezielt. Der Angreifer sendet selbst keinerlei Daten. Er verhält sich sehr passiv, indem er lediglich den Datenverkehr anderer Teilnehmer belauscht, ohne diesen aktiv zu verändern. Damit erhält er wichtige Vermittlungs- und Benutzerinformationen. Das dient ihm z.B. dazu, Verkehrsflussanalyse des Netzes durchzuführen und somit einen Einblick über die Struktur eines Netzwerkes zu bekommen. Sämtliche abgefangenen Informationen können ihm als Ausgangsbasis für einen aktiven Angriff dienen.	1
Aktiv	Aktive Angriffe betreffen die unautorisierte Modifikation von Datenobjekten und richten sich somit gegen die Datenintegrität oder Verfügbarkeit eines Systems. Aktive Angriffe gehen daher über ein passives Beobachten hinaus und beinhalten aktive Eingriffe in die Kommunikation, um Dateien, IT-Systeme oder Benutzer zu manipulieren. Diese Art von Angriffen beinhaltet folglich die nicht autorisierte Modifikation von Daten und richtet sich somit in erster Linie gegen die Datenintegrität und die Verfügbarkeit. Nach der erfolgreichen Durchführung eines aktiven Angriffes hat der Angreifer direkten Zugang zu fremden Betriebsmitteln und kann diese aktiv missbrauchen. So kann er durch Wiederholung, Verzögerung, Einfügung, Modifikation und Löschung bestimmter Daten eine falsche Identität vortäuschen und eventuell Rechte und Attribute modifizieren.	2
Regional	Ein regionaler Angreifer ist in seinem Handlungsspielraum auf einige wenige in seine Gewalt gebrachte Geräte oder Infrastruktureinheiten beschränkt.	1
Überregional	Ein überregionaler Angreifer hat dagegen die Kontrolle über mehrere Geräte oder Infrastruktureinheiten, die über ein überregionales Netzwerk verteilt sind.	2
Rational	Ein rationaler Angreifer strebt nach persönlichem Profit und ist daher vorhersehbar in Bezug auf Angriffsziele und Angriffsmittel.	1
Böswillig	Ein böswilliger Angreifer strebt nicht nach persönlichen Vorteilen, sondern zielt darauf ab, den Mitgliedern zu schaden oder die Funktion des Systems zu beeinträchtigen. Es ist ihm zuzutrauen, dass er jedes mögliche Mittel einsetzt, ungeachtet der Kosten und Konsequenzen.	2
Außenseiter	Ein Angreifer wird als Außenseiter bezeichnet, wenn er von anderen Mitgliedern als unautorisierter Eindringling betrachtet wird. Dadurch ist er in der Vielfalt seiner Angriffe eingeschränkt.	1
Insider	Ein Angreifer wird als Insider bezeichnet, wenn er ein authentifiziertes Mitglied des Systems ist, das mit anderen Mitgliedern kommunizieren kann.	2
Direkt	Ein direkter Angriff ist dadurch gekennzeichnet, dass dieser nur von einem einzigen Akteur ausgeführt wird, nämlich dem Angreifer. Dieser versucht eine Schwachstelle innerhalb einer Anwendung auszunutzen, um darüber vertrauliche Daten zu stehlen (Schutzziel Vertraulichkeit), Inhalte zu manipulieren (Schutzziel Integrität) oder andere Schäden zu verursachen.	1
Indirekt	Für die Durchführung eines indirekten Angriffs nutzt der Angreifer einen Benutzer des Zielsystems, welcher in der Regel bereits am Zielsystem angemeldet ist. Die Unwissenheit des Nutzers wird genutzt, um über dessen Rechte Zugriffe auf weitere Systeme zu erlangen.	2
Einstufig	Benötigt ein Angriff nur einen einzelnen Schritt, um das geplante Ziel anzugreifen, so handelt es sich um einstufigen Angriff.	1
Mehrstufig	Mehrstufige Angriffe kombinieren verschiedene Angriffsarten, um sich dem eigentlichen Ziel schrittweise zu nähern. Hier kann z.B. zunächst zentrale Sicherheitsinfrastrukturen kompromittiert werden, um dann in weiteren Schritten die eigentlichen Ziele anzugreifen. Dazu noch ein Beispiel: Ein Angreifer nutzt eine einfache, unwichtige Applikation, um zuerst einmal ins Intranet zu gelangen. Im zweiten Schritt dann wird versucht, von dort aus auf die datenführenden Systeme zu kommen.	2

Arten des Angriffs | Schadenskategorien | Eintrittswahrscheinlichkeiten | Maßnahmenplanung

Abbildung 25: Risiko-Matrix

[33] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), Datenschutz-Folgenabschätzung für die Corona App, Version 1.6, abrufbar unter: https://www.fiff.de/dsfa-corona , S. 69 i.V.m. den Ausführungen zu „Akteuren“ auf S. 19 ff.

12.4 Bewertung der Schadenshöhe

In der Risikotabelle ist vorgesehen, dass der potentielle Schaden für Betroffene anhand der zu betrachtenden Gewährleistungsziele Datenminimierung, Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Resilienz, Intervenierbarkeit, Transparenz, Zweckbindung/ Nichtverkettung geschätzt wird:

Schutzziel	Definition
Datenminimierung	Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Hierzu gehört auch die Speicherbegrenzung / Löschung nach Zweckerreichung oder -wegfall.
Vertraulichkeit	Personenbezogene Daten dürfen nur einem berechtigten Personenkreis für bestimmte Zwecke offenbar werden. Sie sind vor unbefugter Veränderung zu schützen.
Integrität	Integrität von Daten ist die Abwesenheit von korrumpierten Daten. Integrität bedeutet insbesondere die Abwesenheit unautorisierter Veränderungen.
Verfügbarkeit	Verfügbarkeit von Informationen und Systemen ist Zugreifbarkeit und Nutzbarkeit durch autorisierte Entitäten bei Bedarf.
Authentizität	Authentizität bedeutet, dass die Daten tatsächlich von der Quelle kommen, die angegeben wird; also weder Fälschung noch Fehlzuschreibung.
Resilienz	Resilienz bezeichnet die Fähigkeit Störungen ohne anhaltende Belastungen zu überwinden.
Intervenierbarkeit	Betroffene müssen die Möglichkeit haben, ihre entsprechend der DSGVO gewährten Rechte ungehindert auszuüben. Datenverarbeitungen müssen so gestaltet werden, dass Daten berichtigt und gelöscht werden können.
Transparenz	Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise erhoben und verarbeitet werden.
Zweckbindung/ Nichtverkettung	Personenbezogene Daten sind nur im Rahmen des ursprünglichen Zweckes der Verarbeitung zu verwenden und nicht mit anderen Daten zusammenzuführen. Dementsprechend

	darf im Laufe der Verarbeitungsprozesse stets nur der ursprünglich festgelegte Zweck verfolgt werden.

Es wird geprüft inwiefern Bedrohungen/ Ereignisse zum Eintritt eines physischen, materiellen oder immateriellen Schadens für den Betroffenen führen können. Für jedes Szenario wird dabei geprüft, welche Gewährleistungsziele tangiert sind.

Für die einzelnen Schutzziele wird im Risikoregister die potenzielle Schadenshöhe in Kategorie 1-gering, Kategorie 2- begrenzt, Kategorie 3 – hoch und Kategorie 4 – sehr hoch anhand des Tabellenblattes „Schadenskategorien“ in der Risikomatrix bestimmt.

Das Tabellenblatt ist individuell anpassbar. Die Schadenskategorien wurden wie folgt definiert:

		Schadensausmaß			
		Gering (1)	Begrenzt / mittel (2)	Hoch (3)	Sehr Hoch (4)
Schadenszenarien	**Gesellschaftliche und soziale Nachteile** (Rufschädigungen, Ansehensverluste)	Kein oder unbedeutender Verstoß	geringfügige, vorübergehende Peinlichkeit	Verstöße erheblichen Konsequenzen Beschneidung gesellschaftlicher Teilhabe, Mobbing, erheblicher Gesichtsverlust, aber mit Anstrengungen überwindbar	Fundamentaler Verstoß gegen Vorschriften und Gesetze gesellschaftliche Diskriminierung, schwere öffentliche Bloßstellung mit fundamentalen, irreparablen Folgen
	Einschüchterungseffekt (aus Angst vor negativen Folgen zieht Betroffener davon ab Rechte auszuüben oder sich persönlich zu entfalten (z.B. Besuch von pol./ kulturellen Veranstaltungen)	Keine oder unbedeutende Auswirkung	Eine geringe Betroffenheit bzw. nur örtlich und zeitlich begrenzter Einschüchterungseffekt ist zu erwarten	Ein umfassender Einschüchterungseffekt ist zu erwarten (Umfang, Zeit, Ort), aber jeweils durch Maßnahmen (Befristigung, Lokalisation..) überwindbar	Ein erheblicher, dauernder und örtlich nicht mehr begrenzbarer Einschüchterungseffekt, eventuell sogar existengefährdender Art, ist denkbar.
	Schädigung der Privatsphäre (Verlust der Kontrolle über eigene Daten, Überwachung, Veröffentlichung von pD, inkl.Infektionsstatus, Quarantäne) und **Verletzung weiterer (Grund-)rechte** (Meinungsfreiheit, Anti-Diskriminierung)	Keine oder unbedeutende Beeinträchtigung	Erheblich, überwindbar	Erhebliche Auswirkungen, überwindbar mit ernstzunehmenden Schwierigkeiten	Erhebliche bis irreversible Folgen, nicht überwindbar
	Beeinträchtigung der persönlichen Unversehrtheit (falsche medizinische Behandlung, Vorschubleisten für Gewaltverbrechen)	Keine oder unbedeutende Beeinträchtigung	Tolerable Beeinträchtigungen	Wesentliche, intolerable Beeinträchtigung, die Maßnahmen erfordert (Personenschutz, Therapie)	Akute Gefahr für Leib und Leben
	Beeinträchtigung der Aufgabenerfüllung Zielerreichung der CWA	Keine oder unbedeutende Beeinträchtigung	Tolerable Beeinträchtigungen (kritische Masse an Nutzern vorhanden)	Wesentliche Beeinträchtigung / nicht-nur kurzfristiger Akzeptanzverlust von mehr als ### Prozent der Nutzer, die Maßnahmen zur Akzeptanzerhöhung erfordern	Akzeptanzverlust der App sinkt nicht nur kurzfristig auf ###/ Komplettausfall
	wirtschaftliche Auswirkungen / materielle Schäden (Jobverlust durch berufliche Nachteile durch Leistungs- und Verhaltenskontrolle, Beschneidung staatlicher Leistungen, höhere KV-Beiträge)	≤ 1.000.000 l	finanzielle Verluste bis zu 100 EUR	Verluste bis zu 3 Netto-Monatsgehältern, bis 5.000 EUR oder Beeinträchtigung von Karriere-Chancen	verlust oder langfristiger Verlust von Karriere-Chancen, > drei Netto-Monatsgehälter, 5.000 E

Abbildung 26: Schadensausmaß

Es handelt sich um eine qualitative Bewertung der jeweiligen Bedrohungen bezogen auf das jeweilige Schutzziel/ Gewährleistungsziel. Dabei ist die Tabelle lediglich ein Hilfsmittel; die qualitative Bewertung kann unabhängig von der Risikozahl sowohl grundsätzlich als auch für bestimmte Aspekte ergänzend im DSFA-Bericht und in mitgeltenden Dokumenten beschrieben werden. Dies wird insbesondere für Themen der Einwilligung in die Datenverarbeitung empfohlen, da die Risiken für Betroffene nicht auf einzelne Schutzziele wirken, vielmehr grundsätzliche Fragen der Rechtmäßigkeit der Datenverarbeitung und Akzeptanz betreffen.

Die folgende Abbildung zeigt die Klassifizierung der Risiken und enthält gleichzeitig einen Vorschlag für die Priorisierung durch Ampelfarben. Automatisch wird in der Risikomatrix aus Eintrittswahrscheinlichkeit x Schadenshöhe eine Risikoklasse gebildet, wobei das Produkt mit der höchsten Schadenszahl gebildet wird.

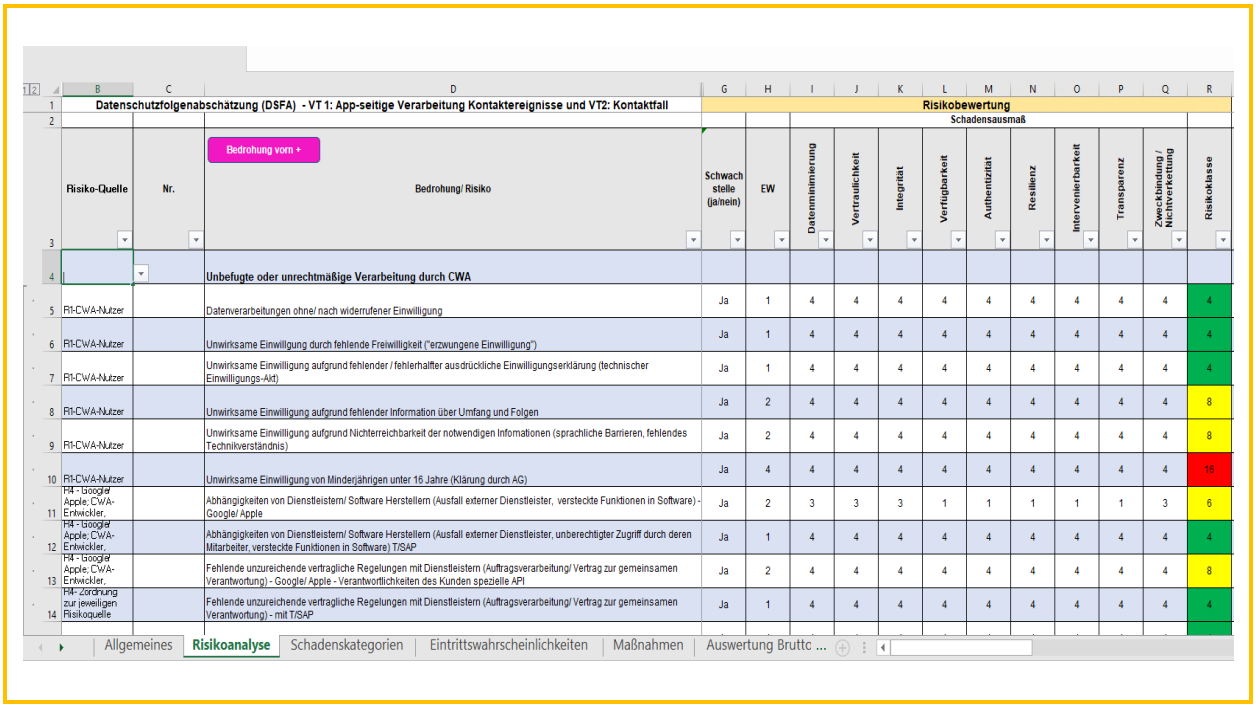
Kategorie	**Risikoklasse**	**Beschreibung**
Niedrig	0-4	Die Auswirkungen des Schadens für Betroffene sind begrenzt und beherrschbar. Das Eintreten einer zu berücksichtigten Schadenssituation erscheint unmöglich.
Mittel	5-7	Der Schadenseffekt wäre nennenswert. Technische und organisatorische Maßnahmen SOLLEN vorgeschlagen werden. Als Teil der Kosten-Nutzen-Abwägung der notwendigen Maßnahmen kann das Risiko akzeptiert werden.
	8-10	Signifikante Schäden können nicht komplett ausgeschlossen werden, aber eine existenzbedrohende Situation erscheint unwahrscheinlich. TOM MÜSSEN vorgeschlagen und innerhalb einer festgelegten Frist umgesetzt werden (siehe hierzu Tabellenblatt „Maßnahmenplanung“). Die Reduktion von Risiken durch TOM und/ oder Kontrollen ist notwendig. Eine Risikoakzeptanz basierend auf einer Kosten-Nutzen-Betrachtung der geplanten Handlungen bedarf einer besonderen Managementbetrachtung. Die Datenschutz-Aufsichtsbehörde SOLL konsultiert werden.
Hoch	11-16	Schadenseffekte können katastrophale oder existenzbedrohende Ausmaße annehmen. Das Eintreten des Risikos hat signifikante negative Auswirkungen. Dieses Risiko bedarf sofortiger Aufmerksamkeit. Eine Akzeptanz dieses Risikos ist ausgeschlossen. Eine Reduktion des Risikos durch hierauf abgestimmte TOM ist notwendig; die Berücksichtigung systematischer und strategischer Maßnahmen wird empfohlen. Die Datenschutz-Aufsichtsbehörde MUSS konsultiert werden.

Einer Anforderung der Auftraggeber folgend können in der Risikomatrix Maßnahmen aus dem Katalog der Referenzmaßnahmen des Standard-Datenschutz-Modells (SDM) zugeordnet werden, die im Tabellenblatt Maßnahmen hinterlegt sind. Nach SDM werden jedem Gewährleistungsziel spezifische technische und organisatorische Abhilfemaßnahmen zugeordnet, mittels derer das Ziel und die dahinter stehenden Anforderungen der DSGVO gewährleistet und der Eintritt des Schadensereignisses verhindert werden kann.

Die Bewertung der Risiken erfolgt auf Basis der etablierten Schutzmaßnahmen und Designentscheidungen. Die Risikomatrix ist generell auf die Durchführung einer Brutto-Risikobetrachtung (ohne Maßnahmen) und einer Netto-Risikobetrachtung (nach Maßnahmenergreifung) angelegt.

Für die Bewertung wird auf die konkreten Risiko-Matrizen der Verarbeitungstätigkeiten verwiesen, die als Anlagen zu diesem DSFA-Bericht beigefügt sind.

Beispielhaft anbei ein Screenshot (Änderungen vorbehalten!) und ohne Anspruch auf Richtigkeit und Vollständigkeit zur Veranschaulichung der Ergebnisse:



	B	C	D	G	H	I	J	K	L	M	N	O	P	Q	R
1	Datenschutzfolgenabschätzung (DSFA) - VT 1: App-seitige Verarbeitung Kontaktereignisse und VT2: Kontaktfall			Risikobewertung											
2						Schadensausmaß									
3	Risiko-Quelle	Nr.	Bedrohung vorn + Bedrohung/ Risiko	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse
4			Unbefugte oder unrechtmäßige Verarbeitung durch CWA												
5	R1-CWA-Nutzer		Datenverarbeitungen ohne/ nach widerrufener Einwilligung	Ja	1	4	4	4	4	4	4	4	4	4	4
6	R1-CWA-Nutzer		Unwirksame Einwilligung durch fehlende Freiwilligkeit ("erzwungene Einwilligung")	Ja	1	4	4	4	4	4	4	4	4	4	4
7	R1-CWA-Nutzer		Unwirksame Einwilligung aufgrund fehlender / fehlerhaffter ausdrückliche Einwilligungserklärung (technischer Einwilligungs-Akt)	Ja	1	4	4	4	4	4	4	4	4	4	4
8	R1-CWA-Nutzer		Unwirksame Einwilligung aufgrund fehlender Information über Umfang und Folgen	Ja	2	4	4	4	4	4	4	4	4	4	8
9	R1-CWA-Nutzer		Unwirksame Einwilligung aufgrund Nichterreichbarkeit der notwendigen Infomationen (sprachliche Barrieren, fehlendes Technikverständnis)	Ja	2	4	4	4	4	4	4	4	4	4	8
10	R1-CWA-Nutzer		Unwirksame Einwilligung von Minderjährigen unter 16 Jahre (Klärung durch AG)	Ja	4	4	4	4	4	4	4	4	4	4	16
11	R4 - Google/ Apple; CWA-Entwickler,		Abhängigkeiten von Dienstleistern/ Software Herstellern (Ausfall externer Dienstleister, versteckte Funktionen in Software) - Google/ Apple	Ja	2	3	3	3	1	1	1	1	1	3	6
12	R4 - Google/ Apple; CWA-Entwickler,		Abhängigkeiten von Dienstleistern/ Software Herstellern (Ausfall externer Dienstleister, unberechtigter Zugriff durch deren Mitarbeiter, versteckte Funktionen in Software) T/SAP	Ja	1	4	4	4	4	4	4	4	4	4	4
13	R4 - Google/ Apple; CWA-Entwickler,		Fehlende unzureichende vertragliche Regelungen mit Dienstleistern (Auftragsverarbeitung/ Vertrag zur gemeinsamen Verantwortung) - Google/ Apple - Verantwortlichkeiten des Kunden spezielle API	Ja	2	4	4	4	4	4	4	4	4	4	8
14	R4- Zordnung zur jeweiligen Risikoquelle		Fehlende unzureichende vertragliche Regelungen mit Dienstleistern (Auftragsverarbeitung/ Vertrag zur gemeinsamen Verantwortung) - mit T/SAP	Ja	1	4	4	4	4	4	4	4	4	4	4

Allgemeines | Risikoanalyse | Schadenskategorien | Eintrittswahrscheinlichkeiten | Maßnahmen | Auswertung Brutto ...

Abbildung 27: Risikoanalyse

12.5 Risikobehandlung/Risikominimierung/Maßnahmenkatalog

Die Maßnahmen zur Risikobehandlung/-minimierung werden in den Risiko-Matrizen der Verarbeitungstätigkeiten aufgeführt, die als Anlagen 3, 4 und 5 diesem Bericht beigefügt sind. Ergänzend wird auf das Dokument Designentscheidungen (Anlage 1) Bezug genommen.

Nachfolgend werden wichtige Maßnahmen aufgeführt, die getroffen wurden, um das Risiko für die von der Datenverarbeitung Betroffenen zu minimieren. Darüber hinaus fließen notwendige

Maßnahmen in die technisch-organisatorischen Maßnahmen mit ein (siehe Anlage 2). Die technisch-organisatorischen Maßnahmen wurden an den Vorgaben des BSI ausgerichtet.

1. Einsatz von Pseudonymen, wo möglich,
2. Trennung von Teilprozessen durch verschiedene Server (CWA-Server, Verification Server, Lab Server),
3. Berechtigungskonzept(e) und der Autorisierungsprozess für (Server-)komponenten beschränken den berechtigten Zugriff auf die pD,
4. Eine elektronische Übertragung von Daten erfolgt verschlüsselt. Die Speicherung der Daten auf Servern und im ENF erfolgt verschlüsselt,
5. Betriebs-, Sicherheits- und Datenschutzkonzepte für die Komponenten gewährleisten eine Minimierung von Ausfallzeiten und die Erfüllung von Sicherheits- und Datenschutzanforderungen.
6. Etablierung eines DSMS (PDCA-Zyklus)

Eine detaillierte Betrachtung der Risiken ist in den Risikomatrizen (Anlagen 3, 4 und 5) sowie in den Designentscheidungen (Anlage 1) erfolgt.

12.6 Bewertung von hohen Restrisiken

Die Risiken wurden ausführlich im Rahmen der Durchführung der DSFA behandelt und in den Risikomatrizen und dem Dokument Designentscheidungen dokumentiert.

Die vollständige Benennung und Dokumentation der Bewertung sämtlicher identifizierten Risiken im Rahmen der Risikoanalyse wird in den Risikomatrizen dargestellt.

Die identifizierten Restrisiken wurden mit dem BfDI und BMG diskutiert und können insgesamt akzeptiert werden.

Nachfolgend werden in zusammengefasster Form die im Rahmen der Risikoanalyse identifizierten hohen Restrisiken, die akzeptiert werden können, ergänzend zu den Designentscheidungen, den Risikomatrizen und den Datenschutzkonzepten datenschutzrechtlich betrachtet.

Aus der Sicht des DSFA-Teams wurden seitens des RKI bis zum Abschluss des Prüfungszeitraums dieser DSFA angemessene Maßnahmen zur Eindämmung hoher Restrisiken umgesetzt bzw. vorbereitet, so dass sie zurzeit akzeptiert werden dürfen (Risikoakzeptanz).

Das RKI muss jedoch fortlaufend beobachten, ob Umstände eintreten, die eine Neubewertung der Ergebnisse der Risikoanalyse notwendig erscheinen lassen.

12.6.1 Risiken durch die Verwendung von Dritt-Technologien

→ Risiko-Matrix VT 1, 2, 4, dort Zeilen 17, 39, 40, 56, 98, 111, 112, 130

Der Umstand, dass die CWA App die Konnektivitäten und das ENF von Google und Apple verwendet, stellt ein erhebliches Risiko dar, welches durch das RKI jedoch praktisch nicht beseitigt und auf technischer Ebene auch nicht reduziert werden kann. Gleiches gilt hinsichtlich des Angewiesenseins der CWA App auf den internationalen BLE-Standard sowie die Hardwarekomponenten des Smartphones, die sich außerhalb des Wirkbereichs des RKI befinden.

Die genaue technische Umsetzung und Funktionsweise aller betriebssystem- und hardwareseitigen Funktionalitäten ist der Kontrolle des RKI entzogen. Es ist anzunehmen, dass Apple und Google durch eine Änderung des ENF auch zur Verknüpfung der dort verarbeiteten Tagesschlüssel und RPIs mit einer geräte- (z. B. Werbe-ID) oder nutzerspezifischen Kennung (z. B. Apple-ID oder Google-Konto) in der Lage sind. Derartige Risiken bestehen allerdings bei jeder Drittanbieter-App, die Schnittstellen eines Betriebssystems oder technische Komponenten des Smartphones nutzt. Allerdings haben die Nutzer durch die Verwendung eines Android- bzw. iOS-Smartphones zum Ausdruck gebracht, 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 (z. B. durch Deaktivierung der Ortungsdienste). Gleiches gilt für den Einsatz von BLE. Es ist damit zu rechnen, dass die Technologie auch bisher nicht bekannte Schwachstellen aufweist, die zu Fehlern oder zur Ermöglichung einer unbefugten Datenverarbeitung hinsichtlich der Daten der CWA ausgenutzt werden können. Derartige Risiken, die auf die nicht vermeidbare Abhängigkeit der CWA von Dritt-Technologien und teilweise auch auf die individuelle Nutzungsverhalten des Nutzers zurückgehen, müssen und dürfen daher – soweit sie vom RKI nicht durch angemessene Maßnahmen reduziert werden können – hingenommen werden. Andernfalls wären die CWA oder andere von Dritt-Technologie abhängige staatliche Angebote nicht realisierbar.

12.6.2 Risiken durch Verhalten oder Technikfehler auf Seiten des Nutzers

→ Risiko-Matrix VT 1, 2, 4, dort Zeile 85

Risiken, die auf Fehlbedienungen, nicht ordnungsgemäßes oder nicht sachgerechtes Nutzungsverhalten des Nutzers (z. B. ungünstige Konfigurationseinstellungen, Unterlassen von Sicherheitsupdates) sowie auf Technikfehler (z. B. Defekt der Bluetooth-Komponente des Smartphones) zurückzuführen sind, können vom Anbieter einer App naturgemäß nicht ausgeschlossen werden. Sie müssen und dürfen daher – soweit sie vom RKI nicht durch angemessene Maßnahmen weiter reduziert werden können – hingenommen werden. Andernfalls wären die CWA oder andere von Dritt-Technologie abhängige staatliche Angebote nicht realisierbar.

12.6.3 Risiken durch den Einsatz von Auftragsverarbeitern

→ Risiko-Matrix VT 1, 2, 4, dort Zeile 85 und 131

In der Risikoanalyse wird das Risiko durch Herausgabeverlangen seitens Strafverfolgungsbehörden als hoch eingeordnet. Diesem Risiko wird begegnet, indem für den Fall von Anfragen seitens Strafverfolgungsbehörden ein organisatorischer Prozess etabliert wird, der die Überprüfung des Vorliegens einer tragenden Rechtsgrundlage für das Herausgabeverlangen juristisch sicherstellt. Mit der Telekom wurde zudem ein Auftragsverarbeitungsvertrag abgeschlossen, der die Verarbeitung von Daten ausschließlich zu Zwecken des Prüfgegenstands vorgibt, soweit eine abweichende Datenverarbeitung nicht gesetzlich verpflichtend vorgeschrieben ist. „Nicht vom RKI beauftragte Datenverarbeitungen" sind dadurch ausgeschlossen.

Durch den Einsatz von Auftragsverarbeiten wird zwangsläufig ein Datenschutzrisiko geschaffen; es handelt sich nicht um ein CWA-spezifisches Risiko. Sofern der Verantwortliche die beauftragte Datenverarbeitung nicht selbst durchführen kann und das Gesetz kein Verbot der Auftragsverarbeitung vorsieht, ist der Einsatz von Auftragsverarbeiten prinzipiell zulässig, sofern sich das dadurch geschaffene Risiko gegenüber dem Interesse an der Datenverarbeitung nicht als unverhältnismäßig darstellt bzw. dem Verantwortlichen oder den Betroffenen der Verzicht auf die Datenverarbeitung nicht zugemutet werden kann.

Die Grundsatzentscheidung zur Nutzung der IT-Infrastruktur eines Auftragsverarbeiters bedarf daher des berechtigten Vertrauens des Verantwortlichen. Ebenso muss sichergestellt sein, dass die Betroffenen das Risiko durch die Beauftragung eines Auftragsverarbeiters zutreffend einschätzen können.

Sofern dies im Fall der CWA gewährleistet ist, darf das verbleibende Restrisiko, soweit es vom RKI nicht durch angemessene Maßnahmen weiter reduziert werden kann – hingenommen werden.

12.6.4 Risiken durch Cyberkriminalität / Sabotageversuche

→ Risiko-Matrix VT 1, 2, 4, dort Zeile 124

→ Risiko-Matrix VT Verification Hotline, dort Zeilen 8, 15

Risiken, die durch Angriffe von Cyberkriminellen (z. B. Hackerangriffe, die sich gegen Serversysteme der CWA oder Schwachstellen der CWA App) oder Gegnern der CWA (z. B. durch Versuche, die Akzeptanz der CWA App durch Verursachen von Fehlalarmen zu schädigen) ausgehen, können von einem Anbieter eines Dienstes naturgemäß nicht ausgeschlossen werden. Sie müssen und dürfen daher – soweit sie vom RKI nicht durch angemessene Maßnahmen weiter reduziert werden können – hingenommen werden. Andernfalls wären die CWA oder andere von Dritt-Technologie abhängige staatliche Angebote nicht realisierbar.

12.6.5 Risiken für Minderjährige

→ Risiko-Matrix VT 1, 2, 4, dort Zeile 10

→ Risiko-Matrix VT 3, dort Zeile 10

Die CWA App erhebt keine Daten zum Alter des Nutzers, eine spezifische Einwilligung für Minderjährige ist deshalb nicht vorgesehen. Aus diesem Grund kann nicht ausgeschlossen werden, dass sich Jugendliche unter 16 Jahren entgegen dieser Vorgabe die CWA App trotzdem herunterladen und nutzen, ohne dass eine Einwilligung eines Sorgeberechtigen vorliegt. Das RKI hat faktisch keine Möglichkeit, dies zu verhindern. Es kann nur gezielt in der Veröffentlichungsphase und auch nach Veröffentlichung der CWA App darauf hinwirken, dass in der Öffentlichkeit ein Bewusstsein über diese Altersgrenzen herrscht, um einer Nutzung durch unter 16-jährige Personen entgegenzuwirken.

Ein Verstoß gegen die Altersbeschränkung führt jedoch nicht zwangsläufig zur Unwirksamkeit der Einwilligung und birgt insoweit nicht zwangsläufig das Risiko einer rechtswidrigen Datenverarbeitung.

Das Risiko muss und darf – soweit es vom RKI nicht durch angemessene Maßnahmen weiter reduziert werden kann – hingenommen werden. Andernfalls wäre die CWA nicht in der vorgesehenen einwilligungsbasierten Form realisierbar.

12.6.6 Risiken durch Fehlfunktionen oder Unwirksamkeit der CWA App

→ Risiko-Matrix VT 1, 2, 4, dort Zeilen 22, 97, 98, 134

Der Einsatz einer Tracing-App zur Bekämpfung einer Virus-Pandemie ist technisches „Neuland“. Daher können Risiken, durch nach Einführung der CWA erkannte Fehlfunktionen oder fehlende epidemiologische Wirksamkeit der CWA App naturgemäß nicht ausgeschlossen werden.

Das Risiko muss und darf – soweit es vom RKI nicht durch angemessene Maßnahmen weiter reduziert werden kann – hingenommen werden. Andernfalls wäre die CWA nicht realisierbar.

12.6.7 Risiken durch missbräuchliche Nutzung des Hotline-Verfahrens

→ Risiko-Matrix VT 3, dort Zeile 8

Der Einsatz der Verifikationshotline dient als flankierende Maßnahme zum digitalen Prozess (QR-Code Verfahren), um eine möglichst breite Wirksamkeit der CWA zu gewährleisten und auch CWA Nutzern, die über keinen QR-Code verfügen oder diesen verloren haben, eine

Meldung des positiven Testergebnisses, zu ermöglichen. Ziel ist es allerdings die Labore schnellstmöglich an den digitalen Prozess (QR-Code Verfahren) anzuschließen.

Bis alle Labore angeschlossen sind, wird die Verifikationshotline erforderlich sein, um eine möglichst hohe Nutzbarkeit der CWA App zu gewährleisten und damit auch eine hohe Wirksamkeit, mit dem Ziel, die Ansteckungsketten schneller zu unterbinden. Vorschläge zur datenschutzfreundlichen Ausgestaltung der Verifikationshotline wurden aufgegriffen und insbesondere im Hinblick auf maximale Datensparsamkeit umgesetzt. Auch die Plausibilitätsfragen wurden entsprechend angepasst. Für den Fall eines konkreten Verdachts auf Missbrauch der Verifikationshotline wurden bereits mit dem BfDI vorsorglich weitere Schritte vorbereitet, um einem konkreten Verdacht missbräuchlicher Nutzung zügig zu begegnen.

Zugleich geht die Verifikations-Hotline mit einem Missbrauchspotential einher, wenn diese gewollte oder ungewollte Rechtsfolgen für Einzelne oder Gruppen entfalten sollte. Die derzeit getroffenen Maßnahmen (Plausibilisierungsfragen und Rückruf des infizierten Nutzers) reduzieren dieses Risiko zwar, bieten jedoch gegen versierte Angreifer keinen hundertprozentigen Schutz. Der Missbrauch könnte 1. erhebliche Auswirkungen auf die Rechte und Freiheiten anderer Nutzer haben, die falsche Risiko-Benachrichtigungen erhalten könnten; 2. das öffentliche Leben beeinträchtigen, wenn beispielsweise Einrichtungen aufgrund falscher Risiko-Benachrichtigungen schließen müssten und 3. die Wirksamkeit der CWA App in Frage stellen, wenn sich das Missbrauchspotenzial auf die Akzeptanz der CWA-App in der Bevölkerung auswirken würde. Durch die Handlungsempfehlungen, insbesondere der Empfehlung sich testen zu lassen, werden diese Risiken reduziert. Die rechtsrelevanten Entscheidungen werden allerdings nicht über die CWA sondern durch die Gesundheitsämter und Ärzte getroffen.

Das Risiko muss und darf – soweit es vom RKI nicht durch angemessene Maßnahmen weiter reduziert werden kann – hingenommen werden. Andernfalls wäre die CWA zum jetzigen Zeitpunkt nicht realisierbar.

13 Nachhaltige Sicherung des Datenschutzes

In regelmäßigen Abständen müssen Kernelemente des Datenschutzes im Rahmen eines wirksam Datenschutzmanagements überprüft werden.

13.1 Evaluierung

Sollte das Ziel der Anwendung der CWA App nicht mehr gegeben sein, also die Corona Pandemie am Abflauen sein, so müssen die Experten des RKI entscheiden, ob die CWA App außer Betrieb genommen werden kann oder weiterhin aufrechterhalten werden muss, weil mit einer bevorstehenden weiteren Welle der Pandemie zu rechnen ist (z.B. auf Grund der Lage in Nachbarländern).

Zur Vorbereitung der zuvor genannten Entscheidung ist eine regelmäßige Evaluierung der Corona Pandemie Lage durch das RKI erforderlich. Eine erstmalige Evaluierung wird spätestens im ersten Quartal 2021 erfolgen. Bis zu diesem Termin wird dringend empfohlen festzulegen, in welchen weiteren Zyklen eine Evaluierung der Gesamtlage der Corona Pandemie und somit des Betriebs der CWA App erfolgt und welche Kriterien hierzu herangezogen werden.

Die eingesetzte BLE Technologie und Ihre Genauigkeit im Rahmen der Kontaktberechnung ist fortlaufend, regelmäßigen sowie anlassbezogen zu evaluieren.

Die vorstehend beschriebenen Missbrauchsrisiken der Verifikations-Hotline sind ebenfalls fortlaufend, regelmäßigen sowie anlassbezogen zu evaluieren.

13.2 Entscheidung bzgl. Information Aufsichtsbehörde

Die Konsultation der Aufsichtsbehörde nach Art. 36 Abs. 1 DSGVO

☒ ist auf Grund des Ergebnisses der DSFA und der Tatsache, dass die Verarbeitungstätigkeit trotz des Ergebnisses durchgeführt werden soll, notwendig.

☐ ist nicht notwendig, da die Verarbeitungstätigkeit auf Grund des Ergebnisses der DSFA nicht durchgeführt wird.

☐ ist nicht notwendig, weil entsprechende Maßnahmen zur Eindämmung des Risikos getroffen wurden.

13.3 Nächster Prüfungstermin

Die nächste Prüfung erfolgt spätestens innerhalb von 3 Monaten nach Freigabe der CWA.

Anlagen

Anlage 1: Designentscheidungen der CWA der Bundesrepublik Deutschland
(V 1.2, Stand: 13.06.2020)

Anlage 2: Technisch-Organisatorische Maßnahmen
(V 1.1, Stand: 10.06.2020)

Anlage 3: Risikomatrix CWA DSFA VT 1_2_4

Anlage 4: Risikomatrix CWA DSFA VT 3_Testing End

Anlage 5: Risikomatrix CWA DSFA_Verification Hotline