

CORONA WARN-APP

**Bericht zur Datenschutz-Folgenabschätzung für die
Corona-Warn-App
der Bundesrepublik Deutschland
Öffentliche Version**

1 Vorausgehende Hinweise

Dieses Dokument enthält die Version 1.1 des Berichts zur Datenschutz-Folgenabschätzung (DSFA)¹ für die **Corona-Warn-App** (CWA), die seit dem 16.06.2020 vom Robert Koch-Institut (RKI) im Auftrag der deutschen Bundesregierung herausgegeben wird.

Die DSFA wird laufend überprüft, um zu bewerten, ob die wesentlichen bisherigen Ergebnisse weiterhin gültig sind oder eine Aktualisierung erforderlich ist. Eine Aktualisierung der DSFA ist jedenfalls dann erforderlich, wenn geänderte technische oder rechtliche Rahmenbedingungen, neue Erkenntnisse oder geplante Änderungen der CWA (z. B. Funktionserweiterungen) zu einer geänderten Risikobewertung führen können. Daher handelt es sich bei dem vorliegenden DSFA-Bericht um ein „lebendiges Dokument“, das von Zeit zu Zeit aktualisiert und in einer neuen Version zur Verfügung gestellt wird.

In diesem DSFA-Bericht wird ausschließlich aus Gründen der leichteren Lesbarkeit auf eine geschlechtsspezifisch differenzierende Verwendung von juristischen und technischen Fachbegriffen verzichtet (z. B. „Nutzer“, „Angreifer“). Selbstverständlich bezieht sich der jeweilige Begriff auf Personen jeglichen Geschlechts.

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

Änderungshistorie

Änderung			Beschreibung der Änderung	Freigabe	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	15.06.2020	Final
3	18.06.2020	1.0.1	Beseitigung Tippfehler	15.06.2020	Final
4	16.10.2020	1.1	Klarstellungen, Berücksichtigung der neuen Funktionen des App-Releases V. 1.5		

2 Inhalt

1	Vorausgehende Hinweise	2
2	Inhalt	4
3	Über diesen DSFA-Bericht.....	8
3.1	Einleitung	8
3.2	Name und Kontaktdaten des Verantwortlichen	10
3.3	DSFA-Team.....	10
3.3.1	Rolle	10
3.3.2	Zusammensetzung und Vorgehen	10
3.4	Glossar	11
3.5	Abkürzungsverzeichnis.....	12
4	Notwendigkeit der DSFA.....	14
5	Beschreibung der CWA (Prüfgegenstand).....	15
5.1	Hintergrund und Historie.....	15
5.2	Anwendungsphasen und Funktionen der CWA.....	17
5.3	Zwecke der Datenverarbeitung.....	17
5.4	Ablauf aus Sicht eines CWA-Nutzers	18
5.4.1	Download und Installation der CWA App	18
5.4.2	Start der CWA App	19
5.4.3	Home-Bildschirm	20
5.4.4	Risiko-Ermittlung	20
5.4.5	Risikodetails und Risikostufen.....	21
5.4.6	Testregistrierung.....	22
5.4.7	Verifikations-Hotline.....	23
5.4.8	Warnfunktion	24
5.4.9	Sonstige Funktionen.....	26
5.5	Systemarchitektur	27
5.5.1	Smartphone (Mobiles Endgerät).....	28
5.5.2	CWA Server.....	29
5.5.3	CDN-Magenta (Content Delivery Network)	29
5.5.4	Verifikationsserver	30
5.5.5	Portalserver	30
5.5.6	Test Result Server.....	31
5.5.7	European Federation Gateway Service (EFGS)	31

5.6	Datenflüsse und Prozesse	33
5.6.1	Anwendungsphase 1: Risiko-Ermittlung	33
5.6.2	Anwendungsphase 2: Berechnung des Infektionsrisikos	36
5.6.3	Anwendungsphase 3: Testregistrierung	37
5.6.4	Anwendungsphasen 3-4: Verifikations-Hotline	39
5.6.5	Anwendungsphase 4: Andere warnen.....	40
5.6.6	Deinstallation der CWA App	45
5.7	Kategorien von Daten	45
5.7.1	Zugriffsdaten.....	46
5.7.2	Tagesschlüssel (TEK)	46
5.7.3	RPI.....	47
5.7.4	RPI-Metadaten	48
5.7.5	Positivschlüssel (Diagnoseschlüssel).....	48
5.7.6	Metadaten zu Positivschlüsseln	48
5.7.7	Bewertungseinstellungen (BWE).....	49
5.7.8	TANs.....	50
5.7.9	Registration Token	50
5.7.10	QR-Code / GUID	50
5.7.11	Risikowert (Total Risk Score)	50
5.7.12	Risikostatus	51
5.7.13	Name und Telefonnummer (Verifikations-Hotline)	52
5.7.14	Antworten auf Plausibilitätsfragen (Verifikations-Hotline).....	52
5.8	Lösung der Daten	52
5.8.1	Lösung der im Rahmen der Risiko-Ermittlung und Berechnung des Infektionsrisikos verarbeiteten Daten.....	52
5.8.2	Lösung der im Rahmen der Testregistrierung verarbeiteten Daten.....	53
5.8.3	Lösung der im Rahmen der Warnfunktion verarbeiteten Daten	53
5.8.4	Lösung der Zugriffsdaten.....	54
5.9	An der Datenverarbeitung beteiligte Akteure	54
5.9.1	Betroffene Personen.....	54
5.9.2	Verantwortliche	54
5.9.3	Weitere Akteure	55
5.9.4	Auftragsverarbeiter	56
5.9.5	Betrieb des EFGS.....	57

5.10	Begleitdokumente zur Beschreibung der geplanten Verarbeitungsvorgänge (Prüfgegenstand).....	57
6	Einholung des Standpunktes der betroffenen Personen	58
7	Datenschutzrechtliche Bewertung	59
7.1	Umfang der Verarbeitung personenbezogener Daten.....	59
7.1.1	Personenbezogene Daten.....	59
7.1.2	Lokale Datenverarbeitung auf dem Smartphone.....	61
7.1.3	Gesundheitsdaten	62
7.2	Rechtsgrundlagen.....	63
7.2.1	Anforderungen an eine Rechtsgrundlage.....	64
7.2.2	Rechtsgrundlagen der CWA.....	65
7.2.3	Begründung der Einwilligung als Rechtsgrundlage	65
7.3	Betroffenenrechte	77
7.3.1	Rechte der CWA-Nutzer.....	77
7.3.2	Rechte anderer Nutzer	80
7.4	Privacy-by-Design-Maßnahmen	80
7.5	Weitere datenschutzrechtliche Anforderungen	81
8	Bewertung der Notwendigkeit und Verhältnismäßigkeit in Bezug auf die Zwecke	83
8.1	Zweck 1 (länderübergreifende Risiko-Ermittlung und Warnung)	83
8.1.1	Legitimer Zweck	83
8.1.2	Eignung	83
8.1.3	Erforderlichkeit.....	85
8.1.4	Angemessenheit.....	86
8.2	Zweck 2 (Testergebnisabruf)	89
8.2.1	Legitimer Zweck	89
8.2.2	Eignung	90
8.2.3	Erforderlichkeit.....	90
8.2.4	Angemessenheit.....	91
9	Risikoanalyse	91
9.1	Methodik	91
9.1.1	Änderungshistorie.....	92
9.2	Risiko-Identifikation.....	92
9.3	Risikoquellen	92
9.3.1	Bedrohungen/Risiken	93
9.3.2	Zuordnung der Risiken zu Betroffenengruppen.....	94

9.3.3	Bewertung der Eintrittswahrscheinlichkeit	94
9.3.4	Bewertung der Schadenshöhe	95
9.4	Maßnahmen zur Risikobehandlung	99
9.5	Bewertung von hohen Restrisiken	100
9.5.1	Hohe Restrisiken der nationalen CWA	101
9.6	Hohe Restrisiken der Interoperabilität	107
9.6.1	Risiken durch fehlende Rechtsgrundlage.....	107
9.6.2	Risiken durch Verarbeitung veralteter oder nicht erforderlicher Daten.....	107
9.6.3	Risiken durch Verwendung und technische Einschränkungen des ENF.....	108
10	Nachhaltige Sicherung des Datenschutzes.....	109
10.1	Evaluierung	109
10.2	Nächster Prüfungstermin	109

3 Über diesen DSFA-Bericht

3.1 Einleitung

Dieser Bericht dokumentiert die Ergebnisse der vom RKI durchgeführten DSFA für die unter Abschnitt 5 beschriebenen Verarbeitungsvorgänge.

Mit dem für den 17.10.2020 geplanten Launch des Release 1.5 der **CWA App** werden die Symptombeginnabfrage und die länderübergreifende Risiko-Ermittlung und Warnung im Rahmen des **European Federation Gateway Service (EFGS)** – sogenannte Interoperabilität – eingeführt. Daher ist eine umfassende Aktualisierung der DSFA erfolgt.

Eine besondere Herausforderung der DSFA und ihrer Dokumentation stellt neben dem pandemiebedingt gegenwärtig hohen Arbeitsanfall beim RKI weiterhin der enge zeitliche Rahmen, die dynamische Architektur und die agile Entwicklungsweise der CWA und des EFGS auf europäischer Ebene dar, wodurch im Projektverlauf laufend Risikobetrachtungen in Architekturentscheidungen eingeflossen sind, die bis zuletzt zu Änderungen geführt haben, die in die vorliegende, aktualisierte Fassung der DSFA aufgenommen werden mussten. Gleichwohl sollen die Vollständigkeit und Transparenz dieses Berichts und der sonstigen CWA-Dokumentation auch unabhängig von zukünftigen funktionalen Änderungen der CWA weiter verbessert werden.

Die Änderungen und Designentscheidungen in Bezug auf die CWA wurden von den verschiedenen Workstreams des CWA-Projekts, dem behördlichen Datenschutzbeauftragten des RKI, den externen juristischen Beratern der Projektbeteiligten und vom Bundesministerium für Gesundheit (BMG) diskutiert und Lösungen entwickelt. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) stand als zuständige Aufsichtsbehörde hierbei dem RKI beratend zur Seite. Zudem wurde das Feedback der Entwicklungscommunity berücksichtigt. Insgesamt stellt sich die Risikobetrachtung im Sinne der DSGVO damit als laufender Prozess dar, der auf ständige Verbesserungen sowohl bei der Entwicklung neuer Funktionen als auch der Anpassung bestehender Funktionen der CWA angelegt ist.

Darüber hinaus erfolgten Diskussionen auf europäischer Ebene betreffend die Anbindung der CWA und anderer **nationaler Corona-Apps** an den EFGS und die hierfür notwendigen Informationsmaßnahmen (insbesondere in Form eines Onboarding-Prozesses).

Zur Verbesserung der Wirksamkeit, Transparenz und infolge auch der Akzeptanz der CWA sind seitens des RKI auch weiterhin Feedback und öffentliche Diskussionen zur CWA gewünscht. Zielgruppe dieses DSFA-Berichts sind technische und juristische Experten, politische Entscheidungsträger und Datenschutzaufsichtsbehörden des Bundes und der Länder sowie Interessengruppen und sonstige Stakeholder.

Methodisch gibt es keine Vorgaben zur Durchführung einer DSFA. Für die vorliegende 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 Risikoanalyse 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 darüber hinaus die vorhandenen und dem DSFA-Team bekannten Veröffentlichungen zu den datenschutzrechtlichen Aspekten einer Corona-Tracing-App umfassend berücksichtigt. Zudem wurden die Stellungnahmen und Forderungen von europäischen Datenschutzaufsichtsbehörden und Datenschutzgremien berücksichtigt². Die durchgeführte Risikoanalyse wurde auf Grundlage einer Risiko-Matrix der Telekom geplant und dokumentiert, die sich ebenfalls an anerkannten Standards orientiert.

Im vorgesetzten Dokument zu den Designentscheidungen (Anlage 1) werden verschiedene von fachkundigen Interessensverbänden und Organisationen (u. a. FIfF, CCC, EDSA) veröffentlichte Anforderungskataloge für eine deutsche bzw. europäische Tracing-Apps aufgeführt und mit Bezügen zu Fundstellen im DSFA-Bericht versehen, damit Leser nachvollziehen können, inwieweit die Anforderungen umgesetzt wurden.

Organisatorisch wurde sichergestellt, dass es bei der Durchführung der DSFA zu keinen Interessenkonflikten 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 RKI wurde Wert darauf gelegt, die weiteren offiziellen Akteure eng in den Entwicklungsprozess einzubinden, um bei unterschiedlichen Auffassungen über die Anwendung von Datenschutzvorschriften und die Bewertung von Risiken schnell zu konsensfähigen Lösungen zu gelangen und vertrauensschädigende Datenschutzbedenken und Verzögerungen zu vermeiden.

² 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 (abgerufen am 15.10.2020) 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 15.10.2020); 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: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (abgerufen am 15.10.2020).

3.2 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. Wieler (Präsident)
----------------	--

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

3.3 DSFA-Team

3.3.1 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.

3.3.2 Zusammensetzung und Vorgehen

Im Abstimmungstermin zwischen RKI und BfDI am 12.05.2020 wurde seitens T-Systems International GmbH (TSI) und SAP Deutschland SE & CO. KG (SAP) der Vorschlag unterbreitet, dass die DSFA im Auftrag des RKI von TSI und SAP für das RKI durchgeführt wird. Hierzu gibt es im Workstream Datenschutz die parallelen Arbeitsstränge

„Datenschutzkonzept“ (DSK) auf der einen und „DSFA“ auf der anderen Seite, welche Hand in Hand arbeiten. Diesem Vorschlag wurde seitens des RKI zugestimmt.

Beratend zur Seite standen dem TSI-/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 SRD, 2. Methodik und Beispiel wurden von dem TSI-/SAP-Team vorgestellt, in einem 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. Seit Anfang an finden regelmäßige Beratungen zwischen dem behördlichen Datenschutzbeauftragten des RKI (DSB), SRD und den weiteren Projektbeteiligten statt. Der BfDI stand hierbei dem RKI beratend zur Seite. Es wurde ein interdisziplinäres DSFA-Team unter Beteiligung von SAP, TSI (von Seiten der Entwickler) sowie SRD zusammengestellt. Der DSB 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.

Auch für die Funktionserweiterungen mit Release 1.5 der CWA App wurde in der beschriebenen Konstellation vorgegangen. Abstimmungstermine des RKI mit dem BfDI zu den Änderungen durch die Einführung der Interoperabilität erfolgten am 02.09.2020 und am 17.09.2020.

3.4 Glossar

Für die effektive Zusammenarbeit der involvierten öffentlichen und privaten Akteure ist ein einheitliches Begriffsverständnis notwendig. Daher werden zentrale Begriffe in einem dokumentationsübergreifenden Glossar definiert. Glossarbegriffe werden bei erstmaliger Verwendung in diesem Dokument **fett** gesetzt. Die in diesem Bericht verwendete Glossarversion ist in der Liste der mitgeltenden Dokumente angegeben.

3.5 Abkürzungsverzeichnis

Begriff	Art	Beschreibung
AEM	T	Associated Encrypted Metadata
BfDI	O	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BLE	T	Bluetooth Low Energy
BMG	O	Bundesministerium für Gesundheit
BWE	T	Bewertungseinstellungen
CCC	O	Chaos Computer Club
CDN	T	Content Delivery Network, CDN-Magenta
CDN-Magenta	T	Content Delivery Network
CWA	O	Corona-Warn-App
DSGVO	§	Datenschutz-Grundverordnung
EDSA	O	Europäischer Datenschutzausschuss
EGS	T	Eigenschlüssel (eigene Tagesschlüssel)
ENF	T	Exposure Notification Framework (Expositionsbenachrichtigungswerkzeug)
EPS	T	Empfangsschlüssel
FAS	T	Positivschlüssel (Tagesschlüssel positiv-getesteter)
FIff	O	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung
FVF	O	Fehlender Verdachtsfall
HKDF	T	Hash Key Derivation Function
IVF	O	Irrtümlicher Verdachtsfall

KOS	T	Kontaktschlüssel
LIS	O	Laboratory Information System
RKI	O	Robert Koch-Institut
RPI	T	Rolling-Proximity-Identifier (zufallsgenerierte Kennnummern)
SES	T	Sendeschlüssel
TAN	T	Transaktionsnummer
TEK	T	Temporary Exposure Keys (Tagesschlüssel)

4 Notwendigkeit der DSFA

Art. 35 Abs. 1 DSGVO regelt die Pflicht zur Durchführung einer DSFA und schreibt diese vor, 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“).

Die CWA unterfällt der „Muss-Liste“ des BfDI³ (dort die Verarbeitungstätigkeiten Nr. 4 a., 5, 7 c. und d. sowie 8).

Auch nach der Auffassung des EDSA muss im Fall einer Corona-Tracing-App (hier: CWA 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.“⁴

Im Zusammenhang mit der Einführung der Interoperabilität ist nach Auffassung des EDSA in der DSFA zudem auf etwaige mit dieser zusätzlichen Verarbeitung und der Mitwirkung zusätzlicher Akteure einhergehende Sicherheitsrisiken einzugehen.⁵

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 aus und ist somit Bestandteil des Gesamtverfahrens der CWA.

³ BfDI: Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO für Verarbeitungstätigkeiten öffentlicher Stellen des Bundes, Stand: Version 1.1-BfDI vom 01.10.2019, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Liste_VerarbeitungsvorgaengeArt35.pdf?blob=publicationFile&v=5 (abgerufen am 15.10.2020).

⁴ EDSA: Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19, angenommen am 21. April 2020, Rn. 39, S. 10 m.w.N., abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_de.pdf (abgerufen am 15.10.2020).

⁵ EDSA: Erklärung über die Datenschutzfolgen der Interoperabilität von Kontaktnachverfolgungs-Apps, angenommen am 16. Juni 2020, Rn. 18, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_de.pdf (abgerufen am 15.10.2020).

5 Beschreibung der CWA (Prüfgegenstand)

Gegenstand der DSFA sind die nachfolgend beschriebenen Verarbeitungsvorgänge im Rahmen des Gesamtverfahrens der CWA.

Teilweise werden auch Verarbeitungsvorgänge außerhalb des Verantwortungsbereichs des RKI beschrieben, um die Beschreibung des Prüfgegenstands verständlicher zu machen. Darauf wird an entsprechender Stelle hingewiesen.

5.1 Hintergrund und Historie

Das Gesamtverfahren der CWA wurde am 16.06.2020 mit der Veröffentlichung der CWA App in den deutschen App Stores von Apple und Google eingeführt.

Die CWA App ist eine Contact-Tracing-App und stellt die zentrale Komponente der CWA dar. Da die CWA einem dezentralen Ansatz folgt, findet die **Begegnungsaufzeichnung** ausschließlich lokal auf dem Smartphone statt. Für den **Testergebnisabruf** und die Warnfunktion muss die CWA App jedoch auf zentrale Dienste zurückgreifen, die von den weiteren Komponenten – **CWA Server**, **Verifikationsserver**, Verifikations-Hotline und weiteren Systemen – bereitgestellt werden. Die Funktionen der datenschutzrechtlich relevanten CWA-Komponenten werden nachfolgend erläutert.

Die CWA App soll die Unterbrechung von Corona-Infektionsketten ermöglichen und damit zur Eindämmung der Corona-Pandemie beitragen. Dies soll erreicht werden, indem **Nutzer** zeitnah über **Risiko-Begegnungen** und ein (positives) **Testergebnis** informiert werden, so dass der betreffende Nutzer sich freiwillig isolieren, testen lassen und im Fall eines positiven Testergebnisses eine Warnung auslösen sowie weitere aus epidemiologischer Sicht gebotene Maßnahmen ergreifen kann.

Die CWA App nutzt das von Apple und Google entwickelte **Expositionsbenachrichtigungswerkzeug** (ENF). Für Smartphones mit **Android** wird das ENF als Bestandteil der Google Play-Dienste und für iPhones als Bestandteil des **Betriebssystems iOS** ab Version 13.5 bereitgestellt. Das ENF ist eine Systemvoraussetzung der CWA App, d. h. auf Smartphones ohne ENF kann die CWA App nicht genutzt werden. Das ENF ermöglicht Smartphones den kontinuierlichen Austausch von **Zufalls-codes (Zufalls-IDs⁶)** zur Kontaktnachverfolgung per **Bluetooth Low Energy** (BLE), ohne dass die

⁶ Der Begriff Zufalls-IDs wird verwendet, um CWA-Nutzern die grundlegende Funktionsweise der CWA App zu erläutern. Um die bessere Nachvollziehbarkeit zu gewährleisten, vernachlässigt der Begriff dabei die technischen Unterschiede zwischen den Schlüsseln und die unterschiedlichen Bezeichnungen je nach Verwendungszusammenhang. Der Begriff Zufalls-ID kann daher abhängig vom Kontext Entfernungsschlüssel, Tagesschlüssel, Positivschlüssel oder Diagnoseschlüssel meinen.

Akkulaufzeit des Smartphones merklich darunter leiden soll. Die Datenverarbeitung durch das ENF liegt außerhalb des Verantwortungsbereichs des RKI.

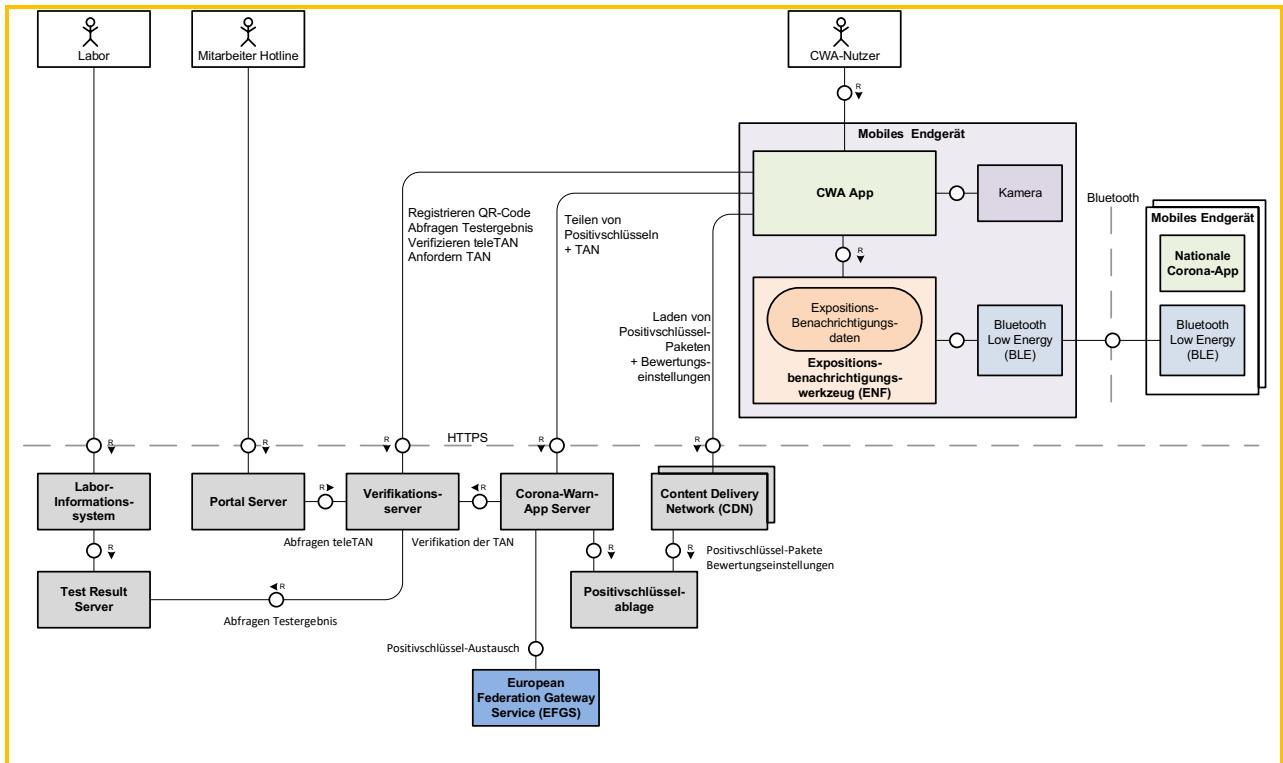


Abbildung 01: Überblick über die Gesamtarchitektur der CWA

Seit ihrer Veröffentlichung hat die CWA App mehrere Updates erhalten, mit denen Fehler behoben und die vorhandenen Funktionen verbessert und barrierefreier gestaltet worden sind.

Wesentliche Funktionserweiterungen werden erstmals mit dem App-Release Version 1.5 eingeführt:

- Die Warnfunktion wird um eine Symptomabfrage erweitert werden, sodass ein **positiv getesteter Nutzer** beim Auslösen einer Warnung freiwillig zusätzlich angeben kann, wann eventuelle typische Corona-Symptome (Fieber, Husten, Geschmacksverlust usw.) erstmals bei ihm aufgetreten sind. Diese Angabe soll genutzt werden, um das Ansteckungsrisiko von **Kontaktpersonen** genauer zu berechnen. Eine Abfrage konkreter Symptome erfolgt nicht.
- Zudem wird die länderübergreifende Funktionsweise der Risiko-Ermittlung und der Warnfunktion (Interoperabilität) eingeführt. Teilnehmende Länder in der Europäischen Union (bzw. potentiell dem Europäischen Wirtschaftsraum) betreiben hierfür einen gemeinsamen Austausch-Server⁷, den **European Federation Gateway Service (EFGS)**, über den untereinander Zufalls-IDs von positiv getesteten Nutzern der

⁷ Der Begriff Austausch-Server wird verwendet, um CWA-Nutzern die grundlegende Funktion des EFGS, die gegenseitige Übermittlung von Positivschlüsseln zwischen den teilnehmenden Verantwortlichen zur Ermöglichung der länderübergreifenden Risiko-Ermittlung, zu verdeutlichen. Im Folgenden wird hierfür der Begriff European Federation Gateway Service (EFGS) verwendet.

nationalen Corona-Apps ausgetauscht werden, um die jeweils eigenen Nutzer über Risiko-Begegnungen informieren zu können.

5.2 Anwendungsphasen und Funktionen der CWA

Die vier zentralen Funktionen der CWA werden in der CWA-Dokumentation jeweils einer eindeutigen Anwendungsphase der CWA App zugeordnet:

- Länderübergreifende Risiko-Ermittlung (Anwendungsphase 1)
- Berechnung des Infektionsrisikos (Anwendungsphase 2)
- Test registrieren (Anwendungsphase 3)
- Andere warnen (Anwendungsphase 4)

Diese Zuordnung von Funktionen zu Anwendungsphasen der CWA App wird auch in dieser DSFA verwendet, um dem Leser die Herstellung von Bezügen zwischen den verschiedenen CWA-Dokumentationen zu erleichtern.

5.3 Zwecke der Datenverarbeitung

Die Datenverarbeitungsvorgänge im Rahmen der CWA dienen folgenden Zwecken:

- (1) Einzelpersonen sollen darüber informiert bzw. gewarnt werden, dass ein erhöhtes Infektionsrisiko besteht, weil sie sich in unmittelbarer Nähe zu einer Corona-infizierten Person⁸ aufgehalten haben, sodass die gewarnte Person so früh wie möglich die gebotenen Verhaltensmaßnahmen (z. B. freiwillige Quarantäne, Konsultieren eines Arztes) ergreifen kann und Infektionsketten unterbrochen werden können.
- (2) Personen, die auf Corona getestet worden sind, sollen ihr Testergebnis ohne Verzögerung erhalten, um im Fall eines positiven Infektionsbefunds so früh wie möglich die gebotenen Verhaltensmaßnahmen ergreifen, andere Personen warnen und Infektionsketten unterbrechen zu können.

Klarstellend wird angemerkt, dass Zweck (1) auch den Zweck der „grenzüberschreitenden Interoperabilität nationaler Mobil-Apps zur Kontaktnachverfolgung und Warnung“ im Sinne von Art. 7 Abs. 1 des Durchführungsbeschlusses (EU) 2020/1023 umfasst.

⁸ Abweichend von dem in anderen Zusammenhängen in der Regel verwendeten Glossarbegriff des „(Corona-)positiv getesteten Nutzers“ wird hier von einer „Corona-infizierten Person“ gesprochen, um kenntlich zu machen, dass es sich um eine Person handelt, die tatsächlich infiziert ist. Diese Unterscheidung ist notwendig, da wegen der bestehenden Unsicherheiten im Testverfahren mit einem gewissen Anteil falsch-positiver Testergebnisse und mit missbräuchlich ausgelösten Falschwarnungen gerechnet werden muss. Daher sind Maßnahmen erforderlich, mit denen das Risiko von unbegründeten Warnungen durch nicht infizierte Personen angemessen reduziert wird.

Folgende „benachbarte“⁹ 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.

5.4 Ablauf aus Sicht eines CWA-Nutzers

5.4.1 Download und Installation der CWA App

Die CWA App wird in den App-Stores von Google (Play Store) und Apple (App Store) bereitgestellt. Das Mindestalter für die Nutzung der CWA App liegt nach den Nutzungsbedingungen der CWA App bei 16 Jahren. Im Apple App Store ist die CWA App zurzeit der Altersstufe „12+“ zugeordnet. Im Play Store ist die CWA App in Deutschland ab 0 Jahren und in den meisten anderen Ländern ab 3 Jahren freigegeben.¹⁰

Wenn sich der **CWA-Nutzer** für den Download 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 den Download der CWA App benötigt der CWA-Nutzer ein persönliches Nutzerkonto bei dem jeweiligen App-Store, der den jeweils gültigen Datenschutzbestimmungen und Nutzungsbedingungen des entsprechenden Betreibers unterliegt. Auf der App-Store-

⁹ 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> (abgerufen am 15.10.2020).

¹⁰ Bei den Alterseinstufungen in den App-Stores handelt es sich um formelle Angaben, die die App-Stores beim Einstellen einer App erzwingen. Eine rechtliche Aussage in Bezug auf die tatsächliche Altersfreigabe für die CWA App aus Sicht des RKI ist damit nicht verbunden. Die Frage nach der Rechtswirksamkeit der Einwilligungen minderjähriger Nutzer aus datenschutzrechtlicher Sicht wird im Abschnitt 7.2.3.2.1 ausgeführt.

Beschreibungsseite der CWA App kann der CWA-Nutzer vor dem Download der CWA App die Datenschutzerklärung und die Nutzungsbedingungen der CWA App aufrufen.

5.4.2 Start der CWA App

5.4.2.1 Initialer Start der CWA App

Wenn der Nutzer die CWA App startet, nachdem er sie erstmals oder erneut nach einer Deinstallation heruntergeladen hat, fragt die CWA App die eingestellte Systemsprache ab, um die Benutzeroberfläche der CWA App in der Systemsprache anzuzeigen. Wenn die CWA App nicht in der Systemsprache angeboten wird, wird die englische Sprachfassung verwendet.

Nach dem initialen Start der CWA App erhält der CWA-Nutzer eine Einführung in die Funktionsweise der CWA App (Onboarding). Im Rahmen der Einführung wird der CWA-Nutzer über die Zwecke und die technische Funktionsweise der CWA App informiert und die aktuelle Datenschutzerklärung wird angezeigt. Im folgenden Onboarding-Schritt wird das Zusammenspiel des ENF mit der CWA App erläutert und auch die länderübergreifende **Risiko-Ermittlung** beschrieben. Die zum jeweiligen Zeitpunkt an der länderübergreifenden Risiko-Ermittlung teilnehmenden Länder werden aufgelistet.

Die Risiko-Ermittlung erfordert initial die **Einwilligung** des CWA-Nutzers und ist daher zunächst deaktiviert. Die Aktivierung der Risiko-Ermittlung erfolgt durch Antippen des Buttons „Risikoermittlung aktivieren“. Hiermit gibt der CWA-Nutzer zugleich die Einwilligung in die Datenverarbeitung für die länderübergreifende Risiko-Ermittlung ab. Ein zweiter Button „Nicht aktivieren“ ermöglicht es dem CWA-Nutzer, die Einwilligung in diesem Schritt wahlweise nicht abzugeben und die Risiko-Ermittlung nicht zu aktivieren.

Da das ENF standardmäßig deaktiviert ist, zeigt das Betriebssystem dem CWA-Nutzer nach Aktivierung der Risiko-Ermittlung zunächst einen Systemdialog an, über den der CWA-Nutzer die Systemfreigabe zur Aktivierung des ENF erteilt. Erst nach dieser Freigabe auf Betriebssystemebene werden zukünftig die in der **Begegnungsaufzeichnung** aufgezeichneten Zufalls-IDs mit der CWA App geteilt. Sobald der CWA-Nutzer auch das ENF aktiviert, ist die Risiko-Ermittlung der CWA App funktionsfähig.

Nutzer eines iPhones werden vom iOS-Betriebssystem mit einem Systemdialog zudem gefragt, ob die CWA App Mitteilungen senden darf. Auf Smartphones mit Android-Betriebssystem erhält die CWA App standardmäßig die Berechtigung zum Versand von Mitteilungen. Die Mitteilungen der CWA App können in den Einstellungen der CWA App deaktiviert werden.

5.4.2.2 Start der CWA App nach Update

Startet der CWA-Nutzer die CWA App erstmalig nach Durchführung des Updates auf die Version 1.5, erhält er bei Start der CWA App eine Einführung über die mit dem Release Version

1.5 eingeführte Funktionsweise der länderübergreifenden Risiko-Ermittlung. Die Informationen erklären die Funktionsweise des EFGS sowie den Zweck der Interoperabilität. Zudem werden die Mitgliedstaaten, die gegenwärtig über eine am EFGS angeschlossene **nationale Corona-App** verfügen mit ihrer jeweiligen Nationalflagge aufgelistet. Die länderübergreifende Risiko-Ermittlung wird in einem hervorgehobenen Hinweis erläutert. Die Datenverarbeitung in Bezug auf den CWA-Nutzer im Rahmen der Risiko-Ermittlung ändert sich durch das Update allerdings nicht. Es werden keine zusätzlichen Daten des Nutzers erhoben oder vorhandene Daten an zusätzliche Empfänger übermittelt.

5.4.3 Home-Bildschirm

Der Home-Bildschirm wird nach dem Abschluss des Onboardings und bei jedem zukünftigen Start der CWA App angezeigt. Dort werden der aktuelle Status der länderübergreifenden Risiko-Ermittlung (aktiv/inaktiv), der für den CWA-Nutzer ermittelte **Risikowert** (z. B. „niedriges Risiko“) sowie die für den CWA-Nutzer aktuell verfügbaren weiteren Funktionen (z. B. **Testregistrierung**, Warnen, Einstellungen) und Inhalte (z. B. Glossar) angezeigt.

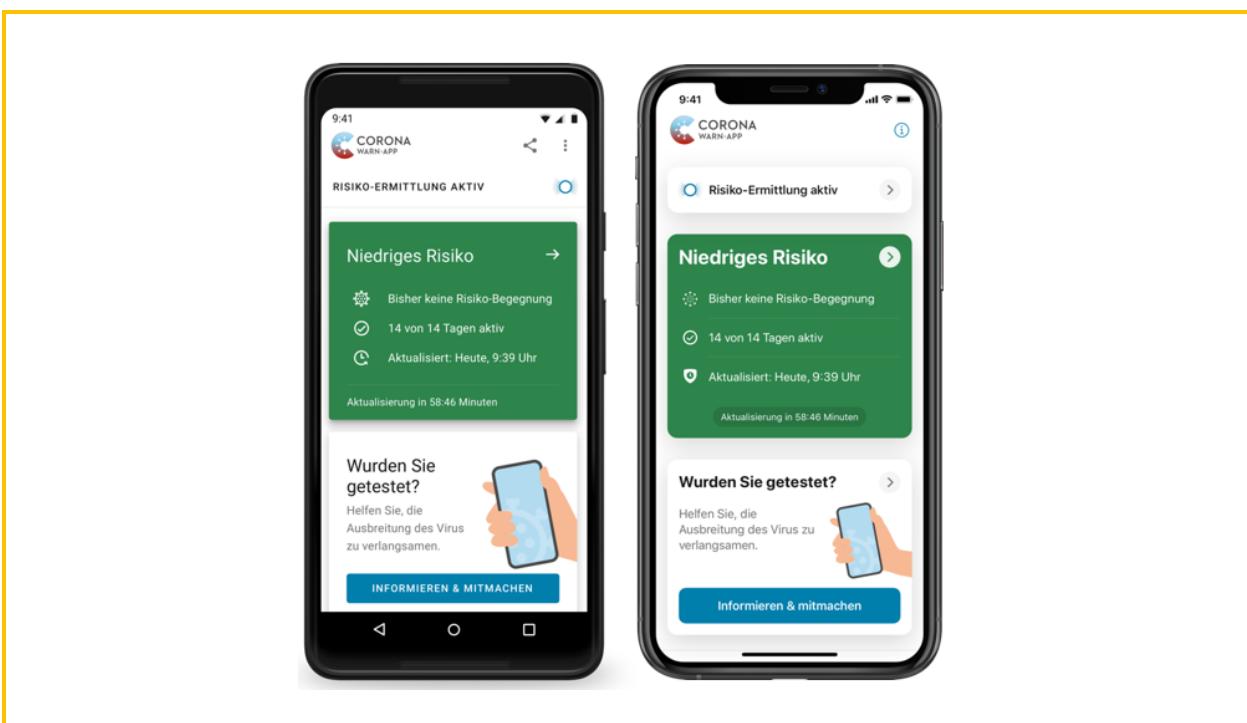


Abbildung 02: Home-Bildschirm bei "niedrigem Risiko" (links Android, rechts iOS)

5.4.4 Risiko-Ermittlung

Der CWA-Nutzer erreicht über den Home-Bildschirm oder über den Menüpunkt „Einstellungen“ den Hauptbildschirm zur Risiko-Ermittlung. Auf diesem Bildschirm wird die Funktionsweise der länderübergreifenden Risiko-Ermittlung erläutert und unter dem Unterpunkt „Länderübergreifende Risiko-Ermittlung“ die Liste der Mitgliedstaaten angezeigt, die gegenwärtig über eine an den EFGS angebundene nationale Corona-App verfügen.

Der CWA-Nutzer kann über einen Schalter die länderübergreifende Risiko-Ermittlung aktivieren bzw. deaktivieren.

Im Falle einer Störung der Risiko-Ermittlung (z. B. weil der CWA-Nutzer die Funktion **Bluetooth** seines Smartphones deaktiviert hat) wird dem CWA-Nutzer der Grund dieser Beeinträchtigung angezeigt und ein Lösungsweg vorgeschlagen.

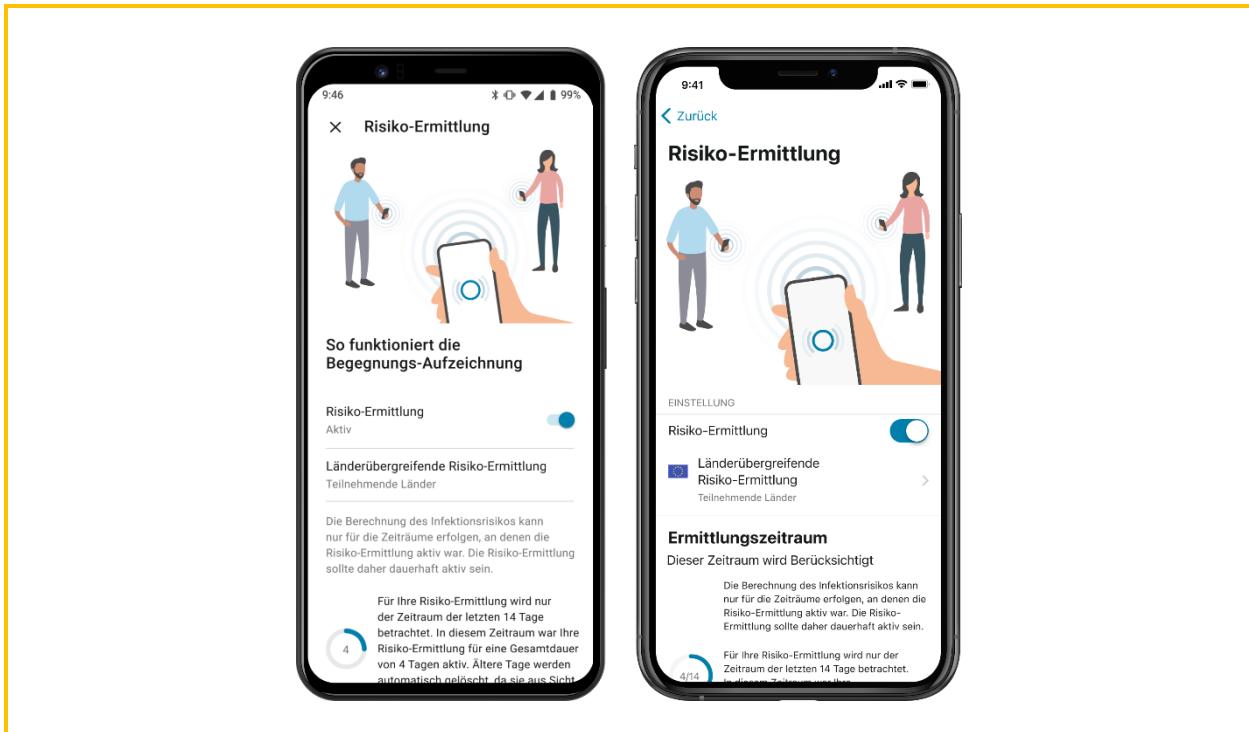


Abbildung 03: Bildschirm der Risiko-Ermittlung (links Android, rechts iOS)

5.4.5 Risikodetails und Risikostufen

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

Der Risikowert wird einer der folgenden Stufen zugeordnet:

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

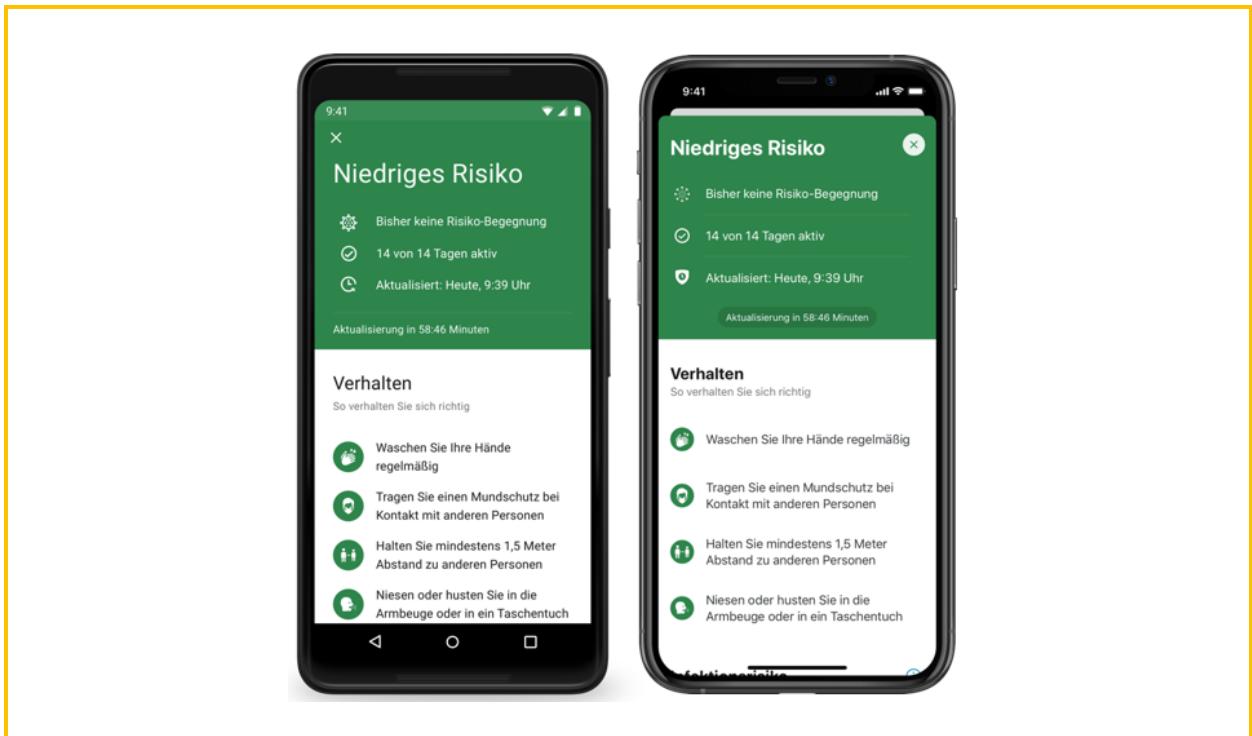


Abbildung 04: Anzeige der Risikodetails bei "niedrigem Risiko" (links Android, rechts iOS)

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

5.4.6 Testregistrierung

Im Fall eines durchgeföhrten Corona-Tests kann der CWA-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 der CWA-Nutzer bei der Durchführung des Tests vor Ort gefragt, ob er sein Testergebnis über die CWA App erhalten möchte und ob er mit einer entsprechenden Übermittlung des Testergebnisses an die dafür vorgesehene Serverinfrastruktur (Test Result Server) der CWA einverstanden ist.

Sofern der CWA-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 mithilfe des QR-Codes, der eine Kennzahl (**GUID**) enthält, die Zuordnung der Proben sowie der Testergebnisse erfolgen. Hierfür kann der CWA-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 und generiert einen Hash, der zur Abfrage des Testergebnisses genutzt wird.

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

der CWA App angezeigt. Über die lokale Mitteilungsfunktion des Betriebssystems kann der CWA-Nutzer über das Vorliegen des Testergebnisses in der CWA App informiert werden. Die Mitteilung selbst enthält keine Information über das konkrete Ergebnis des Tests. Erst nach dem Öffnen der CWA App wird dem CWA-Nutzer das Testergebnis auf dem Home-Bildschirm der CWA App einmalig angezeigt.

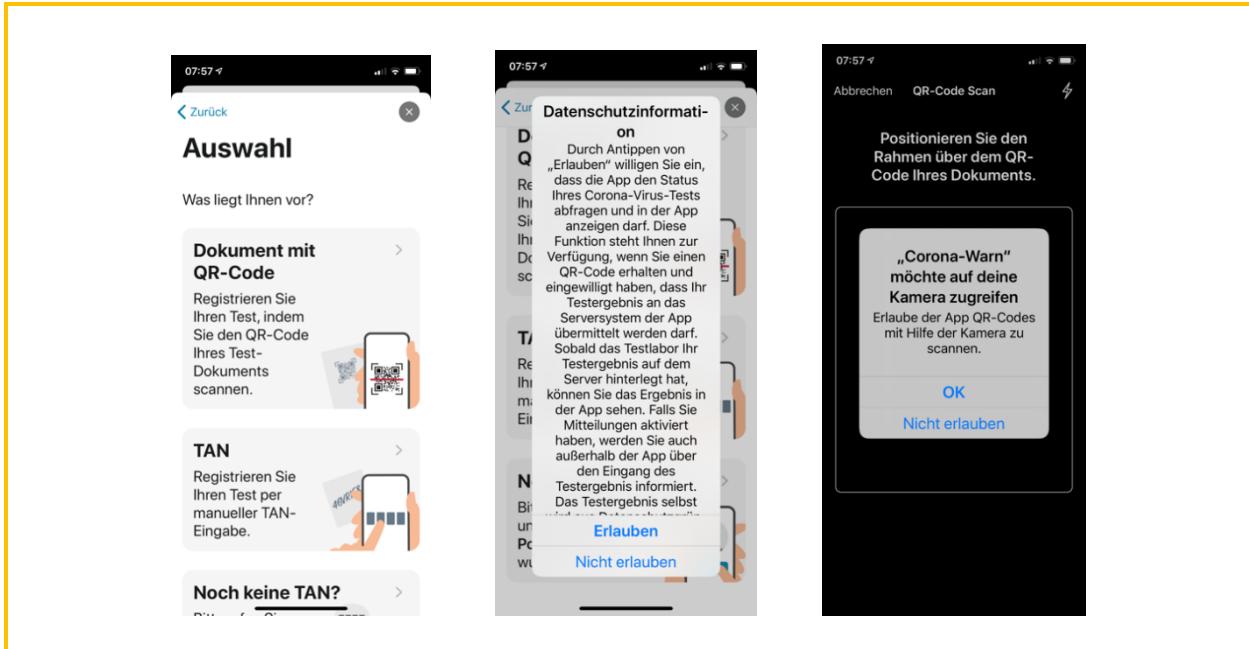


Abbildung 05: Test-Registrierung, QR-Code Verfahren (Beispiel-Screenshot iOS)

5.4.7 Verifikations-Hotline

Die Verifikations-Hotline steht CWA-Nutzern zur Verfügung, die die Risiko-Ermittlung der CWA App aktiviert 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 CWA-Nutzers aufgrund von Beschädigungen nicht lesbar ist oder kein QR-Code an Labor oder CWA-Nutzer ausgegeben wurde.

In diesem Fall kann sich der CWA-Nutzer an die **Hotline** (Verifikations-Hotline) wenden. Dem anrufenden CWA-Nutzer werden durch einen Mitarbeiter der Hotline gemäß einem abgestimmten Skript Plausibilitätsfragen gestellt, um die Gefahr eines Missbrauchs des Warnsystems zu verringern. Wenn der Mitarbeiter der Hotline die Antworten für schlüssig erachtet und den Anrufer somit als einen tatsächlich positiv getesteten CWA-Nutzer verifiziert, erbittet er die Angabe der Telefonnummer und des Namens des CWA-Nutzers. Danach beendet der Mitarbeiter der Hotline das Gespräch, um über eine Weboberfläche bei dem **Portal Server** eine **teleTAN** abzufragen. Die teleTAN wird dem positiv getesteten CWA-Nutzer sodann im Rahmen eines Rückrufs mündlich mitgeteilt. Durch den Rückruf soll die Gefahr eines Missbrauchs der Hotline verringert werden.

Die teleTAN hat eine Gültigkeit von einer Stunde. Innerhalb dieses Zeitraums kann der positiv getestete CWA-Nutzer die teleTAN in der CWA App eingeben. Die Kontaktdaten des CWA-Nutzers, die der Mitarbeiter der Hotline zum Zweck des Rückrufs erhoben hat, werden spätestens nach einer Stunde nach Ausgabe der teleTAN gelöscht.

5.4.8 Warnfunktion

Ein positiv getesteter CWA-Nutzer kann sein verifiziertes Testergebnis mit anderen Nutzern teilen und diese so über eine mögliche Ansteckung informieren. Die anderen Nutzer, die mit dem positiv getesteten CWA-Nutzer in Kontakt waren, erfahren dabei nicht, welche ihrer **Kontaktpersonen** die Warnung ausgelöst hat.

Der CWA-Nutzer hat dabei mit Release 1.5 die Möglichkeit, optionale Angaben zum Symptombeginn mitzuteilen. Hierfür kann er nach der Verifikation des Testergebnisses über einen entsprechenden Button „Weiter mit Symptom-Erfassung“ oder „Weiter ohne Symptom-Erfassung“ fortfahren.

Nach Auswahl der Symptom-Erfassung wird der CWA-Nutzer gefragt, ob bei ihm typische Symptome einer Corona-Infektion aufgetreten sind. Der Symptom-Bildschirm enthält einen Hinweis zum Zweck der Angabe, der gesondert auf die Freiwilligkeit hinweist. Die Buttons „Ja“, „Nein“ und „keine Angabe“ sind nicht vorausgewählt.

Gibt der CWA-Nutzer an, dass Symptome vorlagen, wird er sodann nach dem zeitlichen Beginn des Auftretens der Symptome gefragt. Auch diese Angabe ist freiwillig, weder die Datumsauswahl noch der Button „keine Angabe“ sind vorausgewählt. Eine Abfrage einzelner Symptome erfolgt nicht.

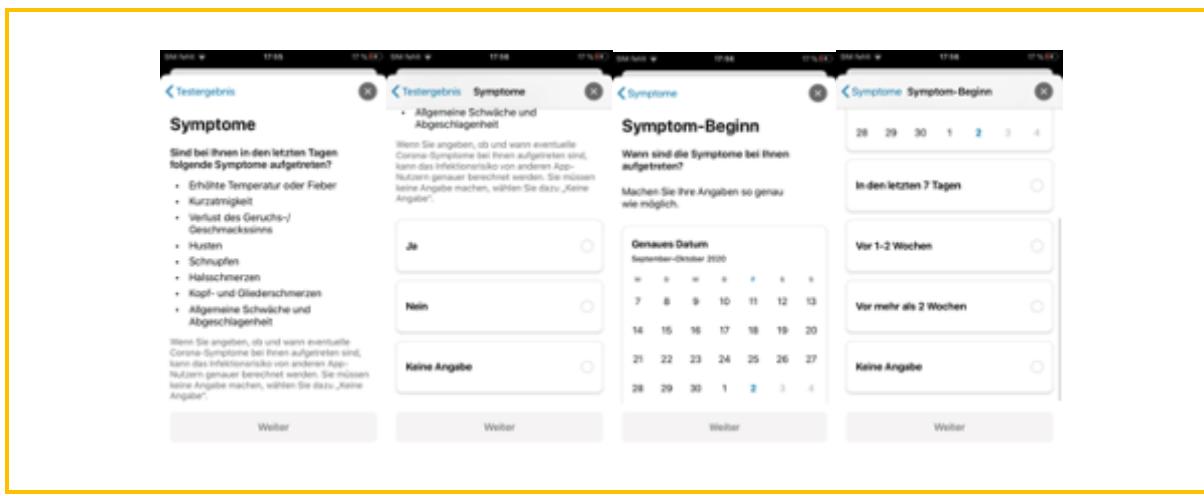


Abbildung 06: Abfrage zum Symptombeginn (Beispiel-Screenshot iOS)

Im Anschluss wird der CWA-Nutzer auf die Funktion der länderübergreifenden Warnung hingewiesen. In einer Liste werden die Mitgliedstaaten angezeigt, die gegenwärtig über eine an den EFGS angebundene nationale Corona-App verfügen und deren Nutzer somit potentiell gewarnt werden können.

Anschließend an die Information wird die Einwilligungserklärung in die Übermittlung zur länderübergreifenden Warnung wiedergegeben. Die Einwilligungserklärung erstreckt sich auf die Übermittlung der Zufalls-IDs der letzten 14 Tage (einschließlich etwaiger optionaler Angaben zum Symptombeginn) an den CWA Server, die der CWA App aus dem ENF nach Freigabe des CWA-Nutzers zur Verfügung gestellt werden, sowie die Weitergabe an den EFGS. Als Empfänger der zu übermittelnden Daten werden die zuvor aufgeführten Mitgliedstaaten angegeben, die gegenwärtig über eine an den EFGS angebundene nationale Corona-App verfügen. Die Übermittlung dient der Bereitstellung der Zufalls-IDs (und ggf. weiteren Angaben zum Symptombeginn) über den EFGS, damit die in den jeweiligen Mitgliedstaaten Verantwortlichen diese abrufen und sie über die nationalen Back-End-Server den Nutzern der jeweiligen nationalen Corona-App im Rahmen der länderübergreifenden Risiko-Ermittlung zur Verfügung stellen können.

Durch Antippen des Buttons „Einverstanden“ erteilt der CWA-Nutzer die Einwilligung in die Übermittlung.

Im Anschluss wird der CWA-Nutzer über einen Systemdialog gebeten, die Freigabe zur Weitergabe der Zufalls-IDs durch das ENF an die CWA App zu erteilen.

Der gesamte Nutzerdialog der Warnfunktion kann jederzeit vom CWA-Nutzer abgebrochen werden. Zuletzt kann die Übermittlung durch die Verweigerung der Freigabe im Systemdialog abgebrochen werden.

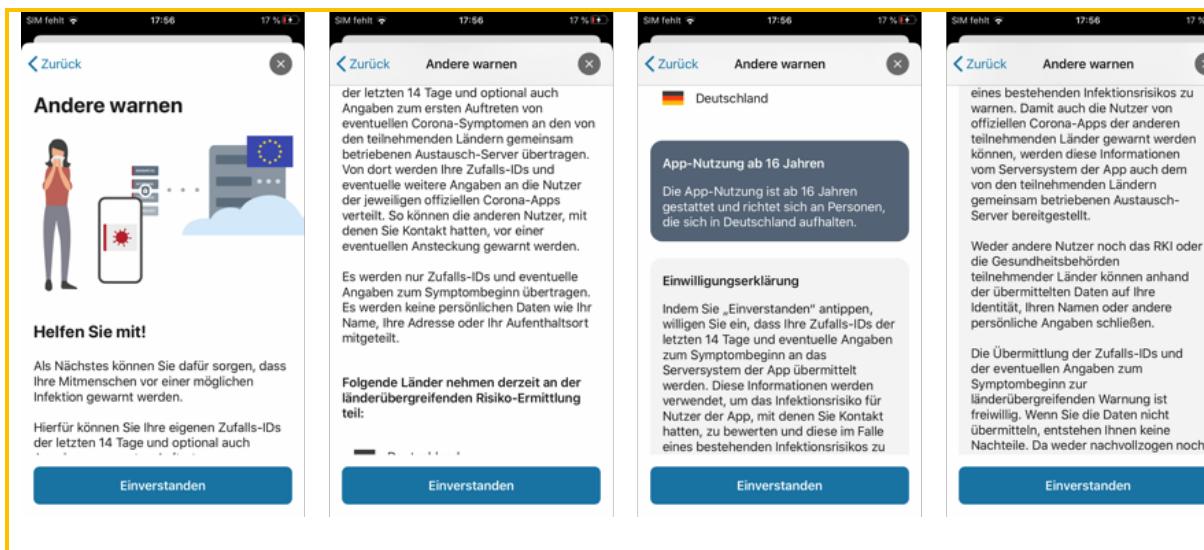


Abbildung 07: Einwilligung länderübergreifende Warnung (Beispiel-Screenshot iOS)

Nach erfolgreicher Übermittlung erhält der CWA-Nutzer im Abschluss-Bildschirm eine diesbezügliche Bestätigung angezeigt.

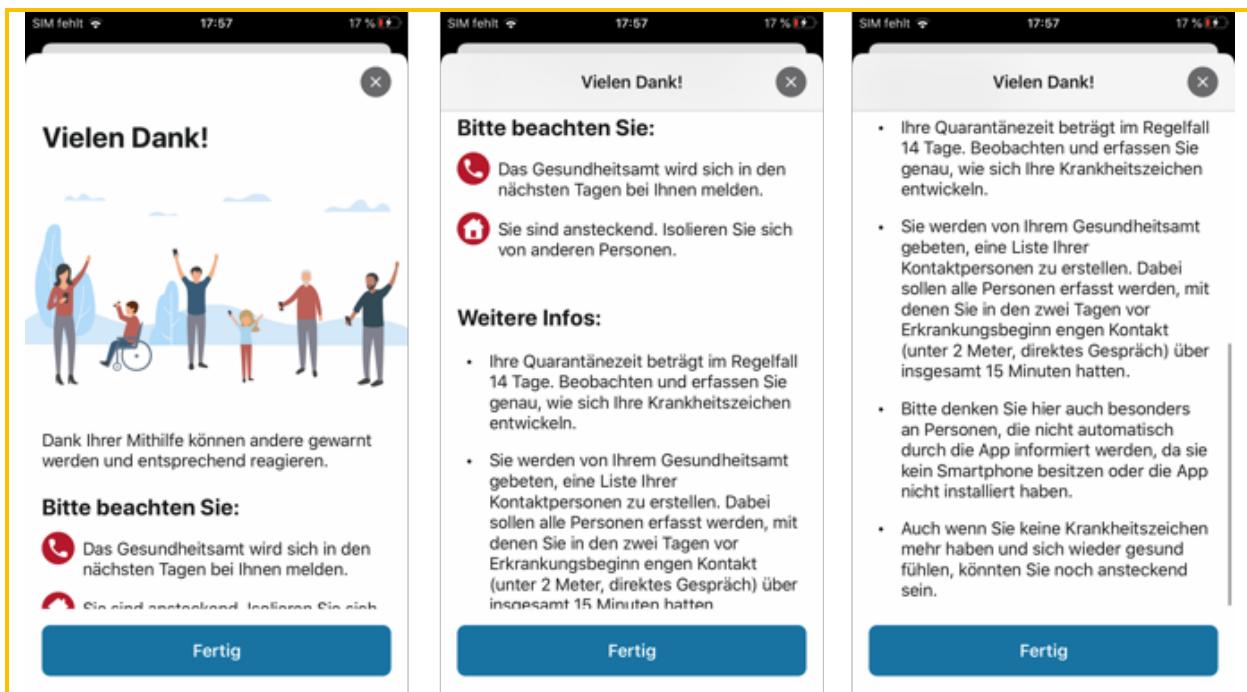


Abbildung 08: Abschluss-Bildschirm (Beispiel-Screenshot iOS)

5.4.9 Sonstige Funktionen

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

5.4.9.1 CWA App teilen

Über den Home-Bildschirm kann der CWA-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 auf die Kontakte des CWA-Nutzers.

5.4.9.2 App-Informationen

Über den Home-Bildschirm kann der CWA-Nutzer den Bereich „App-Informationen“ aufrufen. In diesem Bereich werden die gesetzlichen Pflichtinformationen (Datenschutzerklärung, Impressum) sowie weitere Informationen (z. B. Nutzungsbedingungen, Open-Source-Lizenzhinweise, Kontaktdaten der Hotline) angezeigt.

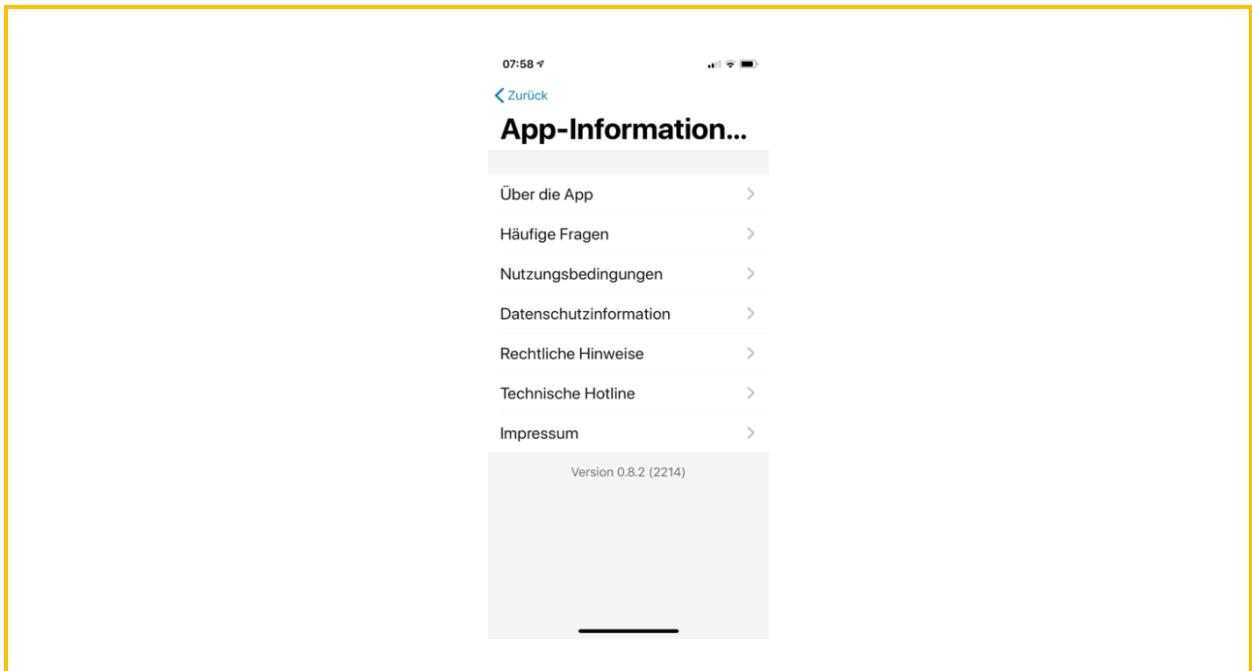


Abbildung 09: App-Information (Beispiel-Screenshot iOS)

5.4.9.3 Einstellungen

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

5.4.9.4 Überblick

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

5.5 Systemarchitektur

Für die technische Umsetzung der Infrastruktur der CWA wurde im Auftrag des RKI durch TSI und SAP eine spezielle Systemarchitektur konzipiert, die die Anforderungen von Datenschutz und Datensicherheit besonders berücksichtigt. Technisch ist das Gesamtsystem der CWA so konzipiert, dass eine Identifizierung einzelner Nutzer durch die an den Datenverarbeitungsvorgängen beteiligten Stellen und andere Nutzer in der Regel ausgeschlossen werden kann. Die CWA verzichtet umfassend auf die Verwendung zentraler Identifikationsmerkmale oder Nutzerkennungen, die eine Zuordnung von Datensätzen zu

spezifischen Nutzern ermöglichen würden. Die für die datenschutzrechtliche Betrachtung maßgeblichen Komponenten der Architektur werden nachfolgend beschrieben.

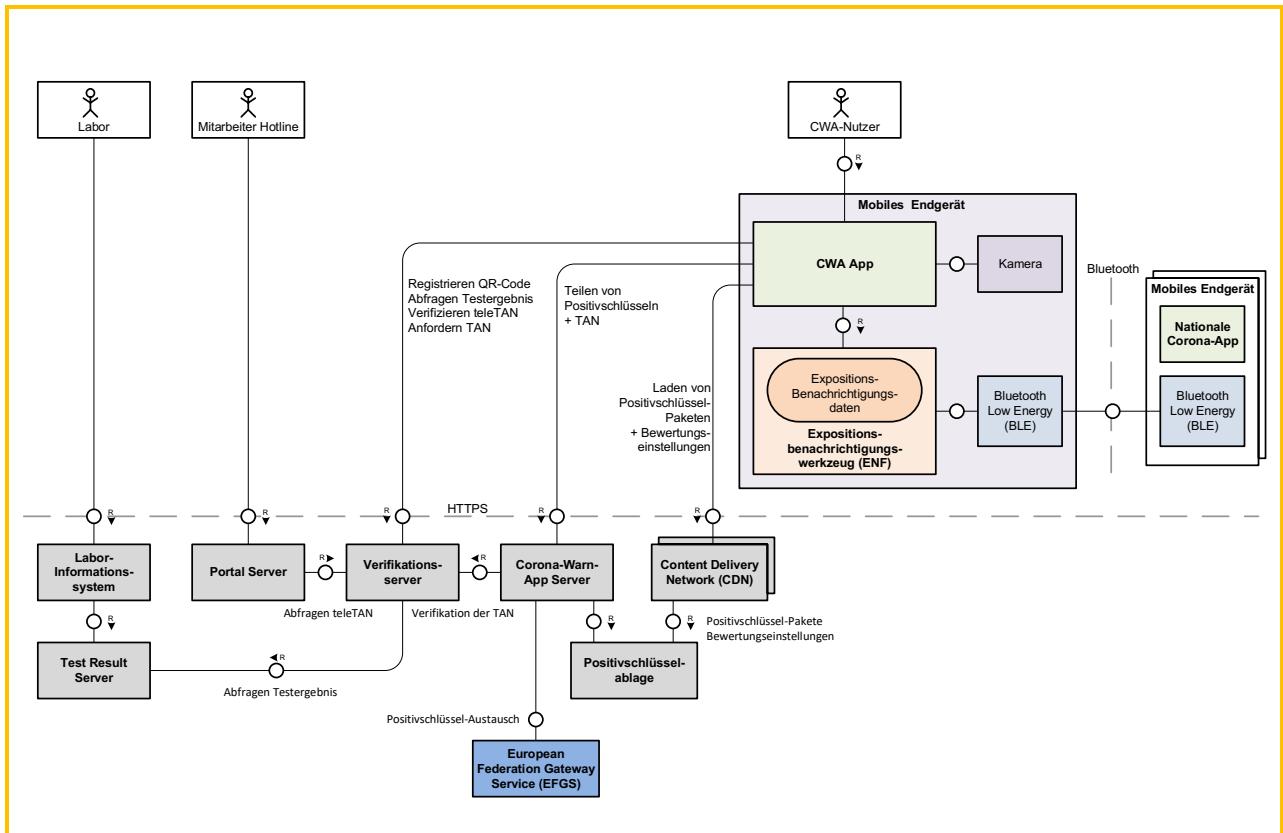


Abbildung 10: Überblick über die Architektur der CWA

Die länderübergreifenden Funktionen bzw. Zwecke der CWA werden durch die Anbindung des CWA Servers an den EFGS realisiert.

Die CWA App interagiert mit dem CWA Server und dem Verifikationsserver über HTTPS sowie mit der ENF-Schnittstelle. Dabei erfolgt die Kommunikation des Endgerätes des CWA-Nutzers mit dem CWA Server und dem **CDN-Magenta** sowie dem Verifikationsserver. Das ENF ist nicht Teil der CWA.

Die Anbindung an den EFGS erfolgt nicht direkt über die CWA App. Die Kommunikation erfolgt stets über den CWA Server.

5.5.1 Smartphone (Mobiles Endgerät)

Das Smartphone (einschließlich des Betriebssystems) stellt die für den Betrieb der CWA App notwendigen Funktionalitäten und Konnektivitäten bereit. Für den Betrieb der CWA App werden insbesondere die folgenden Komponenten und Hintergrunddienste der mobilen Endgeräte benötigt:

Internetkommunikation:

Die CWA App benötigt eine Internetverbindung, um auf den CWA Server, CDN-Magenta und den Verifikationsserver zugreifen zu können. Die Serveranbindung ist für den Bezug der Zufalls-IDs der positiv getesteten Nutzer sowie die Funktion „Andere warnen“ erforderlich.

Kamera:

Zur Nutzung des Testergebnisabrufs benötigt die CWA App Zugriff auf die Kamera des Smartphones, um den QR-Code zu scannen.

ENF:

Das ENF ist ein Bluetooth-Low-Energy-Dienst. Er wurde von Apple und Google vor dem Hintergrund der Corona-Pandemie entwickelt, um Corona-Apps die Annäherungserkennung und Dokumentation von Kontakten zwischen mobilen Endgeräten zur Berechnung eines Ansteckungsrisikos zu ermöglichen. Zurzeit erlauben Apple und Google nur einer offiziellen Corona-App pro Land die Nutzung des ENF, wobei die jeweilige Corona-App von einer Gesundheitsbehörde oder anderen amtlichen Stelle (bspw. Rotes Kreuz) angeboten werden muss. In der Bundesrepublik Deutschland ist die CWA App die nationale Corona-App und somit als einzige Anwendung hierzulande berechtigt, das ENF zu nutzen.

5.5.2 CWA Server

Der CWA Server wird für die Verteilung der **Positivschlüssel** im Rahmen der Funktion „Andere warnen“ benötigt. Wenn ein positiv getester CWA-Nutzer sein (verifiziertes) Testergebnis in der CWA App registriert oder eine teleTAN erhalten hat und daraufhin seine **Tagesschlüssel** zur Verfügung stellen möchte, um andere Nutzer zu warnen, stellt die CWA App eine verschlüsselte Verbindung zum CWA Server her. Über diese Verbindung werden dann die Tagesschlüssel (nunmehr „Positivschlüssel“ genannt) des CWA-Nutzers der letzten 14 Tage von der CWA App an den CWA Server übermittelt. Der CWA Server empfängt und übermittelt zudem Positivschlüssel vom und an den EFGS, um die länderübergreifende Warnung der Nutzer anderer nationaler Corona-Apps zu ermöglichen.

5.5.3 CDN-Magenta (Content Delivery Network)

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

Das CDN-Magenta stellt der CWA App die Liste mit den aktuellen Positivschlüsseln aller Nutzer, die in der CWA App oder einer anderen nationalen Corona-App ihre Positivschlüssel geteilt haben, nachdem sie positiv getestet wurden, über eine verschlüsselte Verbindung zum Download bereit. Die Liste mit den aktuellen Positivschlüsseln wird von der CWA App zyklisch abgefragt (auch im Hintergrundbetrieb). Die CWA-Nutzer können auch manuell eine

Aktualisierung der Bewertung des eigenen Ansteckungsrisikos und somit einen Download der aktuellen Liste der Positivschlüssel anstoßen.

Daneben stellt das CDN-Magenta der CWA App die aktuellen **Bewertungseinstellungen (BWE)** zur Verfügung. Die BWE beinhalten die technische Konfigurationseinstellung für die Analyse und die Risikobewertung der Kontakte mit anderen Nutzern, die auf dem Smartphone des CWA-Nutzers zur Bewertung des Ansteckungsrisikos genutzt werden. Die BWE werden anhand der wissenschaftlichen Erkenntnisse des RKI zur Ansteckungswahrscheinlichkeit konfiguriert. Es können auf diese Weise die aktuellen epidemiologischen Erkenntnisse in die Risikoermittlung einfließen. Details siehe unter Ziffer 5.7.7 (Bewertungseinstellungen).

5.5.4 Verifikationsserver

Der Verifikationsserver dient der Validierung von positiven Testergebnissen, die von CWA-Nutzern in der CWA App registriert werden. Die Echtheitsprüfung soll Falschmeldungen verhindern. Das vom Verifikationsserver verwendete TAN-Verfahren dient zudem dazu, die Identifikation des CWA-Nutzers durch natürliche Personen zu erschweren, zugleich aber eine eindeutige technische Zuordnung in der Kommunikation der spezifischen CWA-App-Instanz des CWA-Nutzers mit dem CWA Server zu ermöglichen. Die TAN ist eine einmalig gültige Transaktionsnummer, die beim Abruf des Testergebnisses automatisch generiert und dann in der CWA App abgelegt wird, sofern der CWA-Nutzer gegenüber dem testenden Labor der Mitteilung des Testergebnisses über die CWA App zugestimmt hat.

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

5.5.5 Portalserver

Über den Portalserver steht den Mitarbeitern der Verifikations-Hotline eine Funktion zur Abfrage der teleTANs zur Verfügung. Über eine Weboberfläche, die 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 im Klartext an den Portalserver zurückgegeben und von dort über die Weboberfläche dem Mitarbeiter der Verifikations-Hotline zur Verfügung gestellt. Zudem wird ein Hashwert der teleTAN gebildet und auf dem Verifikationsserver gespeichert.

5.5.6 Test Result Server

Auf dem **Test Result Server** wird die Datenbank bereitgestellt, in der die Labore die Testergebnisse der CWA-Nutzer speichern können, die einer entsprechenden Übermittlung zugestimmt haben. Die Labore greifen über eine eigene Software, den **Lab Client**, auf den Test Result Server zu.

5.5.7 European Federation Gateway Service (EFGS)

Um die Interoperabilität der nationalen Corona-Apps zur länderübergreifenden Risiko-Ermittlung und Warnung zu ermöglichen, hat die Europäische Kommission einen Durchführungsbeschluss zur Einrichtung eines Gateway Service angenommen und den European Federation Gateway Service (EFGS) ins Leben gerufen¹¹.

Beim EFGS handelt es sich um eine technische Datenplattform, über die die relevanten pseudonymisierten Informationen, die durch die nationalen Corona-Apps zur länderübergreifenden Risiko-Ermittlung und Warnung jeweils erfasst werden, auf effiziente und sichere Weise zwischen den am EFGS teilnehmenden Mitgliedstaaten der Europäischen Union ausgetauscht werden können. In der Folge können auf Grundlage der über die Corona-Apps erfassten Begegnungen und von den jeweiligen Nutzern über ihre jeweilige nationale Corona-App mitgeteilten Positivschlüssel auch zur Warnung von Nutzern anderer nationaler Corona-Apps genutzt werden. Begegnungen zwischen Nutzern verschiedener nationaler Corona-Apps (z. B. auf Reisen) können dann bei den länderübergreifenden Warnungen berücksichtigt werden.

Am EFGS können Mitgliedstaaten der Europäischen Union und des EWR teilnehmen, die über eine nationale Corona-App verfügen, die das ENF von Google und Apple nutzt. Der EFGS wird von den für die teilnehmenden nationalen Corona-Apps Verantwortlichen gemeinsam betrieben und verantwortet. Die Verantwortlichen haben ein formalisiertes Antragsverfahren ausgearbeitet, in dessen Rahmen die rechtlichen und technischen Anforderungen für die Teilnahme überprüft werden.

In technischer Hinsicht sind die Server der einzelnen nationalen Corona-Apps mit dem EFGS verbunden. Die Server der nationalen Corona-Apps – in der Bundesrepublik Deutschland der CWA Server – laden in regelmäßigen Abständen die Positivschlüssel der Nutzer der eigenen nationalen Corona-App hoch und die zur Verfügung gestellten Positivschlüssel der Nutzer der anderen nationalen Corona-Apps herunter. Das Design des EFGS folgt den

¹¹ Europäische Kommission: Coronavirus: new steps towards setting-up of an interoperability solution for mobile tracing and warning apps, vom 15. Juli 2020, abrufbar unter: https://ec.europa.eu/newsroom/sante/item-detail.cfm?item_id=683319&utm_source=sante_newsroom&utm_medium=Website&utm_campaign=sante&utm_content=Coronavirus%20new%20steps%20towards%20setting-up%20of%20an%20interoperability%20solution%20&lang=en (abgerufen am 15.10.2020).

Interoperabilitätsleitlinien¹², den zwischen den Mitgliedstaaten und der Europäischen Kommission vereinbarten technischen Spezifikationen¹³, den in der EU Toolbox aufgeführten Leitlinien und den EU-Leitlinien zur Gewährleistung der uneingeschränkten Einhaltung der Datenschutzstandards durch Mobil-Apps¹⁴ sowie den Empfehlungen der Europäischen Kommission für den Einsatz von Kontaktnachverfolgungs-Apps zur Bekämpfung der Pandemie¹⁵. Im Rahmen des Antragsverfahrens zur Teilnahme am EFGS wird die Kohärenz der zu prüfenden Corona-App mit den genannten Richtlinien durch die übrigen teilnehmenden Länder überprüft.

Die datenschutzrechtlichen Aufgaben und Pflichten der am EFGS teilnehmenden Verantwortlichen sind nicht in einem Vertrag über die gemeinsame Verantwortlichkeit, sondern im Durchführungsbeschluss 2020/1023 der EU-Kommission vom 15.07.2020 niedergelegt. Darin ist festgelegt, dass die Verarbeitung im EFGS allein der Herstellung der Interoperabilität nationaler Corona-Apps zur länderübergreifenden Kontaktnachverfolgung und Warnung sowie der Kontinuität der Ermittlung von Kontaktpersonen in einem länderübergreifenden Kontext dienen darf. Die Zwecke, für die die über den EFGS ausgetauschten Daten verwendet werden dürfen, sind damit abschließend koordiniert.

Zudem sind die Datenkategorien niedergelegt, die im Rahmen der gemeinsamen Verantwortlichkeit über den EFGS übermittelt werden können (Schlüssel, die bis zu 14 Tage vor dem Datum des Hochladens der Schlüssel von den nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung übermittelt wurden; Protokolldaten zu den Schlüsseln gemäß den technischen Spezifikationen, die im Ursprungsland der Schlüssel verwendet werden; die Verifizierung der Diagnose; die relevanten Länder und das Ursprungsland der Schlüssel). Darüber geht die CWA nicht hinaus. Die Angabe zu relevanten Ländern ermöglicht es den teilnehmenden Verantwortlichen, potentiell bestimmte Positivschlüssel aus den am EFGS vorhandenen Daten herauszufiltern und darüber die Menge der an die Nutzer der eigenen nationalen Corona-App zu übermittelnden Positivschlüssel zu steuern, falls sich zukünftig herausstellen sollte, dass die täglichen Downloadmengen andernfalls zu groß werden. Die Anwendung dieses sog. Country of Interest-Ansatzes ist technisch und rechtlich möglich, gegenwärtig wird davon aber im Rahmen der CWA kein Gebrauch gemacht. Die an den EFGS übermittelten Positivschlüssel sind daher gegenwärtig als für alle teilnehmenden

¹² eHealth Network Guidelines to the EU Member States and the European Commission on Interoperability specifications for cross-border transmission chains between approved apps, Detailed interoperability elements between COVID+ Keys driven solutions, V1.0, vom 16.06.2020, abrufbar unter:

https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilitydetailedelements_en.pdf (abgerufen am 15.10.2020).

¹³ [Set of Technical Specifications](#).

¹⁴ eHealth Network: Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States, Version 1.0, vom 15.04.2020, abrufbar unter: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf (abgerufen am 15.10.2020).

¹⁵ Empfehlung (EU) 2020/518 der Kommission vom 8. April 2020 für ein gemeinsames Instrumentarium der Union für den Einsatz von Technik und Daten zur Bekämpfung und Überwindung der COVID-19-Krise, insbesondere im Hinblick auf Mobil-Apps und die Verwendung anonymisierter Mobilitätsdaten, abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1587153139410&uri=CELEX:32020H0518> (abgerufen am 15.10.2020).

Mitgliedstaaten relevant vorgesehen, es werden diesbezüglich keine zusätzlichen Angaben zu den Positivschlüsseln gespeichert.

Des Weiteren ist grundlegend bestimmt, welche Aufgaben die Verantwortlichen im Rahmen der Geltendmachung von Betroffenenanfragen haben und wie mit Verletzungen des Schutzes personenbezogener Daten umzugehen ist.

Die teilnehmenden Länder haben sich zudem darauf verständigt, dass nur Länder an das EFGS angeschlossen werden, die vorab in einem formalisierten und zwischen den Verantwortlichen zuvor abgestimmten Antragsverfahren einen Antrag gestellt haben und umfassende Informationen über die Verarbeitung der Daten in Zusammenhang mit ihrer Corona-App zur Verfügung gestellt haben. Die Anträge und die zur Verfügung gestellten Informationen werden durch die Verantwortlichen geprüft.

5.6 Datenflüsse und Prozesse

Nachfolgend wird dargestellt, in welchen Anwendungsphasen durch welche Akteure welche Daten verarbeitet und übertragen werden. Zudem wird die Phase der Deinstallation der CWA App betrachtet.

5.6.1 Anwendungsphase 1: Risiko-Ermittlung

In der ersten Anwendungsphase werden bei Begegnungen von Personen mit aktiviertem ENF zufällige, fortlaufend wechselnde Kennungen (sog. Entfernungsschlüssel, **Rolling-Proximity-Identifier**, RPIs) zwischen dem Smartphone des CWA-Nutzers und den Smartphones anderer Nutzer per BLE im Rahmen der Begegnungsaufzeichnung des ENF ausgetauscht (Schritt 1). Zudem lädt die CWA App des CWA-Nutzers regelmäßig die Liste mit den Positivschlüsseln vom CDN-Magenta über das Internet (Schritt 2) herunter. Anschließend werden die empfangenen RPIs mit den heruntergeladenen Positivschlüsseln abgeglichen, sog. Matching (Schritt 3). Die von Nutzern anderer nationaler Corona-Apps für die länderübergreifende Warnung über den EFGS zur Verfügung gestellten Positivschlüssel sind Bestandteil der Liste mit den Positivschlüsseln und werden beim Matching daher mitberücksichtigt.

5.6.1.1 Schritt 1: Begegnungsaufzeichnung

Der Austausch von RPIs des CWA-Nutzers mit Smartphones von anderen Nutzern im Rahmen der Begegnungsaufzeichnung findet unter folgenden Voraussetzungen statt:

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

Die nachfolgend dargestellten Datenflüsse und Prozesse hinsichtlich Schritt 1 finden nicht in der CWA App, sondern auf Ebene des Betriebssystems im ENF statt. Für die Begegnungsaufzeichnung verwendet das ENF zwei verschiedene Datenstrukturen:

- Tagesschlüssel (Temporary Exposure Keys, TEK)
- Entfernungsschlüssel (Rolling-Proximity-Identifier, RPI)

Der Tagesschlüssel ist ein Zufalls Wert, der einmal täglich auf dem Endgerät eines Nutzers generiert und im ENF gespeichert wird. 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. Ein Austausch der RPIs erfolgt dabei zwischen allen Endgeräten, die das ENF aktiviert haben – ungeachtet der Frage, welche Corona-App auf dem Endgerät installiert ist.

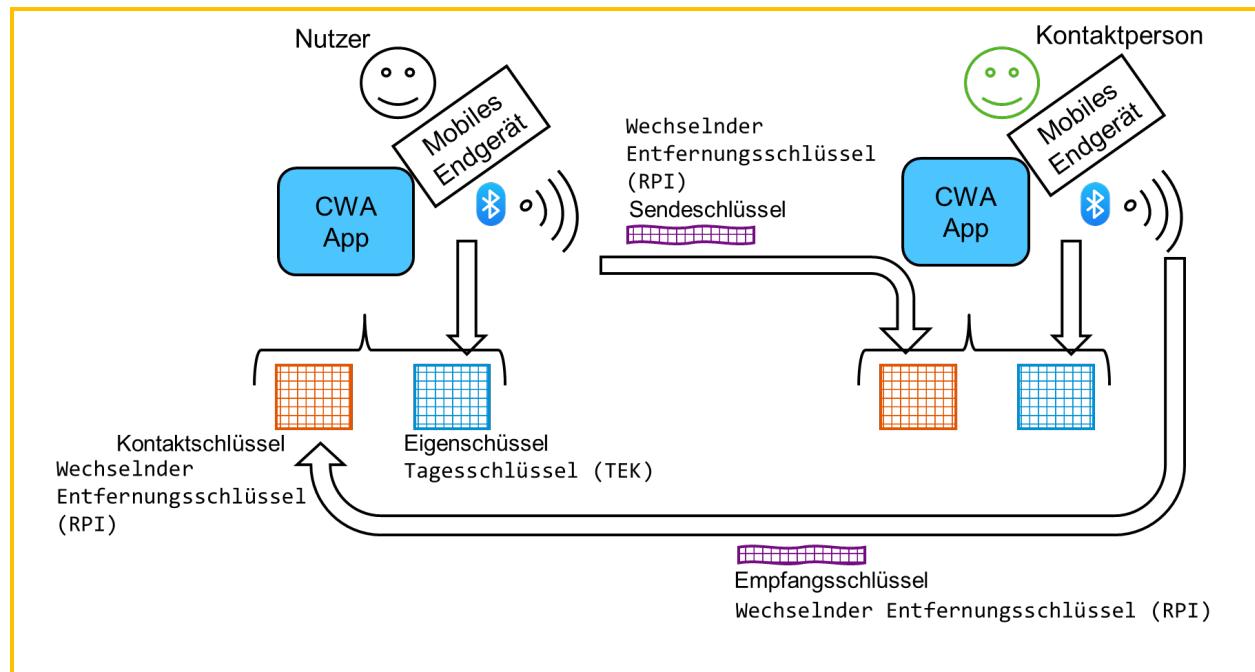


Abbildung 11: Austausch von RPIs

Um die konkrete Risikobewertung nach dem Austausch von RPIs im Rahmen der Begegnungsaufzeichnung zu ermöglichen, werden die RPIs durch zusätzliche RPI-Metadaten ergänzt und im Speicher des ENF über einen Zeitraum von zwei Wochen gespeichert. Die gespeicherten RPI-Metadaten umfassen Angaben zum Datum des Kontakt, zur Kontaktzeit und zum Dämpfungswert (Signalstärke) des Bluetooth-Signals. Die Kontaktzeit wird in 5-Minutenintervallen für maximal 30 Minuten protokolliert.

5.6.1.2 Schritt 2: Download der Positivschlüssel

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

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

Ein Positivschlüssel ist ein Tagesschlüssel eines Nutzers, den dieser über eine nationale Corona-App zur Verfügung gestellt hat, um Nutzer länderübergreifend zu warnen.

Aufgrund der Anbindung des CWA Servers an den EFGS können nicht nur Positivschlüssel von CWA-Nutzern, sondern auch Positivschlüssel anderer nationaler Corona-Apps über die CWA-App heruntergeladen und anschließend berücksichtigt werden.

Die CWA App ruft in regelmäßigen Abständen und bei manueller Aktualisierung des Risikowerts von dem CDN-Magenta eine Liste mit den Positivschlüsseln aller Nutzer ab, die diese in den letzten 14 Tagen über nationale Corona-Apps geteilt haben (**Positivschlüssel-Paket**).

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

Zusätzlich werden die aktuellen **Bewertungseinstellungen** (BWE) von dem CDN-Magenta geladen.

Sowohl die Positivschlüssel-Pakete 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.

5.6.1.3 Schritt 3: Matching der Positivschlüssel mit RPIs

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

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

Die CWA App gibt die heruntergeladenen Positivschlüssel an das ENF weiter, welches aus diesen RPIs ableitet und diese mit den in der Begegnungsaufzeichnung gespeicherten RPIs des CWA-Nutzers abgleicht.

Anschließend löscht die CWA App die heruntergeladenen Positivschlüssel.

Wenn es kein „Match“ gibt – also keine Begegnung mit einem Nutzer aufgezeichnet wurde, der im maßgeblichen Zeitraum Positivschlüssel über eine nationale Corona-App zur Verfügung gestellt hat –, teilt das ENF dies der CWA App mit. Die CWA App zeigt dem CWA-Nutzer in diesem Fall an, dass keine Risiko-Begegnung vorliegt und somit ein „niedriges Risiko“ besteht.

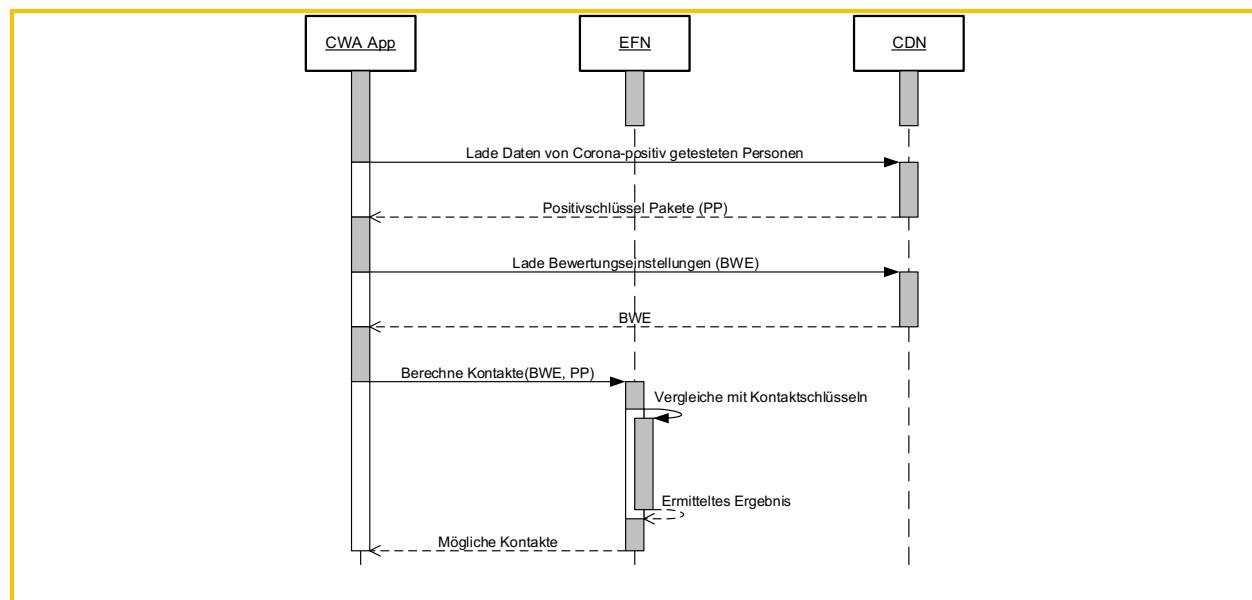


Abbildung 12: Laden der Positivschlüssel-Pakete und Ermittlung möglicher Kontakte

5.6.2 Anwendungsphase 2: Berechnung des Infektionsrisikos

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

Die RPI-Metadaten werden unter Beachtung der BWE ausgewertet, um das spezifische Ansteckungsrisiko (Total Risk Score) für den CWA-Nutzer zu bewerten. Für die Berechnung des Ansteckungsrisikos wird das Produkt aus einem Abstandsfaktor, einem Faktor der vergangenen Zeit zum Kontakt, einem Faktor für die Dauer des Kontaktes und dem Übertragungs-Risiko-Faktor gebildet:

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

Der Abstandsfaktor wird dabei wie folgt ermittelt: Mit Hilfe des empfangenen Positivschlüssels und des daraus errechneten RPI werden die verschlüsselten RPI-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.

Die Berechnung des Ansteckungsrisikos findet lokal auf dem Smartphone statt, das heißt, die Daten werden offline verarbeitet. Das ermittelte Ansteckungsrisiko 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 CWA App zeigt dem CWA-Nutzer schließlich auf dem Home-Bildschirm an, welches Ansteckungsrisiko bzw. welcher Risikowert ermittelt worden ist. Zudem werden dem CWA-Nutzer Handlungsempfehlungen des RKI, basierend auf dem zuletzt ermittelten Risikowert, angezeigt.

5.6.3 Anwendungsphase 3: Testregistrierung

Im Fall eines durchgeföhrten Corona-Tests kann der CWA-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 durchgeführt und an das jeweils angeschlossene Labor weitergegeben. Von den Laboren werden die Testergebnisse auf einen zentralen Test Result Server übertragen und können vom CWA-Nutzer über die CWA App vom Server abgerufen werden, sofern der CWA-Nutzer in dieses Vorgehen zuvor eingewilligt hat.

Um die sichere Zuordnung der Probe bzw. des späteren Testergebnisses mit der CWA App des Nutzers sicherzustellen, ist ein Zusammenspiel aus einer physisch anlässlich der Einwilligung übergebenen Kennung in Form eines QR-Codes und einem technischen Verifikationsverfahren eingerichtet.

Im ersten Schritt erhält der CWA-Nutzer dazu bei der Stelle, die den Test durchführt, z. B. beim Arzt, ein Informationsblatt, auf dem dieses Verfahren beschrieben ist. Zu dem Informationsblatt erhält der CWA-Nutzer einen QR-Code, der mit Hilfe der CWA App eingescannt werden kann. Der CWA-Nutzer entscheidet sodann gegenüber der Stelle, die den Test durchführt, ob er der Übermittlung des Testergebnisses an den Test Result Server zum Zweck des späteren Abrufs über die CWA App zustimmt. Die Erteilung der Einwilligung wird auf dem Probenbegleitschein vermerkt.

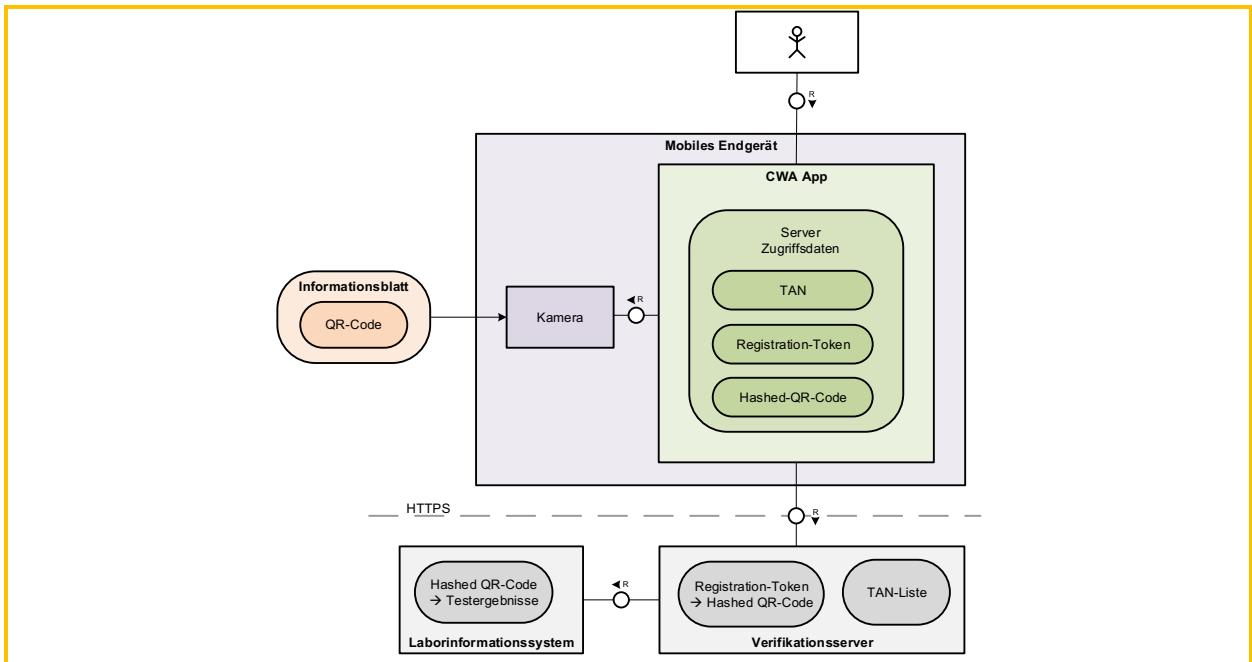


Abbildung 13: Zusammenspiel von QR-Code und Testergebnis über die CWA App

Vor dem Einstellen des QR-Codes willigt der CWA-Nutzer in die Datenverarbeitung in Zusammenhang mit dem Verfahren ein. Der CWA-Nutzer authentifiziert sich – ohne Angaben zu seiner Person zu machen – unter alleiniger Verwendung des QR-Codes und der darin enthaltenen GUID auf dem Verifikationsserver. Die CWA App bestimmt hierfür den Hash der GUID und sendet diesen 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 CWA-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 CWA-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 Eigenschlüssel (**eigene Tagesschlüssel, EGS**) anderen Nutzern zur Verfügung zu stellen. Im weiteren Verfahren können so andere Nutzer bezüglich potenzieller Kontakte mit dem positiv getesteten CWA-Nutzer gewarnt werden (Anwendungsphase 4).

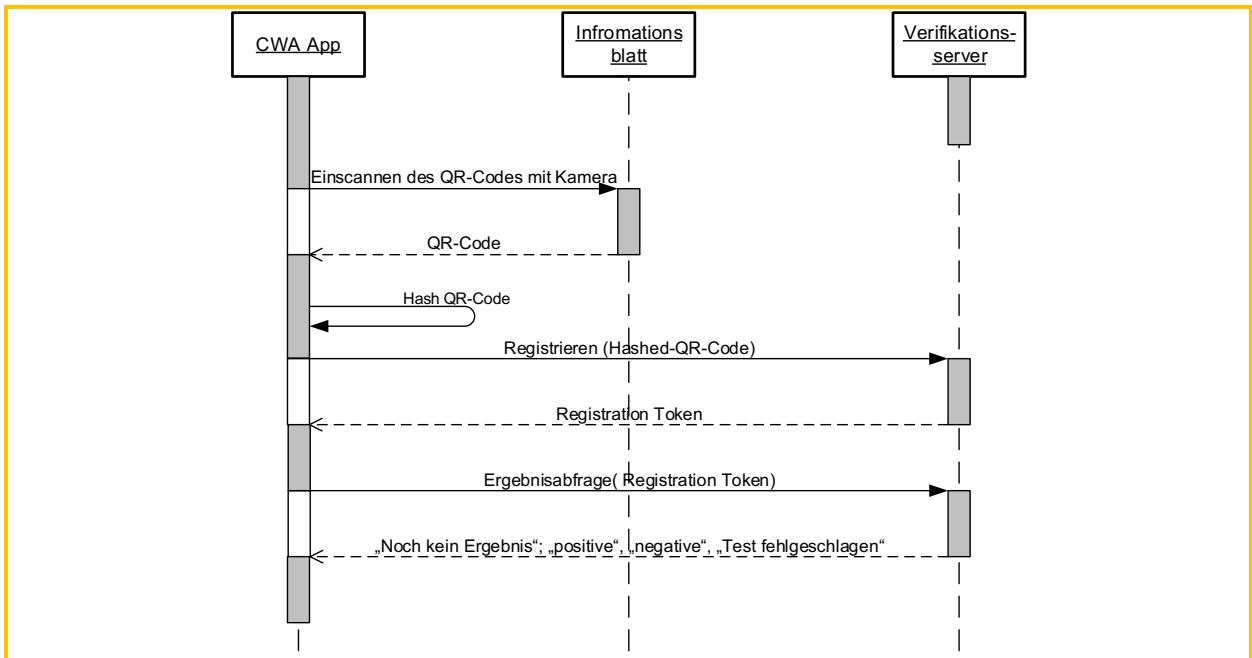


Abbildung 14: Einscannen des QR-Code, Testregistrierung und Testergebnisabfrage

5.6.4 Anwendungsphasen 3-4: Verifikations-Hotline

Die Hotline steht CWA-Nutzern zur Verfügung, die die Risiko-Ermittlung genutzt haben, denen die Testregistrierung 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 CWA-Nutzers aufgrund von Beschädigungen nicht lesbar ist, kein QR-Code an Labor oder CWA-Nutzer ausgegeben wurde oder der CWA-Nutzer nicht in das Verfahren zum Testabruf eingewilligt hat.

Um die Gefahr der Verbreitung von falschen positiven Testergebnissen über nationale Corona-Apps und die daraus folgenden falschen Empfehlungen für andere Nutzer zu verringern, werden dem anrufenden CWA-Nutzer durch einen speziell geschulten Mitarbeiter der Hotline gemäß einem Skript Plausibilitätsfragen gestellt. Die Antworten der CWA-Nutzer werden nicht gespeichert. Wenn der Mitarbeiter der Hotline die Antworten für schlüssig hält und den Anrufer somit als einen positiv getesteten CWA-Nutzer verifiziert, erfragt er beim CWA-Nutzer eine Telefonnummer und den Namen für einen Rückruf. Danach beendet der Mitarbeiter der Verifikations-Hotline das Telefonat, um über die Weboberfläche des Portal servers eine teleTAN abzufragen. Der Portal Server verbindet sich mit dem Verifikationsserver, der die teleTAN generiert. Der Hashwert der teleTAN wird auf dem Verifikationsserver gespeichert, die teleTAN wird im Klartext an den Portal Server zurückgegeben und von dort über die Weboberfläche dem Mitarbeiter der Hotline zur Verfügung gestellt. Die teleTAN wird dem positiv getesteten CWA-Nutzer sodann im Rahmen eines Rückrufs mündlich mitgeteilt. Die vorübergehende physische Aufzeichnung der mitgeteilten Rufnummer und des Namens wird spätestens innerhalb einer Stunde vernichtet.

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

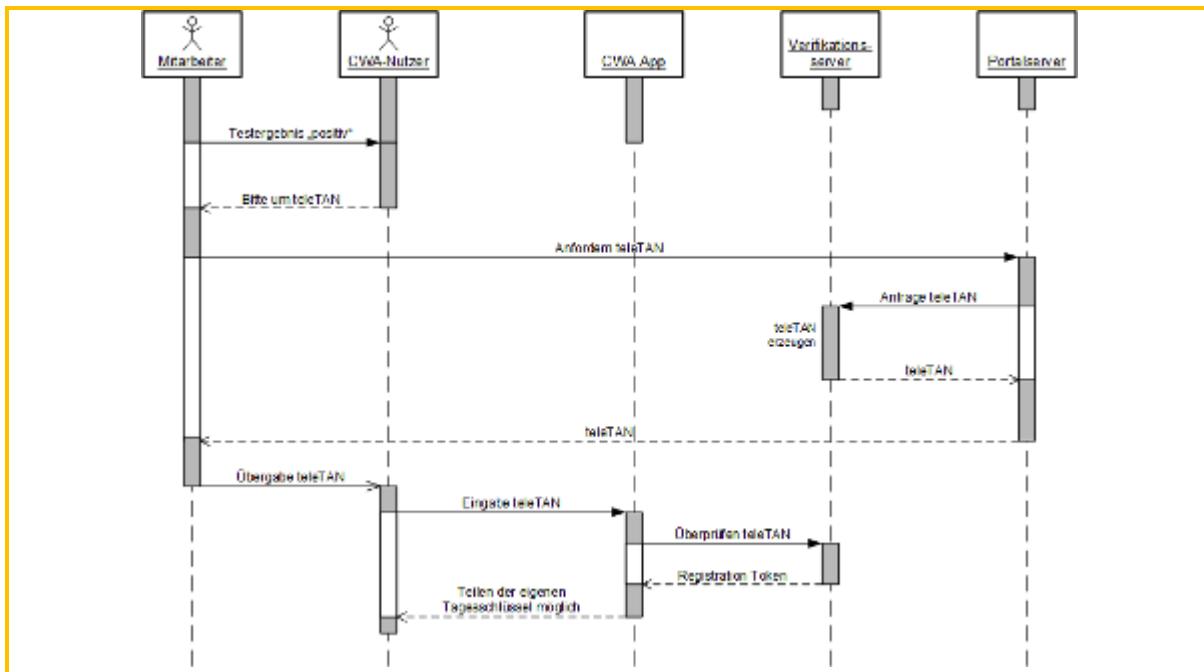


Abbildung 15: Abfrage teleTAN

5.6.5 Anwendungsphase 4: Andere warnen

Nach dem Abruf eines positiven Testergebnisses in der CWA App oder Eingabe einer gültigen teleTAN kann ein positiv getesteter CWA-Nutzer seine Tagesschlüssel übermitteln, damit andere Nutzer, denen der CWA-Nutzer im maßgeblichen Zeitraum begegnet ist, gewarnt werden können. Aufgrund der technisch gewährleisteten Interoperabilität der nationalen Corona-Apps können potentielle Risiko-Begegnungen des positiv getesteten CWA-Nutzers auch länderübergreifend berücksichtigt und länderübergreifende Warnungen ausgelöst werden.

Um eine Warnung auslösen zu können, muss in der CWA App eine TAN hinterlegt sein und der positiv getestete CWA-Nutzer muss in die Verarbeitung seiner Daten zur länderübergreifenden Warnung ausdrücklich einwilligen.

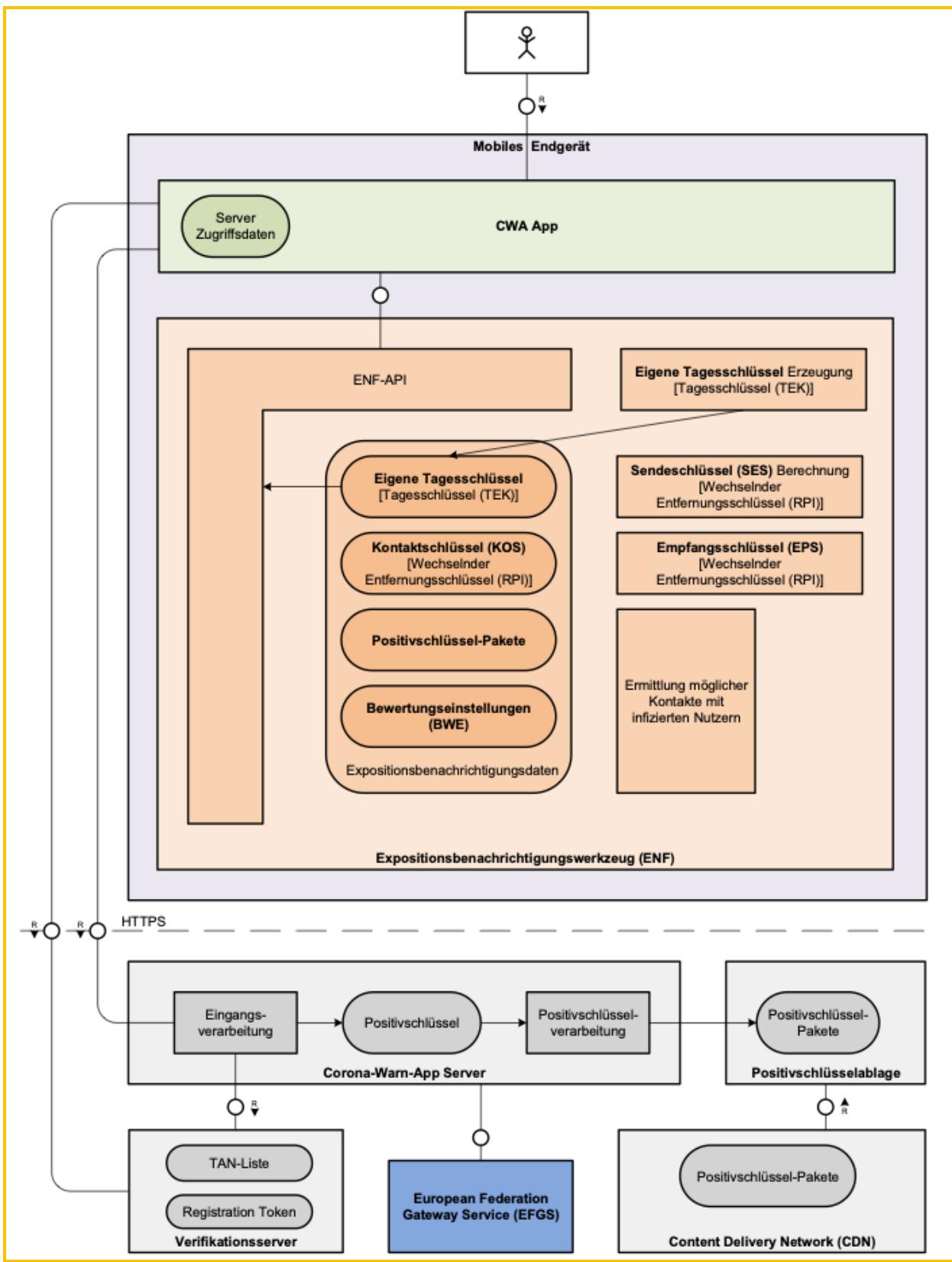


Abbildung 16: Die CWA App übergibt die TAN und die Eigenschlüssel an den CWA Server

Die CWA App ermöglicht es dem CWA-Nutzer, zusätzliche Angaben zum Symptombeginn zu machen. Diese Informationen helfen im Rahmen der Risiko-Ermittlung eine genauere

Einschätzung zum Beginn möglicher Ansteckungszeiträume abzugeben. Der Schritt zur Symptom-Abfrage ist jedoch optional.

Zu Beginn des Symptom-Abfrage-Dialogs wird der Zweck der Angaben erläutert und die Freiwilligkeit der Angaben gesondert betont. Im Rahmen der Symptom-Abfrage erfragt die CWA App sodann, ob beim CWA-Nutzer gegenwärtig die aufgelisteten typischen Corona-Symptome (z. B. Husten und Fieber) vorliegen. Diese Frage kann mit „Ja“, „Nein“ und „keine Angabe“ beantwortet werden. Konkrete Symptome werden nicht erfasst. Sofern der CWA-Nutzer mit „Ja“ antwortet, wird im zweiten Schritt erfragt, wann die Symptome zum ersten Mal aufgetreten sind, andernfalls wird die Symptom-Abfrage beendet. Hat der CWA-Nutzer die Frage nach dem Symptombeginn ebenfalls beantwortet (z. B. durch Auswahl der Buttons „In den letzten 7 Tagen“, „Vor 1-2 Wochen“ oder Auswahl eines spezifischen Datums) oder hat er „keine Angabe“ ausgewählt, wird der Symptom-Abfrage-Dialog beendet.

Nachdem der CWA-Nutzer seine Einwilligung in die Übermittlung der Tagesschlüssel (einschließlich der etwaigen zusätzlichen Angaben zum Symptombeginn) erklärt und die erforderliche Systemfreigabe erteilt hat, fordert die CWA App vom ENF die Tagesschlüssel der letzten 14 Tage an.

Die CWA App setzt sodann jeweils einen Zahlenwert von 0 bis 8 in das Datenfeld „TransmissionRiskLevel“ der vom ENF erhaltenen Tagesschlüssel. Dieser Zahlenwert wird nach Maßgabe der aktuell in der CWA App hinterlegten BWE festgelegt und basiert auf den optionalen Angaben des CWA-Nutzers auf die Frage nach einem eventuellen Symptombeginn (z. B. „Vor 1-2 Wochen“ oder „keine Angabe“). Der Wert des „TransmissionRiskLevels“ der jeweiligen Tagesschlüssel wird in Abhängigkeit vom Tag bzw. Zeitraum des Symptombeginns oder, wenn der CWA-Nutzer keine Angaben gemacht hat, in Abhängigkeit vom Zeitpunkt des Erhalts der TAN festgelegt.

Die Tagesschlüssel mit den darin enthaltenen jeweiligen TransmissionRiskLevel-Werten werden schließlich zusammen mit der TAN an den CWA Server übermittelt. Die Tagesschlüssel werden ab diesem Zeitpunkt Positivschlüssel genannt.

Der CWA Server überprüft die Gültigkeit der TAN mit Hilfe des Verifikationsservers und gibt bei bestätigter Gültigkeit die Verarbeitung der Positivschlüssel frei. Im weiteren Verfahren generiert der CWA Server aus von allen positiv getesteten CWA-Nutzern übermittelten Positivschlüsseln die Positivschlüssel-Pakete und übergibt diese – gemeinsam mit den über das EFGS zur Verfügung gestellten Positivschlüsseln der Nutzer anderer nationaler Corona-Apps – dem CDN-Magenta.

Da der am Übermittlungstag verwendete Tagesschlüssel vom ENF zunächst nicht weitergegeben wird, wird dieser in einem zweiten Schritt am nächsten Tag von der CWA App beim ENF angefordert und mit dem entsprechend gesetzten TransmissionRiskLevel-Wert und der TAN an den CWA Server übermittelt. Dieser Prozess findet im Hintergrund statt.

Der CWA Server prüft das Format der übermittelten Daten auf Korrektheit.

Der CWA Server mischt die Positivschlüssel unterschiedlicher Ladevorgänge miteinander, damit sie nicht einem bestimmten Ladevorgang zugeordnet werden können. Die

Positivschlüssel werden mit einem auf die letzte volle vergangene Stunde abgerundeten Zeitstempel versehen, um eine Zuordnung von IP-Adressen anhand von Log-Daten, bspw. des Internetanbieters, zu übermittelten Positivschlüsseln zu verhindern.

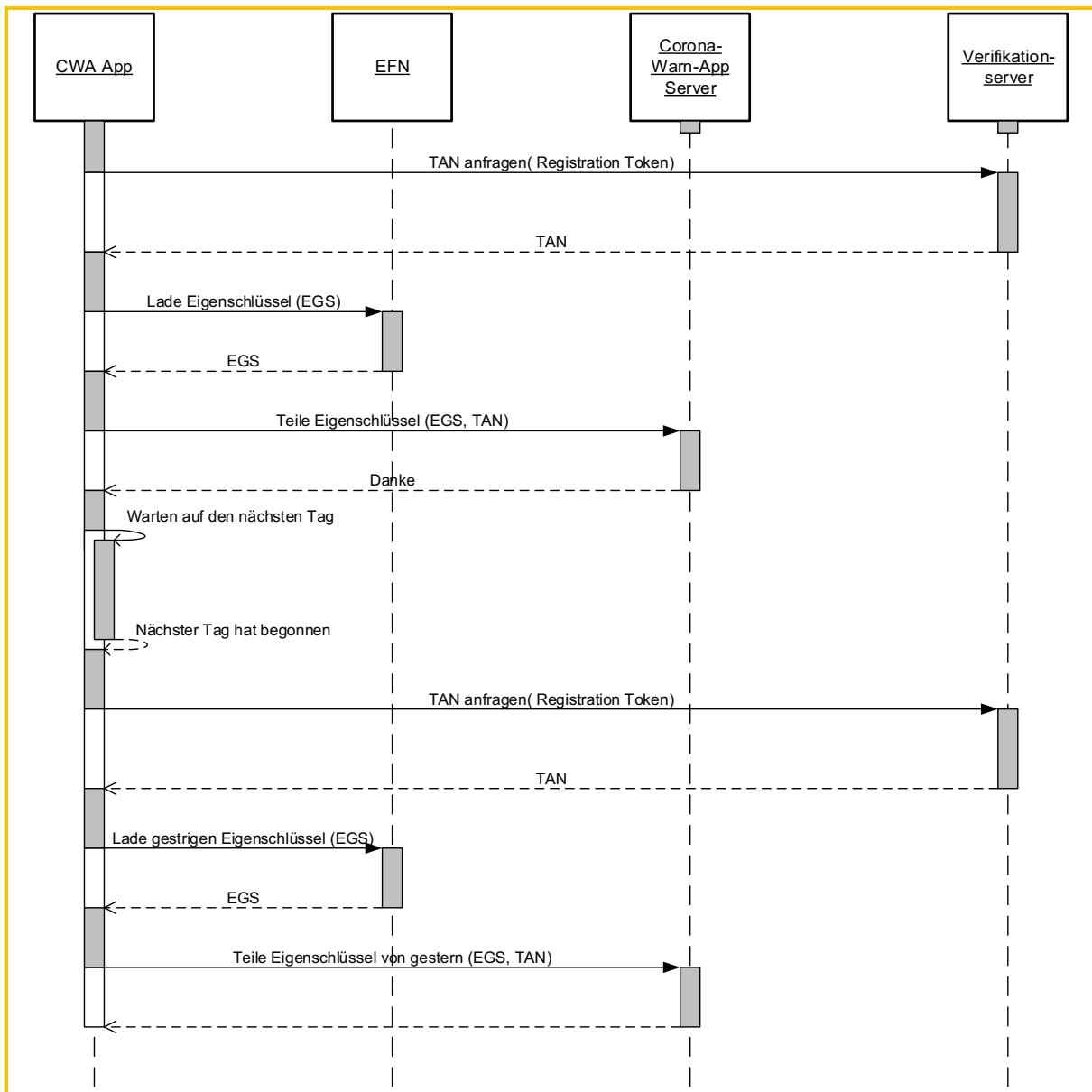


Abbildung 17: Ablauf beim Bereitstellen der Eigenschlüssel durch hochladen auf den CWA Server

Zudem werden auch Positivschlüssel-Metadaten an den CWA Server übermittelt. Nach der Speicherung der Positivschlüssel auf dem CWA Server werden die Positivschlüssel (im Kontext der Interoperabilität) auch als Diagnoseschlüssel bezeichnet. Sie werden auf dem CWA Server um zusätzliche Positivschlüssel-Metadaten ergänzt, die dazu dienen, den Verantwortlichen der anderen nationalen Corona-Apps die Herkunft der Positivschlüssel und Angaben über die Art der Verifikation der Diagnose mitzuteilen. Dadurch können Unterschiede der jeweiligen nationalen Anforderungen an die zugelassenen Testverfahren berücksichtigt werden und bspw. die Berücksichtigung von weniger diagnosegenauen Selbsttests bei der Risiko-Ermittlung verhindert werden.

Der CWA Server speichert hierfür die von der CWA App erhaltenen Positivschlüssel einschließlich des darin enthaltenen Werts zum Symptombeginn „**days since onset of symptoms**“ (**DSOS**) ab und ergänzt die Positivschlüssel-Metadaten zur Art der Verifikation und die Länderkennung „DE“.

Anschließend übermittelt der CWA Server folgende Daten an den EFGS:

- Positivschlüssel (einschließlich des enthaltenen Werts „days since onset of symptoms“)
- ReportType (Verified Test)
- Länderkennung (DE)

Der EFGS wandelt diese Daten in ein Standardformat um, das für alle Server der einzelnen nationalen Corona-Apps lesbar ist. Am EFGS stehen die standardisierten Daten dann für diese Server der einzelnen nationalen Corona-Apps zur Verfügung.

Die Server der einzelnen nationalen Corona-Apps leiten aus dem Wert „days since onset of symptoms“ und der Angabe zum ReportType entsprechend ihrer nationalen Bewertungseinstellungen zur sachgerechten Pandemie-Prävention einen Wert für das TransmissionRiskLevel jedes Positivschlüssels ab. Die Positivschlüssel der anderen nationalen Corona-Apps können dadurch mit den vorliegenden Positivschlüsseln der Nutzer der jeweiligen nationalen Corona-Apps einheitlich im Rahmen der Risiko-Ermittlung berücksichtigt werden und an die eigenen Nutzer verteilt werden.

Die Übermittlung der Positivschlüssel (einschließlich der etwaigen zusätzlichen Angaben) an den CWA Server und von dort an den EFGS erfolgt nur nach ausdrücklicher Einwilligung der CWA-Nutzer. Die Kommunikation zwischen dem CWA Server und dem EFGS erfolgt verschlüsselt. Im EFGS werden Daten zudem verschlüsselt gespeichert.

Am EFGS zur Verfügung stehende Positivschlüssel der CWA-Nutzer stehen den Verantwortlichen der nationalen Corona-Apps gemeinsam und unterschiedslos zur Verfügung. Eine nur teilweise Freigabe für bestimmte nationale Corona-Apps bzw. Mitgliedstaaten erfolgt nicht und ist weder rechtlich in dem dem EFGS zugrundeliegenden Durchführungsbeschluss vorgesehen noch technisch angelegt. Die am EFGS teilnehmenden Verantwortlichen können jeweils entscheiden, ob und in welcher Weise sie die Positivschlüssel der Nutzer der anderen nationalen Corona-Apps im Rahmen der eigenen Risiko-Ermittlung berücksichtigen oder nicht (z. B. weil bestimmte als weniger sicher erachtete Verifikationsmethoden nicht den eigenen Anforderungen an einen verifizierten positiven Test entsprechen).

Die Zwecke, für die die am EFGS abgerufenen Positivschlüssel verwendet werden dürfen, und die Anforderungen an die Rechtsgrundlage für die Übermittlung der Positivschlüssel an den EFGS sind zwischen den gemeinsamen Verantwortlichen koordiniert und sie werden im Rahmen des Antragsverfahrens zur Teilnahme am EFGS von den gemeinsam Verantwortlichen geprüft.

5.6.6 Deinstallation der CWA App

Deinstalliert der CWA-Nutzer die CWA App auf dem Smartphone, werden dadurch sämtliche von der CWA App gespeicherten Daten vom Smartphone gelöscht.

Durch diesen Schritt nicht gelöscht werden die Daten, die durch das jeweilige Betriebssystem gespeichert und verwaltet werden. Dies sind der Verschlüsselungsschlüssel in der KeyChain sowie die Daten in der Begegnungsaufzeichnung des ENF des Betriebssystems.

Auch eine Löschung bereits an den CWA Server übermittelter und von dort an den EFGS und die Server der anderen nationalen Corona-Apps zur Verfügung gestellter Daten erfolgt in Folge der Löschung der CWA App auf dem Smartphone nicht. Diese Daten werden nach Ablauf der jeweiligen Löschfristen automatisiert gelöscht.

5.7 Kategorien von Daten

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

- Zugriffsdaten (Anwendungsphasen 1, 3 und 4)
- Tagesschlüssel (Anwendungsphasen 1, 3 und 4)
- RPIs (Anwendungsphasen 1 und 2)
- Metadaten zu fremden RPIs (Anwendungsphasen 1 und 2)
- Positivschlüssel (bzw. Diagnoseschlüssel) (Anwendungsphasen 1, 2 und 4)
- Metadaten zu Positivschlüsseln (bzw. Diagnoseschlüsseln) (Anwendungsphase 4)
- Bewertungseinstellungen (BWE) (Anwendungsphasen 1, 2 und 4)
- TANs (Anwendungsphasen 3 und 4)
- Registration Token (Anwendungsphasen 3 und 4)
- QR-Code / GUID (Anwendungsphase 3)
- Risikowert (Total Risk Score) (Anwendungsphasen 1 und 2)
- Risikostatus (Anwendungsphasen 1 und 2)
- Name und Telefonnummer (Verifikations-Hotline) (Anwendungsphasen 3 und 4)
- Antworten auf Plausibilitätsfragen (Verifikations-Hotline) (Anwendungsphasen 3 und 4)

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

5.7.1 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, ob der Abruf erfolgreich war

Die Kommunikation des CWA Servers mit dem EFGS beinhaltet keine Requests der CWA App einzelner CWA-Nutzer. Die technischen Zugriffsdaten dieser Kommunikation betreffen nicht die Endgeräte natürlicher Personen.

5.7.2 Tagesschlüssel (TEK)

Der Tagesschlüssel ist eine Datenstruktur. Es handelt sich um einen täglich im ENF neu zufällig generierten Wert. Die Speicherung und Verwaltung der Tagesschlüssel erfolgt im ENF. 14 Tage nach der Generierung wird ein Tagesschlüssel automatisch aus dem ENF gelöscht. Die CWA App erhält nur im Rahmen der Warnfunktion die Tagesschlüssel (auch: Eigenschlüssel (EGS), die nach der Bereitstellung als Positivschlüssel oder Diagnoseschlüssel bezeichnet werden).

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

Ein Tagesschlüssel besteht aus den folgenden Datenfeldern:

RollingPeriod:

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

RollingStartNumber:

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

TransmissionRiskLevel:

Dieses Datenfeld hat einen Wert zwischen 0 und 8. Es wird benutzt, um die Wahrscheinlichkeit zu beschreiben, mit der ein positiv getesteter Nutzer andere Nutzer infizieren könnte. Der gesetzte Wert ist das Ergebnis der wissenschaftlichen Betrachtung üblicher Infektionsverläufe. Es fließen hier beispielsweise epidemiologische Erkenntnisse über Symptomstärke, Symptomstartpunkt oder den Testzeitpunkt in diesen Risikowert ein.¹⁶

KeyData:

Dieses Datenfeld enthält den eigentlichen Tagesschlüssel, auf welchen sich die anderen Datenfelder des Tagesschlüssels beziehen.

DaysSinceOnsetOfSymptoms:

Dieser Wert stellt die Differenz in Tagen zwischen der RollingStartNumber und dem Beginn von Symptomen dar. Diese Information ist Bestandteil der Tagesschlüssel, sobald diese zu Positivschlüsseln werden, indem sie an den CWA Server gesendet werden.

5.7.3 RPI

Die eigenen RPIs (Rolling-Proximity-Identifier) des CWA-Nutzers werden durch das ENF aus dem jeweils aktuell gültigen Tagesschlüssel abgeleitet und alle 10 bis 20 Minuten geändert. Die jeweils letzte RPI wird über die Bluetooth-Schnittstelle ausgesendet und kann von anderen Personen mit aktiviertem ENF (unabhängig von der jeweiligen Corona-App) empfangen werden. Nach Ablauf von 14 Tagen seit der Generierung wird eine RPI automatisch aus der Begegnungsaufzeichnung des ENF gelöscht.

Anhand eines Tagesschlüssels, aus dem ein RPI abgeleitet worden ist, können die später aus demselben Tagesschlüssel abgeleiteten RPIs berechnet werden. Ohne Kenntnis der zugrundeliegenden Tagesschlüssel hingegen kann aus einem RPI weder auf den zugrundeliegenden Tagesschlüssel noch auf andere RPIs geschlossen werden.

Die eigenen RPIs des CWA-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.

¹⁶ Google: Exposure Notifications API, abrufbar unter: <https://developers.google.com/android/exposure-notifications/exposure-notifications-api#data-structures> (abgerufen am 15.10.2020).

5.7.4 RPI-Metadaten

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 positiv getesteten Person (exposure) in 5er Schritten (<5/5/10/15/20/25/30/>30 Minuten)

Im Kontaktfall übergibt das ENF diese RPI-Metadaten im Rahmen der Risiko-Ermittlung an die CWA App, die unter Verwendung dieser Daten dann den Total Risk Score hinsichtlich dieses Kontakts berechnet.

5.7.5 Positivschlüssel (Diagnoseschlüssel)

Ein Positivschlüssel ist ein „umgewidmeter“ Tagesschlüssel eines Nutzers, der in der CWA App oder einer anderen nationalen Corona-App eine Warnung ausgelöst hat.

Wenn ein CWA-Nutzer eine Warnung auslöst, werden die im ENF gespeicherten Tagesschlüssel der letzten 14 Tage vom ENF mit der Einwilligung des CWA-Nutzers und nach der vom Betriebssystem eingeholten Freigabe des CWA-Nutzers an die CWA App übergeben und von dieser dann gebündelt an den CWA Server übermittelt. Von dort werden sie am EFGS den Verantwortlichen der anderen nationalen Corona-Apps zur Verfügung gestellt, um die länderübergreifende Risiko-Ermittlung zu ermöglichen.

Vor der Übermittlung durch die CWA App an den CWA Server ergänzt die CWA App das Datenfeld „transmissionRiskLevel“ des Positivschlüssels. Dieses wird abhängig von den Angaben des CWA-Nutzers zum Symptombeginn auf einen Wert zwischen 0 und 8 gesetzt. Wenn der CWA-Nutzer keine Angaben zum Symptombeginn macht, werden Standardwerte ausgehend vom Zeitpunkt des Testergebnisabrufs gesetzt.

5.7.6 Metadaten zu Positivschlüsseln

Nach Eingang der Positivschlüssel auf dem CWA Server werden von diesem folgende Metadaten technisch für alle über die CWA App zur Verfügung gestellten Positivschlüssel ergänzt:

- Das Datenfeld „reportType“ wird abhängig von der Diagnoseart auf einen Wert zwischen 0 und 5 gesetzt. Da Warnungen mit der CWA App nur bei Vorliegen eines

labordiagnostischen Befunds ausgelöst werden können, ist der Wert für alle CWA-Nutzer stets (1=Confirmed_Test).

- Das Ursprungsland des Positivschlüssels wird im Datenfeld „CountryOfOrigin“ in Form der Länderkennung „DE“ ergänzt.

5.7.7 Bewertungseinstellungen (BWE)

Bei den Bewertungseinstellungen (BWE, Exposure Parameter Configuration) handelt es sich um eine komplexe Datenstruktur, die die Konfigurationseinstellung für die Analyse und die Risikobewertung der Kontakte beinhaltet. Das Ergebnis der Berechnung ist der Total Risk Score. Die BWE werden vom RKI herausgegeben und aktualisiert. Es können auf diese Weise neueste 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 von 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.

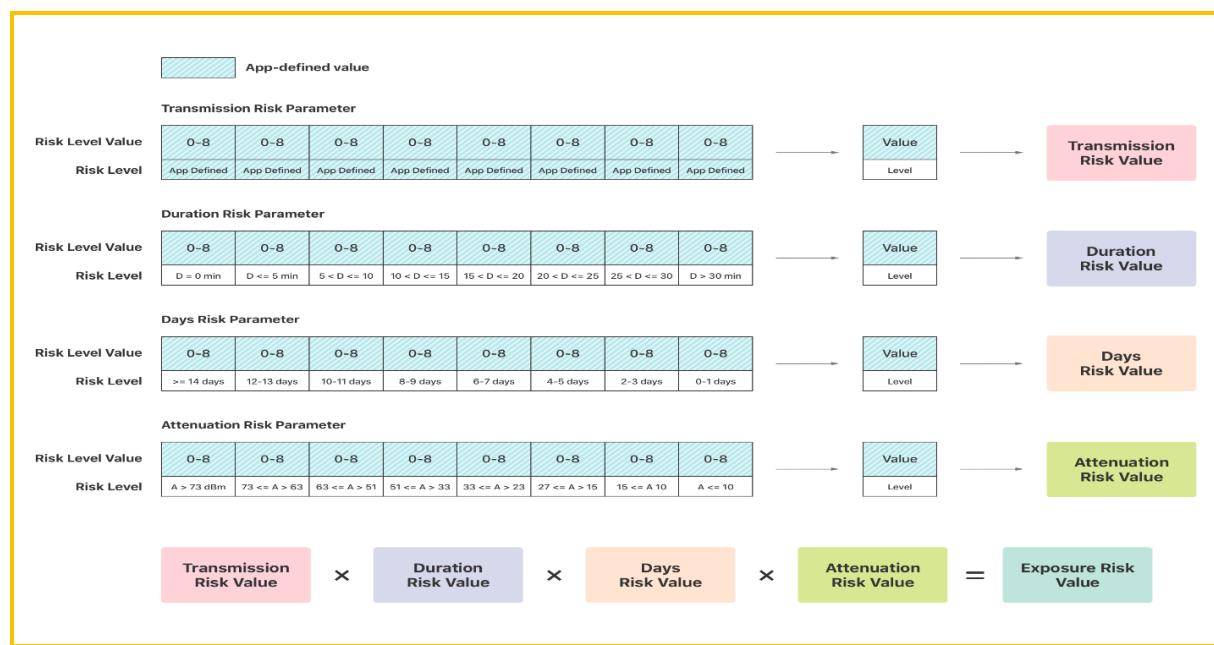


Abbildung 18: Übersicht über Risikoparameter (Quelle: Apple/Google)

5.7.8 TANs

Die TAN ist eine einmal verwendbare Transaktionsnummer, die beim Abruf des Testergebnisses automatisch generiert und dann in der CWA App abgelegt wird. Hat ein CWA-Nutzer im Rahmen der länderübergreifenden Warnfunktion in die Übermittlung der Positivschlüssel eingewilligt, wird die TAN gemeinsam mit den Positivschlüsseln an den CWA Server übermittelt. Dieser überprüft die Gültigkeit der TAN mit Hilfe des Verifikationsservers und gibt dann die Verarbeitung der Positivschlüssel frei.

5.7.9 Registration Token

Das Registration Token wird nach Auslesen der in einem QR-Code enthaltenen einzigartigen Kennung (GUID) vom Verifikationsserver erstellt und an die CWA App übermittelt. Das Registration Token dient als zusätzlicher Schritt der Verifikation des CWA-Nutzers und ermöglicht gleichzeitig die technische Zuordenbarkeit zur Kommunikation mit dem Verifikationsserver, um ein Testergebnis abzufragen.

5.7.10 QR-Code / GUID

Der QR-Code wird einer Person bei Durchführung eines Corona-Tests mit Abnahme der Probe auf einem Probenbegleitschein ausgedruckt übergeben. Er dient der Zuordnung des Corona-Tests. Der QR-Code enthält eine einzigartige Kennung (GUID), welche der CWA-Nutzer im Rahmen der Verifikation des Tests innerhalb der CWA App über die Kamerafunktion seines Smartphones scannen kann. Die CWA App übermittelt dann einen Hashwert der GUID an den Verifikationsserver und erhält vom Server das Registration Token zurück, das für die Abfrage des Testergebnisses notwendig ist. Der Verifikationsserver speichert den Hashwert der GUID zusammen mit dem Registration Token, der ausgehändigte QR-Code wird damit als entwertet markiert, ein erneuter Scan führt nicht zur Rückgabe eines neuen Registration Token. Das Testergebnis kann nicht mehr von anderen mobilen Endgeräten mit installierter CWA App abgerufen werden.

5.7.11 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 ein Match gibt, übergibt das ENF die in der Begegnungsaufzeichnung gespeicherten Angaben zur Kontaktzeit, 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.

Aufgrund der Interoperabilität der nationalen Corona-Apps werden sowohl Kontakte zwischen CWA-Nutzern untereinander als auch mit anderen Nutzern berücksichtigt und die entsprechenden Angaben (Dauer, Datum und Dämpfungswert) durch das ENF an die CWA App weitergegeben.

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

Für die Berechnung des Total Risk Score wird das Produkt aus einem Abstandsfaktor (attenuationLevelValue), einem Faktor der vergangenen Zeit zum Kontakt (daysSinceLastExposureLevelValue), einem Faktor der Dauer des Kontaktes (durationLevelValue) und dem Übertragungs-Risiko-Faktor (transmissionRiskLevelValue) gebildet:

$$\text{TotalRiskScore} = (\text{attenuationLevelValue}) * (\text{daysSinceLastExposureLevelValue}) * (\text{durationLevelValue}) * (\text{transmissionRiskLevelValue})$$

Der Abstandsfaktor wird dabei wie folgt ermittelt: Mit Hilfe des empfangenen Positivschlüssels und des daraus errechneten RPI werden die verschlüsselten RPI-Metadaten des empfangenen Bluetooth Signals entschlüsselt. Von der darin enthaltenen Sendesignalstärke wird die Empfangsstärke des Signals subtrahiert. Der sich ergebene Wert (Dämpfungswert) wird als Maß für die Entfernung betrachtet und als Abstandsfaktor verwendet.

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

Auf dem Homes-Bildschirm der CWA App wird angezeigt, dass und welches Ansteckungsrisiko ermittelt worden ist. Zudem werden dem CWA-Nutzer Handlungsempfehlungen, basierend auf dem ermittelten Risikostatus, angezeigt.

Bei einer erneuten, späteren Ermittlung des Risikostatus werden nur die aktuellen Positivschlüssel vom CWA Server geladen, die noch nicht in vorherige Bewertungen eingeflossen waren. Um dies zu gewährleisten, wird das Datum des letzten Downloads der Positivschlüssel in der CWA App gespeichert.

5.7.12 Risikostatus

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

- Unbekanntes Risiko
- Niedriges Risiko

- Erhöhtes Risiko

Der Risikostatus wird ausschließlich in der CWA App gespeichert und nicht an andere Empfänger (auch nicht an das RKI, Apple, Google und sonstige Dritte) weitergegeben.

5.7.13 Name und Telefonnummer (Verifikations-Hotline)

Im Rahmen der Verifikations-Hotline werden Telefonnummer und Name des anrufenden CWA-Nutzers erfragt und notiert. Die physische Aufzeichnung des Namens und der Telefonnummer werden spätestens nach Ablauf einer Stunde gelöscht.

5.7.14 Antworten auf Plausibilitätsfragen (Verifikations-Hotline)

Im Rahmen der Verifikations-Hotline stellen Mitarbeiter den Anrufern Plausibilitätsfragen, um die Gefahr eines Missbrauchs des **Corona-Warn-Systems** durch Falschmeldungen zu verringern. Wenn der Mitarbeiter die Antworten für plausibel hält, ruft er den Anrufer unter der angegebenen Telefonnummer zurück und teilt ihm eine teleTAN mit.

5.8 Löschung der Daten

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

5.8.1 Löschung der im Rahmen der Risiko-Ermittlung und Berechnung des Infektionsrisikos verarbeiteten Daten

Für alle im Rahmen der Risiko-Ermittlung (Anwendungsphase 1) und der Berechnung des Infektionsrisikos (Anwendungsphase 2) verarbeiteten Daten erfolgt eine automatisierte Löschung nach Eintritt bestimmter Ereignisse oder nach Zeitablauf.

In der CWA App gespeicherte Positivschlüssel anderer Nutzer werden nach 14 Tagen automatisch aus dem Speicher der App gelöscht. Über die Einstellung in der CWA App zum Zurücksetzen der CWA App oder durch Löschung der CWA App kann eine vorzeitige Löschung angestoßen werden.

Im Kontaktprotokoll des ENF werden Positivschlüssel anderer Nutzer ebenfalls automatisch nach 14 Tagen gelöscht.

Auf die im ENF gespeicherten Daten und die diesbezüglichen Löschräten und -routinen haben das RKI und die Verantwortlichen anderer nationaler Corona-Apps keinen Einfluss. Die Löschung der im ENF gespeicherten fremden RPIs, der Metadaten der fremden RPIs, der eigenen Tagesschlüssel sowie der auf fremden Smartphones gespeicherten RPIs und

diesbezüglichen Metadaten der CWA-Nutzer ist Bestandteil der von Apple und Google bereitgestellten Systemkomponenten. Gegenwärtig erfolgt die automatische Löschung der genannten Datenkategorien im ENF nach 14 Tagen. Über die Systemeinstellungen der Betriebssysteme haben CWA-Nutzer die Möglichkeit, eine vorzeitige Löschung der im ENF gespeicherten Daten anzustoßen.

Der in der CWA App angezeigte Risikostatus wird nach jeder Aktualisierung des Risikostatus im App-Speicher überschrieben. Die Aktualisierung des Risikostatus erfolgt in der Regel unmittelbar nachdem die Liste der aktuellen Positivschlüssel runtergeladen wurde. Eine Löschung des zuletzt ermittelten und angezeigten Risikostatus erfolgt spätestens nach 14 Tagen.

5.8.2 Löschung der im Rahmen der Testregistrierung verarbeiteten Daten

Für alle im Rahmen der Testregistrierung (Anwendungsphase 3) verarbeiteten Daten erfolgt eine automatisierte Löschung nach Eintritt bestimmter Ereignisse oder nach Zeitablauf.

Die GUID wird auf dem CWA Server nach 21 Tagen gelöscht. Die gehashte Kennzahl und das Testergebnis auf dem Test Result Server werden im Fall eines negativen Testergebnisses unmittelbar nach dem Abruf des Testergebnisses und im Fall eines positiven Testergebnisses unmittelbar nach dem Löschen der auf dem Serversystem gespeicherten Kopie der TAN gelöscht.

Das Gegenstück des Registration Token auf dem CWA Server wird ebenfalls nach 21 Tagen gelöscht.

Das Registration Token, das in der CWA App gespeichert ist, wird mit der Löschung der CWA App vom Smartphone oder unmittelbar nachdem der CWA-Nutzer eine Warnung auslöst und die Positivschlüssel übermittelt hat gelöscht.

5.8.3 Löschung der im Rahmen der Warnfunktion verarbeiteten Daten

Für alle im Rahmen der Funktion “Andere Warnen” (Anwendungsphase 4) verarbeiteten Daten erfolgt eine automatisierte Löschung nach Eintritt bestimmter Ereignisse oder nach Zeitablauf.

Auf dem CWA Server gespeicherte Positivschlüssel einschließlich der Angaben zum Symptombeginn werden automatisch nach 14 Tagen nach der Übermittlung gelöscht.

An den EFGS übermittelte und von anderen Servern der nationalen Corona-Apps abgerufene Positivschlüssel der CWA-Nutzer werden dort ebenfalls spätestens nach 14 Tagen gelöscht.

Die Kopie der TAN und die teleTAN, die auf dem CWA Server gespeichert sind, werden nach 21 Tagen gelöscht.

Die TAN und die teleTAN, die in der CWA App gespeichert sind, werden mit der Löschung der CWA App vom Smartphone oder unmittelbar nachdem der CWA-Nutzer die Funktion „Andere warnen“ ausgeführt und die Positivschlüssel übermittelt hat gelöscht.

Die teleTAN, die dem Mitarbeiter der Hotline übermittelt wird, wird direkt nach der telefonischen Weitergabe an den CWA-Nutzer gelöscht.

Die Kopie des Registration Token, das auf dem CWA Server gespeichert ist, wird nach 21 Tagen gelöscht.

Das Registration Token, das in der CWA App gespeichert ist, wird unmittelbar nachdem der CWA-Nutzer eine Warnung ausgelöst und die Positivschlüssel übermittelt hat, gelöscht.

5.8.4 Löschung der Zugriffsdaten

Zur Löschung von Zugriffsdaten siehe unter Ziffer 7.1.1.

5.9 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.

5.9.1 Betroffene Personen

Die betroffenen Personen sind die Nutzer. Dies umfasst begrifflich sowohl Personen, die die CWA App verwenden, als auch Personen, die eine andere nationale Corona-App verwenden.

5.9.2 Verantwortliche

Gemäß Art. 4 Nr. 7 DSGVO ist für die Verarbeitung **Verantwortlicher**, „wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

5.9.2.1 RKI

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.

5.9.2.2 Nationale Behörden und Stellen der am EFGS teilnehmenden Länder

Für die vom Prüfgegenstand umfasste Datenverarbeitung durch den EFGS zur Ermöglichung der Interoperabilität ist das RKI gem. Durchführungsbeschluss (EU) 2020/1023 der Kommission vom 15. Juli 2020 zur Änderung des Durchführungsbeschlusses (EU) 2019/1765 hinsichtlich des grenzüberschreitenden Datenaustauschs zwischen nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung zwecks Bekämpfung der COVID-19-Pandemie gemeinsam mit den zuständigen nationalen Behörden und amtlichen Stellen der am EFGS teilnehmenden Mitgliedstaaten verantwortlich.

5.9.3 Weitere Akteure

5.9.3.1 BMG

Die CWA ist ein „Projekt im Auftrag der Bundesregierung“.¹⁷

5.9.3.2 Apple/Google

Soweit personenbezogene 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” auch die Unternehmen Apple und Google als Anbieter des ENF 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 gegenwärtig nicht ersichtlich, sollte jedoch fortlaufend kritisch geprüft werden.

Für eine eigene Verantwortlichkeit von Apple und Google im Hinblick auf die im ENF erfolgende Datenverarbeitung spricht, dass diese das ENF nach ihren Vorstellungen und Designkriterien entwickelt und als eigene Systemkomponente in ihre jeweiligen Betriebssysteme integriert haben; die Speicherdauer von Tagesschlüsseln und RPIs, die möglichen Konfigurationsparamater der BWE und die Verfügbarkeit des ENF sowie die technischen Maßnahmen zur Gewährleistung der Sicherheit, Vertraulichkeit und Integrität der im ENF verarbeiteten Daten werden einseitig von Google und Apple festgelegt. Apps dürfen nur auf die Funktionen und Daten des ENF zugreifen, wenn die einseitig von Apple bzw. Google formulierten Vorgaben eingehalten werden. Änderungen an Verfahren und Vorgaben werden ebenso allein von Google und Apple festgelegt. Die Hersteller haben zudem die

¹⁷ Bundesregierung: Corona-Warn-App: Die wichtigsten Fragen und Antworten, Stand: 14. Oktober 2020, abrufbar unter: <https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392> (abgerufen am 15.10.2020).

Möglichkeit, die bestehenden Systemkomponenten zu eigenen vollwertigen Kontaktpersonennachverfolgungs-Systemen auszubauen.

Insoweit bestimmen Apple und Google den Zweck und die wesentlichen Mittel der Verarbeitung durch das ENF und sind dahingehend als eigenständige Verantwortliche anzusehen.

5.9.4 Auftragsverarbeiter

Für den Betrieb der CWA werden folgende **Auftragsverarbeiter** eingesetzt:

5.9.4.1 Nationale Auftragsverarbeiter

Mit dem Betrieb eines Teils der CWA-Komponenten hat das RKI folgende externe Dienstleister beauftragt. Die Datenverarbeitung durch diese Dienstleister erfolgt jeweils auf Grundlage eines schriftlichen Auftragsverarbeitungsvertrags nach Art. 28 Abs. 3 DSGVO.

5.9.4.1.1 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.

5.9.4.1.2 T-Systems International GmbH

Die T-Systems International GmbH (im Folgenden „TSI“) hat zusammen mit SAP die CWA entwickelt. TSI übernimmt den Applikationsbetrieb als Auftragsverarbeiter, wobei die CWA App in Containern in Kubernetes-Clustern der **Open Telekom Cloud** (OTC) läuft. In diesem Zusammenhang verarbeitet TSI die über die CWA App erzeugten technischen Zugriffsdaten, 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 TSI für den sogenannten 1st- und 2nd-Level-Support zuständig. Hierzu gehören insbesondere die Anwendungsüberwachung, die Ticketerstellung, Problemlösung, die Ursachenanalyse und Problembehandlung sowie der Betrieb und die Verwaltung der technischen Infrastruktur. Schließlich ist TSI für die technische Hotline und die Verifikations-Hotline zuständig, bei der

gegebenenfalls nach erfolgter Verifikation von Anrufern eine teleTAN generiert und übermittelt wird.

TSI 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), die wiederum die 3wphone GmbH als genehmigten weiteren Auftragsverarbeiter einbindet,
- Deutsche Telekom Technik GmbH (für das CDN-Magenta).

5.9.5 Betrieb des EFGS

Mit dem Betrieb und der Wartung des EFGS haben die zuständigen nationalen Gesundheitsbehörden der teilnehmenden Länder die EU-Kommission als Auftragsverarbeiter beauftragt.

Gemäß Art. 28 DSGVO und Art. 29 der Verordnung (EU) 2018/1725 erfolgt die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines Rechtsinstruments nach dem Recht der Union oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter an die Weisungen des Verantwortlichen bindet und die Verarbeitung regelt.

Die EU-Kommission hat die T-Systems International GmbH und die SAP Deutschland SE & Co. KG als Unterauftragsverarbeiter mit der technischen Bereitstellung und Verwaltung des gemeinsam betriebenen Warnsystems der teilnehmenden Länder beauftragt.

Die technischen und organisatorischen Einzelheiten der Zusammenarbeit werden in einem Beschluss der EU-Kommission festgelegt (Durchführungsbeschluss (EU) 2020/1023 vom 15. Juli 2020, abrufbar unter https://eur-lex.europa.eu/eli/dec_impl/2020/1023/oj).

5.10 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	Version
1	Datenschutzkonzept der CWA der Bundesrepublik Deutschland (Rahmendokument)	1.5
2	Datenschutzkonzept der CWA der Bundesrepublik Deutschland – Verifikation und Testergebnis	1.3
3	Datenschutzkonzept der CWA der Bundesrepublik Deutschland – CWA App	1.5
4	Datenschutzkonzept der CWA der Bundesrepublik Deutschland – CWA Server	1.3
5	Datenschutzkonzept der CWA der Bundesrepublik Deutschland – Verifikations-Hotline	1.1
6	Designentscheidungen bei der Entwicklung der Corona-Warn-App der Bundesrepublik Deutschland und des European Federation Gateway Service (EFGS)	1.5 und 1.2
7	Technisch-Organisatorische Maßnahmen	1.1
8	Datenschutzkonzept European Federation Gateway Service	1.2
9	Durchführungsbeschluss (EU) 2020/1023 der Kommission vom 15. Juli 2020 zur Änderung des Durchführungsbeschlusses (EU) 2019/1765 hinsichtlich des grenzüberschreitenden Datenaustauschs zwischen nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung zwecks Bekämpfung der COVID-19-Pandemie	/

6 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 in Rede stehenden Verfahrens zu fördern.

Da die betroffenen Personen alle Nutzer sind und daher ein sehr breites Spektrum der Bevölkerung verschiedener Länder 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. EDSA)¹⁸ und
- Stellungnahmen von Verbänden und Interessensgruppen¹⁹.

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

7 Datenschutzrechtliche Bewertung

Nachfolgend werden die maßgeblichen 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.

7.1 Umfang der Verarbeitung personenbezogener Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO). Die im Rahmen der CWA verarbeiteten Daten haben zumindest teilweise Personenbezug. In welchem Umfang das RKI personenbezogene Daten verarbeitet, wird im Folgenden dargestellt.

7.1.1 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 Warnen anderer Nutzer (Anwendungsphase 4),
- in Form von **Positivschlüsseln** und eindeutigen Kennungen (**Registration Token, TAN**) beim Warnen anderer Nutzer (Anwendungsphase 4) und

¹⁸ 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 (abgerufen am 15.10.2020).

¹⁹ 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 15.10.2020);

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> (abgerufen am 15.10.2020).

- in Form eindeutiger Kennungen (**GUID**) beim Registrieren eines Tests, jedoch jeweils nur solange, wie die vom CWA-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 eines 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 verarbeitet wird. Denn bei IP-Adressen handelt es sich 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.²⁰ 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 infolgedessen auch eine IP-Adresse einer natürlichen Person zuzuordnen, die ohne das Zusatzwissen des Dritten für das RKI durch die nicht auflösbare Pseudonymisierung faktisch anonym sind. Sofern und solange das RKI diese Daten in Verbindung mit einer IP-Adresse speichert oder anderweitig verarbeitet, handelt es sich für das RKI somit insgesamt um personenbezogene Daten.

Da seitens des RKI die IP-Adressen aus den Server-Logfiles auf dem CWA Server und CDN-Magenta unmittelbar nach Beantwortung eines Requests gelöscht werden, besteht der oben beschriebene Personenbezug in Verbindung mit einer IP-Adresse für das RKI jedoch nur für eine „technische Sekunde“.

Die Auswertung der IP-Adressen auf Infrastrukturebene im Rahmen des Betriebs des CWA Servers ist zeitlich stark begrenzt und durch die etablierten Sicherheitsprozesse zur Angriffserkennung in den DDoS Systemen definiert; die Verarbeitung wird nur dort systemintern vorgenommen. IP-Adressen werden in Echtzeit auf mögliches Angriffsverhalten hin untersucht. Nur IP-Adressen, die als Angreifer erkannt wurden, werden zur Gefahrenabwehr bis zu einer Stunde lang gespeichert. Zur Wahrung und zum Nachweis der Systemintegrität der gesamten OTC werden zudem statistische Reports erstellt, die selbst keine IP-Adressen enthalten. Zur Erstellung dieser Reports werden Stichproben aus den Angreifer-IP-Adressen – und nur aus diesen (Stichprobenumfang circa 1:1000) – bis zu 7 Tage gespeichert.

Die beiden Betriebsebenen (Applikation und Infrastruktur) sind organisatorisch und räumlich getrennt. Mit dem Infrastruktur-Betrieb der OTC und den Applikationsbetrieben der CWA sind insgesamt fünf unterschiedliche Betriebsteams betraut. Die IP-Adressen der Netzwerkverbindung werden bereits auf dem vorgelagerten Load Balancer maskiert und erreichen den CWA Server nicht.

²⁰ EuGH, Urt. v. 19.10.2016, Rs. Breyer, C-582/14.

7.1.2 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 CWA-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 unmittelbarste Einflussmöglichkeit hinsichtlich des Ablaufs der lokalen Datenverarbeitung durch die CWA App und das ENF haben einerseits der CWA-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 der Nutzer unauflösbare Pseudonyme und 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 im Sinne einer unauflösaren **Pseudonymisierung** 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 wird. 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 Drittewissen 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 faktische

Anonymität oder Unauflöslichkeit von Pseudonyme aufzuheben.²¹ Wenn man davon ausgeht, dass das RKI vernünftigerweise keine entsprechenden Maßnahmen ergreifen kann oder wird, 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. Gleichwohl muss das Risiko einer Identifikation durch andere Stellen wie insbesondere die Hersteller des ENF im Rahmen dieser DSFA in den Blick genommen und erforderlichenfalls durch entsprechende Maßnahmen zur Risikobehandlung behandelt werden.

Der BfDI hat im Rahmen seiner projektbegleitenden Beratung 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.²²

7.1.3 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 ein Nutzer einen bestimmten Risikostatus hat oder sich testen ließ, als Gesundheitsdatum einzustufen. Denn aus diesen Informationen geht hervor, dass eine erhöhte Wahrscheinlichkeit einer COVID-19-Erkrankung des Nutzers besteht. Gesundheitsdaten sind **besondere Kategorien personenbezogener Daten** gem. Art. 9 Abs. 1 DSGVO.

Bei den Tagesschlüsseln des CWA-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,

²¹ Vgl. zusammenfassend und m.w.N. bei: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 4 Nr. 1 Rn. 61 und 64.

²² 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.“

könnten die Tagesschlüssel allenfalls vorsorglich als Gesundheitsdaten betrachtet werden. Dies erscheint jedoch nicht sachgerecht. Denn die CWA App wird voraussichtlich ganz 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 CWA-Nutzers zu. Der Tagesschlüssel erlaubt nur den Rückschluss, dass der Träger dieses Pseudonyms ein Nutzer der CWA App ist. Zudem hat es allein der CWA-Nutzer in der Hand, ob eine Umwidmung seiner Tagesschlüssel zu Positivschlüsseln erfolgt, nämlich indem er ausdrücklich bestätigt und einwilligt, dass sein Testergebnis mit anderen Nutzern nationaler Corona-Apps geteilt wird.

Bei der vom CDN-Magenta heruntergeladenen Liste der Positivschlüssel anderer Nutzer, die lokal auf dem Smartphone des CWA-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 eine Risiko-Begegnung 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 CWA-Nutzer entweder ein erhöhtes Ansteckungsrisiko und somit einer COVID-19-Erkrankung besteht oder er bereits positiv getestet ist.

Daher handelt es sich auch bei den im Rahmen des Verifikations-Hotline-Prozesses verarbeiteten personenbezogenen Daten um Gesundheitsdaten, weil davon auszugehen ist, dass sie sich auf einen positiv getesteten CWA-Nutzer beziehen.

7.2 Rechtsgrundlagen

Eine Datenverarbeitung ist nur dann rechtmäßig, wenn sie durch eine wirksame Einwilligung oder einen anderen Zulässigkeitstatbestand legitimiert wird und im Einklang mit den in Art. 5 DSGVO festgelegten Grundsätzen erfolgt. Die Zulässigkeitstatbestände ergeben sich in erster Linie aus Art. 6 DSGVO sowie aus Art. 9 DSGVO, soweit Gesundheitsdaten verarbeitet werden. Für die in der DSGVO festgelegten Rechtsgrundlagen gibt es keine Rangfolge, d. h. eine Einwilligung ist nicht per se besser oder schlechter als eine andere Rechtsgrundlage geeignet.

7.2.1 Anforderungen an eine Rechtsgrundlage

An die verschiedenen möglichen Rechtsgrundlagen im Rahmen der CWA statuiert die DSGVO folgende Anforderungen.

7.2.1.1 Einwilligung

Die Wirksamkeitsvoraussetzungen einer Einwilligung ergeben sich aus Art. 4 Nr. 7 DSGVO in Verbindung mit Art. 6 Abs. 1 S. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DSGVO sowie Art. 7 DSGVO. Eine wirksame Einwilligung ist demnach jede

- freiwillig,
- für den bestimmten Fall,
- in Kenntnis der Sachlage 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.²³

7.2.1.2 Nationale Rechtsvorschriften

Art. 6 Abs. 1 lit. c oder e DSGVO in Verbindung mit den Ausnahmen nach Art. 9 Abs. 2 lit. i oder j DSGVO können eine Rechtsgrundlage für die Verarbeitung personenbezogener (Gesundheits-) Daten für die Zwecke einer Corona-Tracing-App darstellen.

Gemäß Art. 9 Abs. 2 lit. h und i DSGVO müssen diese Vorschriften „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses“ vorsehen. Gleichermassen ist es nach Art. 9 Abs. 2 lit. j DSGVO erforderlich, dass das Recht eines Mitgliedstaats „in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht“. Ferner sind solche Rechtsvorschriften im Lichte der Grundsätze nach Art. 5 DSGVO und unter Berücksichtigung der EuGH-Rechtsprechung auszulegen.

²³ Siehe zu diesen Anforderungen im Einzelnen European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679, Version 1.1, Abschnitt 3, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (zuletzt abgerufen am 15.10.2020).

7.2.2 Rechtsgrundlagen der CWA

Die in Betracht kommenden Rechtsgrundlagen der Datenverarbeitung im Rahmen der CWA hängen davon ab, ob es sich bei den betroffenen Personen um CWA-Nutzer oder um Nutzer anderer nationaler Corona-Apps handelt.

7.2.2.1 Verarbeitung von Daten der CWA-Nutzer

Rechtsgrundlage für die Verarbeitung personenbezogener Daten von CWA-Nutzern ist jeweils die Einwilligung des betroffenen CWA-Nutzers (Art. 4 Nr. 7 DSGVO, Art. 6 Abs. 1 S. 1 lit. a DSGVO). Da in weiten Teilen Gesundheitsdaten verarbeitet werden, gelten insoweit ergänzend die Anforderungen von Art. 9 Abs. 2 lit. a DSGVO. Für die Verarbeitung in den unterschiedlichen Anwendungsphasen der CWA App werden situativ jeweils separate zweck- bzw. funktionsspezifische Einwilligungen eingeholt. Die Einwilligungen der CWA-Nutzer werden, soweit möglich und sachgerecht, in der CWA App eingeholt. 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.

Zur Begründung der Wahl der Einwilligung als Rechtsgrundlage siehe Abschnitt 7.2.3.

7.2.2.2 Verarbeitung von Daten anderer Nutzer (EFGS)

Die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten von Nutzern anderer nationaler Corona-Apps für die Bereitstellung der länderübergreifenden Funktionen im Zusammenhang mit dem EFGS wird von den jeweils erhebenden nationalen Verantwortlichen (nationale Gesundheitsbehörden oder entsprechende amtliche Stellen) festgelegt.

Da alle für die nationalen Corona-Apps Verantwortlichen der DSGVO unterliegen, kommen als Rechtsgrundlagen des RKI für die Verarbeitung der Daten anderer Nutzer im Rahmen der CWA neben Einwilligungen der Nutzer anderer nationaler Corona-Apps auch nationale Rechtsvorschriften der jeweiligen teilnehmenden Länder in Betracht.

Im Rahmen der Antragstellung auf Teilnahme am EFGS wird vom jeweils antragstellenden Verantwortlichen eine Erklärung über die Rechtsgrundlage für die Verarbeitung im Rahmen des EFGS abgegeben, die von den Vertretern der am EFGS teilnehmenden Länder geprüft wird.

7.2.3 Begründung der Einwilligung als Rechtsgrundlage

Von verschiedenen Seiten wurden im Vorfeld der Veröffentlichung der CWA App Zweifel am Vorliegen der Wirksamkeitsvoraussetzungen einer Einwilligung für die Datenverarbeitung im

Rahmen der CWA geäußert.²⁴ Aus diesem Anlass wird nachfolgend dargestellt, auf welchen Erwägungen die Entscheidung des RKI für die Einwilligung als Rechtsgrundlage trotz der geäußerten Bedenken beruht.

Da sich die am EFGS teilnehmenden Verantwortlichen verbindlich verpflichtet haben, dass die Nutzung ihrer jeweiligen nationalen Corona-App freiwillig ist und die Datenverarbeitung im Einklang mit der DSGVO stehen muss, gelten die Erwägungen entsprechend auch für die grundsätzliche Bewertung der von einem anderen Verantwortlichen ggf. eingeholten Einwilligungen.

7.2.3.1 Wirksamkeitsvoraussetzungen einer Einwilligung

Die Wirksamkeitsvoraussetzungen einer Einwilligung ergeben sich aus Art. 4 Nr. 7 DSGVO in Verbindung mit Art. 6 Abs. 1 S. 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.

Die vom RKI eingeholten Einwilligungen der CWA Nutzer genügen diesen Wirksamkeitsvoraussetzungen:

7.2.3.1.1 Zweckbestimmtheit

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

- Für die länderübergreifende Risiko-Ermittlung,
- für die Testregistrierung (einschließlich des Testabrufs),
- für die länderübergreifende Warnung anderer und
- für die Nutzung der Verifikations-Hotline.

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“²⁵.

Da die oben genannten Funktionen bzw. Zwecke klar abgrenzbar und aus der Sicht eines Nutzers, der sich bewusst für die Installation der CWA App bzw. die Nutzung der einzelnen

²⁴ 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 15.10.2020) wenn möglich, die Nutzung einer gesetzlichen Rechtsgrundlage, da es an der Freiwilligkeit fehlen könnte.

Vgl. auch netzpolitik.org: EU-Abgeordnete hinterfragen Contact Tracing, abrufbar unter: <https://netzpolitik.org/2020/eu-abgeordnete-hinterfragen-contact-tracing/> (abgerufen am 15.10.2020).

²⁵ Klement in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, DSGVO Art. 7, Rn. 68.

Funktionen entscheidet, jeweils nachvollziehbar sind, ist nicht anzunehmen, dass der Zweck der Einwilligung nicht ausreichend bestimmt werden kann. Die Einwilligungen erfolgen situativ im jeweiligen Zusammenhang mit der Auslösung einer Funktion (z.B. beim Auslösen der Warnung anderer Nutzer oder im Rahmen eines Tests im Hinblick auf die Abrufmöglichkeit des Testergebnisses in der CWA App) und jeder Einwilligung geht eine konkrete Erläuterung des Zweckes und Verarbeitungszusammenhangs voraus.

Die Einwilligungserteilung erfolgt jeweils durch eine dem jeweiligen Kontext entsprechende geeignete und eindeutige bestätigende Handlung (z.B. durch Antippen eines entsprechenden Buttons, mündliche Erklärung im Rahmen der Verifikations-Hotline oder Erklärung zum Testabruf im Rahmen eines Tests).

Die spezifische Zweckbindung für die länderübergreifenden Aspekte der Funktionen im Zusammenhang mit dem EFGS ist in Artikel 7a Absatz 1 des Durchführungsbeschlusses (EU) 2019/1765 der EU-Kommission vorgeschrieben. Für die länderübergreifende Komponente der Risiko-Ermittlung wird keine separate Einwilligung eingeholt, sobald die CWA App ab Version 1.5 keine rein nationale Verwendung mehr vorsieht. Die Einwilligungserklärung im Rahmen der Aktivierung der Risiko-Ermittlung erfolgt nur einheitlich in Bezug auf alle nationalen Corona-Apps. CWA-Nutzer müssen und können die Herkunft der Positivschlüssel nicht länderspezifisch auswählen. Daher wird auch im Rahmen des Starts nach dem Update auf Version 1.5 (vgl. Ziffer 5.4.2.2) keine separate Einwilligung eingeholt, sondern die Datenverarbeitung auf die ursprüngliche Einwilligung des CWA-Nutzers zur Datenverarbeitung in Zusammenhang mit der Risiko-Ermittlung gestützt. Durch die Einführung der länderübergreifenden Komponente ändert sich die Verarbeitung personenbezogener Daten des CWA-Nutzers im Rahmen der Risiko-Ermittlung nicht. Der CWA-Nutzer erhält fortan nur potentiell zusätzliche Positivschlüssel - nunmehr auch von Nutzern anderer nationaler Corona-Apps.

Um die Zweckbestimmtheit fortwährend zu gewährleisten, muss die Transparenz der Einwilligungserklärungen sprachlich und optisch sichergestellt sein. Auch grafische und textliche Gestaltung der Bestätigungsbuttons dürfen keinen Zweifel am Bestätigungswillen des CWA-Nutzers zulassen.

Diese Anforderungen sind gegenwärtig erfüllt. Die Zwecke sind in der jeweiligen Situation konkret dargelegt und die Einwilligungserklärungen knüpfen an die einleitenden Erläuterungstexte an. In jeder Einwilligungserklärung wird die erklärende Handlung (bspw. Antippen des Buttons "Einverstanden") konkret benannt.

Im Rahmen der Verifikations-Hotline wird die Einwilligung fernmündlich eingeholt. In diesem Fall wird auf die verständliche mündliche Erläuterung der Datenverarbeitung Wert gelegt und eine eindeutige bestätigende Aussage des CWA-Nutzers eingeholt. Die Mitarbeiter der Verifikationshotline halten sich hierfür an ein vorgegebenes Skript, das auf die telefonische Erläuterung der Verarbeitung und die Erklärung der Einwilligung in diesem Medium abgestimmt ist.

Im Rahmen eines Tests bei einem an die Systeme zum Testergebnisabruf angeschlossenen Labor wird der CWA-Nutzer gefragt, ob er der Übermittlung des Testergebnisses an den Test

Result Server zustimmt, damit er das Testergebnis über die CWA App erhalten kann. Er erhält hierzu ein erläuterndes Begleitdokument, das den Zweck der Übermittlung erläutert.

Im Rahmen der in der CWA App eingeholten Einwilligungen wird situativ der Zweck beim Auslösen der jeweiligen Funktion erläutert. Die Möglichkeiten der grafischen Darstellung in der CWA App werden genutzt, um die Zwecke transparent darzulegen. So wird im Kontext der Funktion “Andere warnen” die länderübergreifende Übermittlung an die Verantwortlichen der anderen nationalen Corona-Apps durch die mit Nationalflaggen bebilderte Länderliste unterstrichen.

7.2.3.1.2 Informiertheit

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

Der CWA-Nutzer muss insbesondere darüber in Kenntnis gesetzt werden, welche Arten von Daten zu welchem Zweck verarbeitet werden, wer der oder die Verantwortlichen sind und wie diese zu erreichen sind sowie an welche Dritten die Daten im Falle der Übermittlung weitergegeben werden, wobei der Detailgrad der erforderlichen Informationen in einem angemessenen Verhältnis zur Bedeutung des Vorgangs und dem Kontext der Einwilligung zu halten ist.²⁶ Wäre sich ein CWA-Nutzer des Bedeutungsgehaltes der abgegeben Einwilligungserklärung nicht bewusst, könnte die Einwilligung die Datenverarbeitung nicht rechtfertigen. Es ist daher entscheidend, dass jedem CWA-Nutzer konkret die Funktionsweise der Kontaktverfolgung, der länderübergreifenden Risiko-Ermittlung, der Abläufe im Zusammenhang mit einem durchgeföhrten Test und die Datenverarbeitung der Funktion “Andere warnen” bewusst ist, bevor die jeweiligen Schritte im Einzelfall vom CWA-Nutzer initiiert werden.

Im Fall der CWA App erfolgt die jeweils relevante Information im Vorfeld einer Einwilligungserteilung. Der Gesamtzusammenhang der in Rede stehenden Datenverarbeitung wird jeweils konkret erläutert. Die Folgen der Abgabe oder Verweigerung der Einwilligung werden ausdrücklich dargelegt. In der Datenschutzerklärung werden die Datenverarbeitungen weitergehend erklärt und auf den Fundort der Datenschutzerklärung wird jeweils konkret hingewiesen. Auf diese Weise hat jeder CWA-Nutzer sowohl im Vorfeld als auch im Nachgang der Erklärung einer Einwilligung die Möglichkeit, die Zusammenhänge nachzuvollziehen. Die erklärenden Texte sind mit besonderem Augenmerk auf eine gute Verständlichkeit formuliert und setzen kein technisches Grundverständnis der betroffenen Person voraus. Im Hinblick auf die mit der Interoperabilität zusammenhängende Datenverarbeitung wird der CWA-Nutzer

²⁶ Buchner/Kühling, in: Kühling/Buchner, 2. Aufl. 2018, DS-GVO Art. 7 Rn. 59.

explizit auf die Datenverarbeitung durch die am EFGS teilnehmenden weiteren für die anderen nationalen Corona-Apps Verantwortlichen hingewiesen.

Zu beachten ist, dass eine Einwilligung, die sich auf die Verarbeitung von Gesundheitsdaten bezieht, den Gesundheitszusammenhang ausdrücklich benennen muss. Die verwendeten Einwilligungstexte weisen ausdrücklich auf den Gesundheitsbezug hin. Im Zusammenhang mit der Einwilligung in den Testabruf und der länderübergreifenden Warnung wird daher explizit herausgestellt, dass es sich bei den zu verarbeitenden Daten um Angaben mit einem Gesundheitsbezug handelt. Die Informationstexte und die Einwilligungserklärung im Rahmen der länderübergreifenden Warnung erläutert den Bedeutungsinhalt der Tagesschlüssel und weist darauf hin, dass diese – entsprechend der Funktion der Kontaktnachverfolgung dem Zweck der Warnung der Mitmenschen vor möglichen Infektionen bzw. Risiko-Begegnungen dienen. Auch der Bedeutungsgehalt der optionalen Angaben zum Symptombeginn wird konkret erläutert. Zugleich wird dargelegt, welche Schlüsse aus den Positivschlüsseln nicht gezogen werden können, wer Informationen über das Vorliegen eines positiven Testergebnisses nicht erfährt und welche konkreten Folgen auch die Nicht-Abgabe einer Einwilligung hat bzw. nicht hat.

In Bezug auf alle Einwilligungserklärungen muss sichergestellt sein, 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 und wer die Empfänger zu übermittelnder Daten sind. In Bezug auf die Interoperabilität der CWA App ist zudem entscheidend, dass der CWA-Nutzer nachvollziehen kann, dass das RKI und die am EFGS teilnehmenden weiteren für die anderen nationalen Corona-Apps Verantwortlichen gemeinsame Verantwortliche sind.

Die Anforderungen an die Informiertheit sind gegenwärtig erfüllt. Die erklärenden Texte, die Einwilligungserklärungen und die Datenschutzerklärung der CWA App sowie die weiterführenden FAQ enthalten die maßgeblichen Informationen. Die CWA App enthält überdies die Pflichtangaben gemäß § 5 TMG (Impressum).

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 und ihr Name zum Zweck des Rückrufs erfasst und anschließend zeitnah durch Vernichtung gelöscht werden. Die Informiertheit ist auch bei der flüchtigen Kommunikation sichergestellt.

7.2.3.1.3 Freiwilligkeit

Von verschiedenen Seiten und in der öffentlichen Diskussion²⁷ wurde 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“.²⁸ Wenn die Einwilligung des CWA-Nutzers in die Datenverarbeitung informiert und ohne Zwang erteilt wird, ist sie freiwillig. Ohne Zwang ist die Einwilligung, wenn der CWA-Nutzer in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne dadurch Nachteile zu erleiden oder dies zu befürchten (vgl. DSGVO-Erwägungsgrund 42).

Die Freiwilligkeit könnte im Fall der CWA insofern fehlen, als dass zwischen dem CWA-Nutzer und dem RKI als Verantwortlichen ein Über- und Unterordnungsverhältnis besteht (vgl. DSGVO-Erwägungsgrund 43). Denn als Bundesoberbehörde ist das RKI ein staatliches Organ. Allein daraus kann jedoch nicht grundsätzlich auf die fehlende Freiwilligkeit geschlossen werden.²⁹ Die Freiwilligkeit fehlt erst, wenn in Anbetracht aller Umstände des Einzelfalls nicht anzunehmen ist, dass die Einwilligung freiwillig gegeben würde. Besaß die betroffene Person keine echte Wahl, da sie 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

²⁷ Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIff), Datenschutz-Folgenabschätzung für die Corona App, Version 1.6, S. 53, abrufbar unter: <https://www.fiff.de/dsfa-corona> (zuletzt abgerufen am 15.10.2020);

EDSA: 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, S. 7;

Kühling/Schildbach: Corona-Apps – Daten- und Grundrechtsschutz in Krisenzeiten, NJW 2020, 1545, S. 1547;

statt vieler zudem Verweis auf den folgenden Presseartikel: Krempf, Corona-Tracing-Apps: Freiwilligkeit bedeutet nicht Freiwilligkeit, abrufbar unter: <https://www.heise.de/newsticker/meldung/Corona-Tracing-Apps-Freiwilligkeit bedeutet nicht Freiwilligkeit-4713114.html> (abgerufen am 15.10.2020) 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).

²⁸ Heckmann/Paschke in Ehmann/Selmayr, DSGVO Kommentar, 2. Aufl. 2018, DS-GVO Art. 7, Rn. 48.

²⁹ So aber Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIff), Datenschutz-Folgenabschätzung für die Corona App, Version 1.6, S. 54, abrufbar unter: <https://www.fiff.de/dsfa-corona> (zuletzt abgerufen am 15.10.2020);

Bedingung beispielsweise für Lockerungsmaßnahmen oder Zutrittsvoraussetzungen gemacht würde. Derartige Planungen waren und sind jedoch nicht bekannt.

Zudem ist für Dritte nicht ohne Weiteres erkennbar, wer Nutzer der CWA App ist und wer nicht. 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 App Vorteile abhängig zu machen, da deren Nutzung dem Einzelnen nicht angesehen und somit auch nicht nachgewiesen werden kann.

Teilweise wird die Eignung der Einwilligung als Rechtsgrundlage auch deshalb in Frage gestellt, weil für die Annahme der Freiwilligkeit eine echte Wahlmöglichkeit voraussetzt wird und nur so die Schutzwirkung der Einwilligung erfüllt werden könne.³⁰ An einer echten Wahlmöglichkeit kann es fehlen, wenn 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, dass eine Person aus ihrem Kreis dies nicht tut, 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 oder die Gewährung anderer Vorteile abhängig gemacht würden, denn ggf. hinge es dann tatsächlich von der einzelnen Person ab, ob auch seine Familie, Freunde und Arbeitskollegen von weiteren Lockerungsmaßnahmen profitieren. Hier käme dann neben einem sozialen Druck auch ein staatlicher Druck zum Tragen. Zudem könnten auch private Einrichtungen eine Installation und Nutzung der CWA App 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 App gleichwohl zu nutzen, um von dem Angebot nicht ausgeschlossen zu werden. Auch insoweit könnte sich die Freiwilligkeit der Nutzung der CWA App zu einem faktischen Zwang durch sozialen Druck umwandeln.

Im Ergebnis geht das RKI trotz dieser nachvollziehbaren Bedenken von der Freiwilligkeit der im Rahmen der CWA eingeholten Einwilligungen aus. Dies aus folgenden Gründen:

- Es wäre 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.
- Die Nutzung der CWA App ist nicht überprüfbar, ohne dass der Nutzer die CWA App vorzeigt. Weder dem Verantwortlichen noch Dritten ist es ohne Mitwirkung des Nutzers möglich einzusehen, ob die CWA App auf einem Smartphone installiert und vollumfänglich genutzt wird. Eine solche Veröffentlichung von Daten ist nicht vorgesehen und geplant.

³⁰ Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIff), Datenschutz-Folgenabschätzung für die Corona App, Version 1.6, S. 54, mit weiterem Verweis auf Article 29 Data Protection Working Party 2018, S. 5, abrufbar unter: <https://www.fiff.de/dsfa-corona> (zuletzt abgerufen am 15.10.2020), mit weiterem Verweis auf Article 29 Data Protection Working Party 2018, S. 5.

Auch gibt es keine Pläne oder gesetzliche Normierungen, die bspw. die Ausweitung von staatlichen Lockerungsmaßnahmen von der Nutzung der CWA App abhängig machen.

- Dem RKI sind seit der Veröffentlichung der CWA App keine Anhaltspunkte bekannt geworden, die Anlass geben, zu vermuten, dass von privaten Stellen – abgesehen von praktisch unvermeidlichen Einzelfällen im Freizeitbereich – ein Zwang zur Nutzung der CWA App ausgeübt wird.

Vor diesem Hintergrund geht das RKI davon aus, dass die Nutzung der CWA App freiwillig erfolgt, sodass auch die Freiwilligkeit der in der CWA App eingeholten Einwilligungen gegeben ist.³¹

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

Gegenwärtig gibt es im Hinblick auf die obigen Erwägungen keinen Grund zu der Annahme, dass die Freiwilligkeit der Einwilligungen der CWA-Nutzer nicht ausreichend gewährleistet ist. Die Formulierungen der Einwilligungserklärungen sowie die erläuternden Texte und die Ausführungen in der Datenschutzerklärung der CWA App unterstreichen die Freiwilligkeit der Einwilligungen ausdrücklich. Es wird konkret erläutert, dass die Verweigerung einer Einwilligung keine negativen Folgen für den jeweiligen CWA-Nutzer hat und es wird auf die Möglichkeit und die praktische Ausübung des Widerrufsrechts hingewiesen.

In Bezug auf die optionale Angabe zum Symptombeginn im Rahmen der Funktion „Andere warnen“ wird durch die zusätzliche Entscheidungsmöglichkeit („weiter mit Symptom-Abfrage“ oder „weiter ohne Symptom-Abfrage“) sowie die ausdrücklichen Erklärungen in dem Eingabeschritt und bei Abgabe der Einwilligungserklärung am Ende des Eingabedialogs auf die Freiwilligkeit hingewiesen.

Die Erwägungen zur Freiwilligkeit lassen sich auf die Einwilligung für die Verarbeitung der personenbezogenen Daten in Zusammenhang mit der Verifikations-Hotline übertragen. Das Skript enthält auch hier ausdrückliche Hinweise auf die Freiwilligkeit der Einwilligung.

³¹ Zu dem Ergebnis der grundsätzlichen Zulässigkeit der Verarbeitung personenbezogener Daten in Zusammenhang mit Contact Tracing Apps auf der Basis einer freiwilligen Einwilligung kommt auch der EDPA, sofern eine tatsächliche Möglichkeit zur Verweigerung und dem Widerruf der Einwilligung gegeben ist. EDPA: Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19, angenommen am 21. April 2020, Rn. 32, S. 9, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_de.pdf (abgerufen am 15.10.2020).

7.2.3.2 Besondere Einwilligungsfälle

7.2.3.2.1 Minderjährige

Bei der Verwendung einer Einwilligung eines nicht identifizierten CWA-Nutzers als Rechtsgrundlage besteht stets das Risiko, dass die Einwilligung von einem nicht einwilligungsfähigen minderjährigen CWA-Nutzer erteilt wird und diese in der Folge keine wirksame Rechtsgrundlage darstellen kann.

Daher ist die Nutzung der CWA App durch Minderjährige unter 16 Jahren nach den Nutzungsbedingungen der CWA App nicht erlaubt. Auch eine besondere Einwilligung für unter 16-jährige Personen ist nicht vorgesehen. Somit kann nicht ausgeschlossen werden, dass sich Minderjährige unter 16 Jahren entgegen der Nutzungsbedingungen die CWA App herunterladen und diese nutzen, ohne dass eine Einwilligung oder Erlaubnis eines Erziehungsberechtigten vorliegt.

Es gibt derzeit keine praktikable, datensparsame Möglichkeit, dies zu verhindern. Eine verlässliche Altersverifikation hätte die Erhebung weiterer, identifizierender Datenpunkte zur Folge. Jede Erstellung von "Nutzeraccounts" würde dem Grundgedanken des möglichst datensparsamen Designs der CWA widersprechen. Das RKI kann daher nur gezielt darauf hinwirken, dass in der Öffentlichkeit ein Bewusstsein über diese Altersgrenze 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 einer eingeholten Einwilligung. Unwirksam wäre die Einwilligung im Fall von unter 16-jährigen Personen nur bei fehlender Einsichtsfähigkeit, wenn also dem minderjährigen CWA-Nutzer die Reichweite der erteilten Einwilligung nicht klar wäre.

Die Regelung des Art. 8 DSGVO, wonach die Wirksamkeit von Einwilligungen von unter 16-jährigen Personen 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 CWA App ist jedoch kein solcher Dienst. 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.

Weder die CWA App noch die anderen nationalen Corona-Apps stellen eine solche Dienstleistung dar, da mit ihnen keine kommerziellen Interessen verfolgt und die Nutzung

ausnahmslos ohne Zahlung eines Entgelts möglich ist, zumal eine entgeltliche Bereitstellung ein erhebliches Verbreitungshindernis darstellen und daher im Widerspruch zu den Zwecken der Corona-Apps stehen würde.

Auch wenn die Verarbeitung von Daten anderer Nutzer im Rahmen der CWA auf eine Einwilligung gemäß dem abweichenden nationalen Recht eines anderen Verantwortlichen gestützt wird, die nach dem in Deutschland geltenden Recht unwirksam wäre, stünde dies der Wirksamkeit dieser Einwilligung als Rechtsgrundlage für das RKI nicht entgegen. Denn hinsichtlich der Verarbeitung im EFGS und der Folgebearbeitung in den nationalen Back-End-Systemen der nationalen Verantwortlichen ist die Übereinstimmung der Einwilligung mit der nationalen Gesetzgebung des die Einwilligung einholenden Mitgliedstaats ausreichend, um eine Rechtsgrundlage auch für die Verarbeitung im EFGS und für die Folgeverarbeitung zu bilden. Denn der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten nicht eingeschränkt werden, Art. 1 Abs. 3 DSGVO. Das Datenschutzrecht ist harmonisiertes Recht. Es muss überall in der EU einheitlich angewendet werden, um die Ausübung der durch die europäischen Verträge garantierten Grundfreiheiten zu ermöglichen.

7.2.3.2.2 Verifikations-Hotline

Die Frage der datenschutzrechtlichen Relevanz der Vorgänge in Zusammenhang mit der Verifikations-Hotline ist differenziert zu betrachten.

Jedenfalls das Erfragen und Niederschreiben der Telefonnummer und 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 DSGVO 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 die Erhebung des Namens und der Telefonnummer durch den Mitarbeiter sowie der anschließende Rückruf hierunter fällt, kann 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.³² Da es sich bei dem RKI um eine öffentliche Stelle handelt und jedenfalls eine Datenverarbeitung vorliegt, sind 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 CWA-Nutzers zu Beginn des Telefonats verhalten. Nach allgemeiner Ansicht setzt das

³² Ernst in: Paal/Pauly, § 1 BDSG Rn. 18; Klar, Kühling/Buchner, § 1 BDSG Rn. 34.

Erheben von Daten im Sinne von Art. 4 Nr. 2 DSGVO ein aktives Tun voraus.³³ 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 Verifikations-Hotline selbst personenbezogenen 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 EuGH³⁴ 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. Eine solche Möglichkeit besteht für das RKI oder die sonstigen am Betrieb der CWA App beteiligten Akteure indes nicht, 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.

7.2.3.3 Nachteile anderer Rechtsgrundlagen

Auch unter Berücksichtigung der identifizierten Schwächen einer Einwilligung als Rechtsgrundlage ist diese aufgrund der mit ihr verbundenen höheren Transparenz und Rechtssicherheit gegenüber den CWA-Nutzern und der ihr innewohnenden Warnfunktion im Ergebnis datenschutzfreundlicher und daher gegenüber den in Betracht kommenden gesetzlichen Zulässigkeitstatbeständen vorzugswürdig.

7.2.3.3.1 § 3 BDSG

Soweit keine besonderen Kategorien personenbezogener Daten in der CWA App verarbeitet werden, käme auch § 3 BDSG als Rechtsgrundlage der Verarbeitung in Betracht. Danach ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe erforderlich ist.

³³ Vgl. nur Roßnagel in: Simitis/Hornung/Spiecker gen. Döhmann. Art. 4 Nr. 2, Rn. 15.

³⁴ EuGH, Urt. v. 19.10.2016, Rs. Breyer, C-582/14, Rn. 42 ff.

Fraglich wäre, ob der Betrieb der CWA App als eine solche Aufgabe des RKI qualifiziert werden kann. Dies gilt insbesondere mit Blick auf die Verarbeitung der Daten der Nutzer anderer nationaler Corona-Apps für die länderübergreifenden Funktionen.

7.2.3.3.2 § 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). Zudem ist der Anwendungsbereich der Regelung ausdrücklich auf die Zusammenarbeit des RKI mit internationalen Organisationen und ausländischen Stellen beschränkt (§ 4 Abs. 3 S. 4 Hs. 2 IfSG), so dass sie keine Rechtsgrundlage für die rein nationale Datenverarbeitung (ohne EFGS) darstellen kann. Es ist zudem unklar, ob auch die Verarbeitung besonderer Kategorien personenbezogener Daten erfasst wäre.

7.2.3.3.3 § 22 BDSG

Als Rechtsgrundlage der Verarbeitung auch besonderer Kategorien von personenbezogenen Daten kommt in Zusammenhang mit der CWA 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 gesehen, dass die Regelungen die Formulierung der Öffnungsklauseln aus Art. 9 Abs. 2 lit. g und lit. i DSGVO im Wesentlichen wiederholen, ohne dabei konkretere Vorgaben zu enthalten. Dies verstößt gegen die Systematik der Öffnungsklauseln, die eine spezifische Umsetzung verlange.³⁵

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 ein möglichst konkreter Tatbestand der Norm erforderlich. Diesem Anspruch werden die Rechtsgrundlagen in § 22 BDSG jedoch nicht gerecht.

³⁵ Vgl. nur Frenzel in: Paal/Pauly, § 22 Rn. 2; Rose in: Taeger/Gabel, § 22 Rn. 8.

7.3 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 für die Zukunft sichergestellt werden. Ausnahmen hiervon sind nur unter engen gesetzlichen Voraussetzungen möglich.

7.3.1 Rechte der CWA-Nutzer

7.3.1.1 Widerrufsrecht

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.

Bereits auf dem Test Result Server, dem Verifikationsserver und dem CWA Server sowie dem EFGS sowie den nationalen Back-End-Systemen gespeicherte Daten werden im Falle des Widerrufs erst nach Ablauf der jeweils vorgesehenen Löschfristen gelöscht. Weder das RKI noch der Betreiber des EFGS oder die anderen für die nationalen Corona-Apps Verantwortlichen haben Zugriff auf identifizierende Zuordnungsmerkmale, anhand derer eine Zuordnung der bereits übermittelten Daten zu dem CWA-Nutzer möglich wäre, der eine Einwilligung widerrufen hat. Diese Umsetzung ist im Hinblick auf die Ausprägung der Datenminimierung gem. Art. 11 DSGVO sachgerecht. Es würde den Gewährleistungszielen der DSGVO, dem dezentralen Ansatz der CWA und des EFGS sowie den zum Schutz der Rechte und Freiheiten implementierten technischen und organisatorischen Maßnahmen entgegenwirken, wenn für die Löschung in Folge des Widerrufsrechts zentrale Identifikationsmerkmale im Rahmen der CWA verarbeitet würden.

Dementsprechend gelten gemäß Artikel 11 Absatz 2 und Artikel 12 Absatz 2 DSGVO die Bestimmungen über die Rechte der betroffenen Person nicht.

7.3.1.1.1 Einwilligung für die Risiko-Ermittlung

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

7.3.1.1.2 Einwilligung für die Testregistrierung

Zum Widerruf der Einwilligung für die Testregistrierung können CWA-Nutzer die Testregistrierung in der CWA App löschen. Das Token zum Abruf des Testergebnisses wird dann aus dem App-Speicher gelöscht. Weder das RKI noch das Labor können die bereits übermittelten oder auf einem Server gespeicherten Daten dann der CWA App oder dem Smartphone des CWA-Nutzers zuordnen, so dass es sich für das RKI dann um anonyme Daten handelt.

7.3.1.1.3 Einwilligung für die Warnfunktion

Zum Widerruf der Einwilligung in die Datenverarbeitung für die länderübergreifende Warnfunktion muss der CWA-Nutzer die CWA App löschen oder zurücksetzen. Sämtliche in der CWA App gespeicherten Daten werden dann entfernt, so dass etwaige Kopien dieser Daten bei den Verantwortlichen oder auf anderen Smartphones von keinem Verantwortlichen oder Nutzer mehr dem Smartphone des CWA-Nutzers zugeordnet werden können und als anonyme Daten anzusehen sind.

Eine spezifische Funktion für den Widerruf der Einwilligung für die Warnfunktion bietet die CWA App nicht an, da eine Löschung der bereits an andere Nutzer verteilten Daten (im Sinne eines Rückrufs der Warnung) ohne eine Erhebung zusätzlicher identifizierender Daten nicht realisierbar ist. Diese Umsetzung ist legitim, da sie sich aus dem Grundsatz der Datenminimierung ergibt und sicherstellt, dass eine Beziehung zwischen der betroffenen Person und den verarbeiteten personenbezogenen Daten weitestgehend unkenntlich gemacht wird. Die damit verbundene Unbequemlichkeit ist dem CWA-Nutzer insoweit zumutbar.

7.3.1.1.4 Einwilligung für die Verifikations-Hotline

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

7.3.1.2 Gewährleistung weiterer Betroffenenrechte

Die Umsetzung der weiteren Betroffenenrechte der CWA-Nutzer nach Art. 15 ff. DSGVO ist aktuell weder dem RKI noch den anderen (EFGS-)Verantwortlichen möglich, da eine Zuordnung der ggf. von einem Verantwortlichen jeweils gespeicherten pseudonymen Daten zu einem bestimmten CWA-Nutzer nicht vorgenommen werden kann. Die Gestaltung der

Verarbeitung der nationalen Back-End-Systeme und des EFGS ist auf Datenminimierung bzw. Minderung der Korrelation zwischen den gesammelten und verarbeiteten Daten und den dazugehörigen Identitäten ausgerichtet. Eine Zuordnung ist den jeweiligen Verantwortlichen daher auch dann nicht möglich, wenn der betroffene CWA-Nutzer dem jeweiligen Verantwortlichen zusätzliche Informationen zur Identifizierung bereitstellt.

Dies führt dazu, dass die Verantwortlichen nicht in der Lage sind, die Rechtmäßigkeit eines Anspruchs in Bezug auf die Rechte des betroffenen CWA-Nutzers festzustellen. Da die Verantwortlichen keinen Zusammenhang zwischen den spezifischen Datenpunkten, die sie verarbeiten, und der Identität des CWA-Nutzers, der sich hinter diesen Datenpunkten verbirgt, herstellen können, sind sie auch nicht in der Lage, festzustellen, ob eine Person, die die Rechte eines betroffenen CWA-Nutzers zu haben behauptet, diese Rechte tatsächlich beanspruchen kann. Selbst wenn die den Anspruch geltend machende Person ihre Identität gegenüber einem Verantwortlichen offenlegt, könnte dieser die Legitimität der Ansprüche nicht feststellen.

Im Fall einer Testregistrierung verarbeitet das RKI die TAN, die gehashte GUID und den Registration Token eines CWA-Nutzers. Im Fall einer Warnung verarbeiten das RKI und die weiteren Verantwortlichen der anderen nationalen Corona-Apps die Positivschlüssel und die zugehörigen Positivschlüssel-Metadaten der CWA-Nutzer.

Da es sich bei diesen Daten um zufällig generierte Kennungen handelt, stehen diese in keinem Zusammenhang mit der Identität des CWA-Nutzers. Die Weitergabe dieser Daten gibt keinerlei Aufschluss darüber, wer sich hinter den weitergegebenen Positivschlüsseln verbirgt, denn es werden von der CWA App weder zusätzliche identifizierende Informationen aufgezeichnet noch bereits auf dem Endgerät gespeicherte identifizierende Informationen weitergegeben. Daher ist es nicht möglich, eine verlässliche Verbindung zwischen der jeweiligen Kennung und später bereitgestellten Informationen herzustellen, da es für eine solche Verbindung keinerlei Anhaltspunkte gibt.

Die Verantwortlichen sind daher mangels identifizierender Zuordnungsmerkmale oder Daten im Klartext, anhand derer eine Zuordnung der bereits übermittelten Daten zu dem CWA-Nutzer möglich wäre, nicht in der Lage, Pflichten hinsichtlich der Rechte betroffener CWA-Nutzer zu erfüllen.

Dementsprechend finden gemäß Artikel 11 Absatz 2, Artikel 12 Absatz 2 DSGVO die Bestimmungen über die Rechte der betroffenen Person keine Anwendung.

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

7.3.2 Rechte anderer Nutzer

Soweit im Rahmen der CWA die Daten von anderen Nutzern verarbeitet werden, die über eine andere nationale Corona-App eine länderübergreifende Warnung ausgelöst haben, gelten hinsichtlich deren Betroffenenrechte die Ausführungen in Abschnitt 7.3.1 entsprechend.

Denn auch die Verarbeitung im EFGS ist so gestaltet, dass eine Zuordnung der Pseudonyme zu natürlichen Personen und auch die erneute Identifizierung der hinter den Pseudonymen stehenden natürlichen Personen durch die EFGS-Verantwortlichen verhindert wird.

7.4 Privacy-by-Design-Maßnahmen

Für die technische Realisierung der CWA und des EFGS 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 auch zukünftig weiter einfließen werden. Die daraus resultierenden Design-Maßnahmen führen zu einem konzeptionsbedingten Datenschutz der CWA und des EFGS.

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

- 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 Kontaktdaten
- 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 Auffangen von Übertragungsdaten

7.5 Weitere datenschutzrechtliche Anforderungen

Bei der Entwicklung und Weiterentwicklung der CWA wurde und wird konsequent versucht, die von verschiedenen fachkundigen Organisationen aufgestellten Datenschutzanforderungen an eine Corona-Tracing-App 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 2020³⁶
- Chaos Computer Club (CCC), 10 Prüfsteine für die Beurteilung von „Contact Tracing“-Apps vom 6. April 2020³⁷
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF), Datenschutz-Folgenabschätzung (DSFA) für eine Corona-App, Version 1.6 vom 29. April 2020³⁸
- Digitalcourage e.V., Einordnung zur geplanten „Corona-Kontakt-Tracing-App“ des RKI, Stand 4. Mai 2020³⁹
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF), Analyse und konstruktive Kritik der offiziellen Datenschutzfolgenabschätzung der Corona-Warn-App, Version 1.0 vom 29. Juni 2020⁴⁰

Die Maßnahmen, die zur Umsetzung der in den genannten Dokumenten aufgestellten

³⁶ EDSA, Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19, angenommen am 21. April 2020,, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_de.pdf (abgerufen am 15.10.2020).

³⁷ Chaos Computer Club e.V., 10 Prüfsteine für die Beurteilung von „Contact Tracing“ App, abrufbar unter: <https://www.ccc.de/de/updates/2020/contact-tracing-requirements> (zuletzt abgerufen am 15.10.2020).

³⁸ 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 (zuletzt abgerufen am 15.10.2020).

³⁹ Digitalcourage e.V., Einordnung zur geplanten „Corona-Kontakt-Tracing-App“ des RKI, abrufbar unter: <https://digitalcourage.de/blog/2020/corona-app-einordnung-digitalcourage>, zuletzt abgerufen am 15.10.2020).

⁴⁰ 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 (zuletzt abgerufen am 15.10.2020).

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.

8 Bewertung der Notwendigkeit und Verhältnismäßigkeit in Bezug auf die Zwecke

8.1 Zweck 1 (länderübergreifende Risiko-Ermittlung und Warnung)

8.1.1 Legitimer Zweck

Die Datenverarbeitung zur länderübergreifenden Warnung dient dem legitimen Zweck der frühzeitigen Information von Einzelpersonen darüber, dass ein erhöhtes Infektionsrisiko besteht, weil sie sich in unmittelbarer Nähe zu einer Corona-infizierten Person aufgehalten haben, sodass die gewarnte Person so früh wie möglich die gebotenen Verhaltensmaßnahmen (z. B. freiwillige Quarantäne, Konsultieren eines Arztes) ergreifen kann und Infektionsketten frühzeitig unterbrochen werden.

Laut dem derzeitigen epidemiologischen Kenntnisstand handelt es sich bei der Corona-Pandemie um eine sich schnell ausbreitende, ansteckende Krankheit, die Leben und Gesundheit des Einzelnen und der Bevölkerung der Europäischen Union in erheblichem Maße gefährden kann.

Um die Infektionsrate der Pandemie einzudämmen, haben mehrere Mitgliedstaaten der Europäischen Union und des EWR ebenfalls nationale Corona-Apps eingeführt, die eine Kontaktnachverfolgungs- und Warnfunktionen bieten. Diese nationalen Corona-Apps sollen - wie die CWA App - ebenfalls eine Warnung der jeweiligen Nutzer und eine frühzeitige Unterbrechung von Infektionsketten ermöglichen.

Die Information von Einzelpersonen über ein erhöhtes Infektionsrisiko aufgrund eines Kontakts mit einer positiv getesteten Person ermöglicht es diesen Personen, sich selbst frühzeitig testen zu lassen und individuellen Gesundheitsgefahren aufgrund einer möglichen Erkrankung begegnen zu können. Zugleich ermöglicht sie es dieser Person, sich freiwillig in Quarantäne zu begeben und so eine Ansteckung weiterer Personen zu verhindern.

Die länderübergreifende Warnung erweitert die Möglichkeit der Information über ein erhöhtes Infektionsrisiko auf die teilnehmenden Länder des EFGS, sodass auch Kontakte mit den Nutzern der anderen nationalen Corona-Apps berücksichtigt werden können und somit die Wirksamkeit der CWA erhöht.

8.1.2 Eignung

Die Verarbeitungsvorgänge im Rahmen der CWA sind geeignet, wenn sie den festgelegten Zweck fördern.

Es wird davon ausgegangen, dass das ENF als zentrale technische Systemvoraussetzung der CWA App zur Kontaktnachverfolgung grundsätzlich geeignet ist, um Kontakte zwischen Nutzern zu dokumentieren und es diesen zu ermöglichen, sich im Falle eines positiven Testergebnisses gegenseitig zu warnen. Aufgrund der Warnung können sich betroffene Nutzer selbst isolieren und weitere Maßnahmen ergreifen und so Infektionsketten unterbrechen.

Die im Zusammenhang mit der **Kontaktverfolgung** ausgetauschten Informationen erlauben die individuelle Risiko-Ermittlung im Falle einer Risiko-Begegnung. Die technischen Gegebenheiten des ENF ermöglichen nach derzeitigem Kenntnisstand eine ausreichend präzise Entfernungsmessung, um in Kombination mit den weiteren Werten eine **Risiko-Überprüfung** anhand der gegenwärtigen epidemiologischen Erkenntnisse über die Infektiosität vorzunehmen.

Die für den CWA-Nutzer optionale Symptomabfrage erlaubt zudem eine genauere Berechnung des zum Zeitpunkt des Kontakts bestehenden Ansteckungsrisikos, da auf diese Weise die im Zeitverlauf unterschiedliche Infektiosität ausgehend vom Zeitpunkt des Symptombeginns als Bezugspunkt berücksichtigt werden kann.

Soweit noch aufgrund der Neuartigkeit unklar ist, wie effektiv das ENF bei der Kontaktverfolgung ist, kann jedenfalls festgestellt werden, dass das ENF nicht gänzlich ungeeignet ist. Darüber hinaus entwickelt das RKI derzeit ein Konzept zur Evaluierung der Effektivität der CWA, welche wiederum entscheidend von der Effektivität des ENF abhängt.

Der Austausch von Daten mit für die anderen nationalen Corona-Apps Verantwortlichen über das EFGS erlaubt die länderübergreifende Risiko-Ermittlung und Warnung. Die Weitergabe der Informationen über die gemeinsame technische Infrastruktur des EFGS ist daher zur Erreichung des obenstehenden Zweckes geeignet. Die in diesem Zusammenhang zu den ausgetauschten Positivschlüsseln ergänzten Angaben zum Herkunftsland und zur Verifikation des Tests ermöglichen den anderen Verantwortlichen im Rahmen des jeweiligen nationalen Äquivalents zur Risiko-Ermittlungsfunktion der CWA die Vornahme einer eigenen Bewertung unter epidemiologischen Gesichtspunkten, so dass bei Bedarf auch vom RKI abweichende Gewichtungen einzelner Kriterien vorgenommen werden können.

Die Eignung der Verarbeitung des Namens, der Telefonnummer sowie der Antworten auf die Plausibilitätsfragen zum Zweck der Verringerung der Gefahr des Missbrauchs im Rahmen der Nutzung der Verifikations-Hotline ist fraglich. Auch wenn die Kombination aus der Abfrage von Plausibilitätsfragen und der Erhebung von Name und Telefonnummer sowie dem Rückruf es im Einzelfall erlauben, einen dolosen Nutzer zu erkennen, so sind die Maßnahmen jedenfalls nicht geeignet, denselben CWA-Nutzer daran zu hindern, erneut anzurufen und zu versuchen, sich gegenüber einem anderen Mitarbeiter der Verifikations-Hotline unter anderem Namen und mit anderen Antworten auf die Plausibilitätsfragen Zugang zu einer teleTAN zu verschaffen und so eine Falschwarnung auszulösen. Es ist zudem nicht auszuschließen, dass es im Social Engineering erfahrenen Angreifern 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, kann die Eignung nicht generell ausgeschlossen werden. Es sind jedoch effektivere Mittel der Missbrauchsverhinderung denkbar.

Eine vom Datenschutzbeauftragten des RKI empfohlene Alternative besteht darin, die Verifikations-Hotline nicht für CWA-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 CWA-Nutzers vom Labor erhalten haben und die teleTAN anschließend an den jeweiligen CWA-Nutzer 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.

8.1.3 Erforderlichkeit

Die beschriebene Verarbeitungstätigkeit im Rahmen der Risiko-Ermittlungs- und Warnfunktion ist für die Erfüllung des in Rede stehenden Zwecks erforderlich. Gleich geeignete mildere Mittel sind derzeit nicht ersichtlich.

Die Nutzung einer Tracing-App, die über die App Stores von Apple und Google angeboten wird, ist erforderlich, um allen Teilen der Bevölkerung den Download der CWA App zu ermöglichen und somit eine nennenswerte Verbreitung zu erreichen.

Es wird eine konzeptionsbedingt datensparsame Systemarchitektur eingesetzt. Ohne die Nutzung des ENF wäre die CWA App zurzeit nicht zum zuverlässigen Hintergrundbetrieb in der Lage, da Apps ohne Nutzung des ENF technisch keine Möglichkeit haben, im Hintergrundbetrieb dauerhaft auf die Bluetooth-Schnittstelle zuzugreifen. Erfahrungen anderer Länder weisen darauf hin, dass eine Corona-App ohne Nutzung der ENF-Schnittstelle zurzeit nicht ausreichend zuverlässig ist und daher – auch wegen des infolge fehlenden Nutzervertrauens – keinen Erfolg haben kann. Die Nutzung von GPS- oder Mobilfunk-Metadaten wäre insoweit keine mildere Alternative, da konkrete Standortdaten verarbeitet werden müssten, die – anders als die von dem ENF per BLE ausgetauschten RPIs – zur Erstellung von individuellen Bewegungsprofilen verwendet werden können, die wiederum aussagekräftige Rückschlüsse auf die Identität des einzelnen Nutzers zulassen können. Eine ausreichend zuverlässige Kontaktnachverfolgung und zeitnahe Warnung von Kontakten, die dem CWA-Nutzer nicht persönlich bekannt sind, ist ohne den Einsatz einer Corona-App und des ENF – auch in pseudonymer oder gar faktisch anonymer Form – zurzeit praktisch nicht realisierbar.

Durch die Verwendung von Pseudonymen wird bei der Verarbeitung ein Indikator verwendet, der von der tatsächlichen Identität der betroffenen Person so weit wie möglich entfernt ist. Dadurch wird bei der Verarbeitung ein Ansatz verfolgt, der die Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen auf ein Mindestmaß reduziert. Eine gänzlich

anonyme Technikgestaltung würde die Umsetzung von späteren Warnungen verhindern und kann daher kein gleich geeignetes, milderes Mittel darstellen.

Die Verarbeitung betrifft auch pseudonyme Gesundheitsdaten derjenigen Nutzer, die eine Warnung über eine nationale Corona-App ausgelöst haben. Die Verarbeitung von Gesundheitsdaten ist erforderlich, da nur durch die Verarbeitung der Pseudonyme positiv getesteter Nutzer eine zuverlässige zeitnahe Warnung anderer Nutzer möglich ist. Die Angabe, dass ein Nutzer positiv getestet wurde, ist daher notwendig, um über das ENF Risiko-Begegnungen ermitteln zu können, ohne dass den für die nationalen Corona-Apps Verantwortlichen die Identität der Kontaktpersonen des positiv getesteten Nutzers bekannt werden.

Die festgelegte maximale Speicherdauer richtet sich nach den epidemiologischen Erfordernissen, die auf Basis der aktuellen Erkenntnisse zur Dauer der Inkubationszeit (bis zu 14 Tage) und der anschließenden Dauer der Ansteckungsfähigkeit festgelegt worden sind.

Die Verarbeitung im EFGS und die nachfolgenden Verarbeitungen durch die Verantwortlichen der am EFGS angeschlossenen nationalen Corona-Apps sind notwendig, da andere Mittel, die zur länderübergreifenden Risiko-Ermittlung und Warnung und damit der Durchbrechung der Infektionsketten ebenso wirksam wären und die Rechte und Freiheiten der betroffenen Personen weniger stark beeinträchtigen würden, nicht zur Verfügung stehen.

Die Verarbeitung des Namens und der Telefonnummer im Rahmen der Verifikations-Hotline wird zurzeit als erforderlich bewertet. Auch wenn die Kombination aus dem Stellen von Plausibilitätsfragen und Erheben von Name und Telefonnummer sowie dem Rückruf es im Einzelfall ermöglichen kann, einen dolosen CWA-Nutzer zu erkennen, so sind die Maßnahmen zwar nicht geeignet, denselben CWA-Nutzer 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 und zumindest erschwert und ein mildereres Mittel zurzeit nicht zur Verfügung steht, kann für eine Übergangszeit, d. h. bis alle Labore an den Test Result Server angeschlossen sind, von der Erforderlichkeit dieser Maßnahme ausgegangen werden.

8.1.4 Angemessenheit

Die Datenverarbeitung ist zur Erreichung des im Interesse der Allgemeinheit verfolgten und individuell gewünschten Ziels der Nutzer angemessen. Durch ihren Beitrag zur Unterbrechung von Corona-Infektionsketten führt die Verarbeitung im Rahmen der Kontaktnachverfolgung, länderübergreifenden Risiko-Ermittlung und Warnung dazu, dass Nutzer schnell vor möglichen Ansteckungsrisiken gewarnt werden können. Gewarnete Nutzer können sodann umgehend die von den Gesundheitsbehörden empfohlenen Maßnahmen ergreifen, Infektionsketten können unterbrochen und die allgemeine Gesundheit der Bevölkerung kann geschützt werden.

Eine zu prüfende Verarbeitung ist zur Erreichung eines Zweckes angemessen, wenn die konkrete Interessenabwägung im Rahmen einer Zweck-Mittel-Relation zugunsten des 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 Verantwortlichem und die Interessen der Nutzer gegenüber. Soweit die CWA der Warnung und der Unterbrechung von Infektionsketten dient, sind die Interessen der Nutzer und des RKIs insoweit gleichgerichtet. Demgegenüber stehen die Interessen der Nutzer nicht einer Überwachung, gesellschaftlichem Druck zur Nutzung der CWA App oder rechtlichen, wirtschaftlichen oder sozialen Nachteilen infolge der Nichtnutzung der CWA App ausgesetzt zu sein.

Gegen die Angemessenheit der Verarbeitung zu den mit der Risiko-Ermittlung verfolgten Zwecken würde es daher sprechen, wenn die CWA gegenüber der durch die Gesundheitsämter durchgeführten Ermittlung und Kontaktierung von Kontaktpersonen keinerlei Vorteil bringt. Es darf jedoch angenommen werden, dass eine Corona-Tracing-App der lokalen Verfolgung durch die Gesundheitsämter jedenfalls bei der Nachverfolgung von Infektionsketten in Zusammenhang mit länderübergreifenden Kontakten aufgrund der höheren Effizienz und Vermeidung bürokratischer oder auch sprachlicher Hürden bei der grenzüberschreitenden Zusammenarbeit regelmäßig überlegen sein wird. Gleches gilt bei sich schnell ausbreitenden Infektionswellen, nicht zuletzt wegen dem bei den lokalen Gesundheitsbehörden anfallenden erheblichen personellen Aufwand, der mit der Kontaktnachverfolgung einhergeht.

Gegen die Angemessenheit der Verarbeitung zu den mit der länderübergreifenden 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 für die Gesamtbevölkerung zu geringeren Eingriffen führen, da nur solche Personen kontaktiert und mit dem **Gesundheitsamt** in Verbindung gebracht werden, bei denen ein begründeter Verdacht für eine Corona-Infektion besteht. Es darf hier 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 der manuellen Nachverfolgung von Gesundheitsämtern überlegen sein wird. Allerdings soll die CWA gerade keinen Ersatz, sondern allenfalls eine Unterstützung bzw. Ergänzung der gesetzlich vorgeschriebenen Kontaktnachverfolgung durch die zuständigen Gesundheitsämter darstellen.

Gegen die Angemessenheit der Verarbeitung können auch die mit dem technischen Ansatz der CWA zwangsläufig verbundene – jedenfalls abstrakten – Risiken sprechen:

Es besteht das Risiko, dass durch die CWA App (oder eine andere 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 nicht erforderlich sind. Somit würden die CWA-Nutzer der Gefahr ausgesetzt, dass die dabei angesammelten Daten für andere Zwecke genutzt werden, die er 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 7.4, Privacy-by-Design-Maßnahmen). Insbesondere wurde bewusst auf eine zentrale Speicherung von Kontakten sowie die Erfassung von einer Identifizierung einzelner Nutzer ermöglichen Angaben wie etwa Standortdaten verzichtet. Die CWA App ist technisch so konzipiert, dass die personenbezogene Datenverarbeitung durch Verwendung von unauflösbaren Pseudonymen faktisch anonym abläuft und sich auf ein minimales Maß beschränkt.

Zugunsten der Verhältnismäßigkeit spricht die Freiwilligkeit der Nutzung. Damit wird 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 im Zusammenhang mit der Risiko-Ermittlung auf den Einwilligungen des spezifischen Nutzers. Vor Erteilung der Einwilligungen wird der CWA-Nutzer in der CWA App oder im Rahmen von Probenentnahmen über die Datenverarbeitung informiert. Auf die Freiwilligkeit und die etwaigen Folgen der Erklärung oder Verweigerung der Einwilligung wird ausdrücklich hingewiesen. Zudem besteht keine Pflicht der Testperson, nach Abruf eines positiven Testergebnisses eine Warnung auslösen zu müssen. 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. Derzeit erscheint es jedoch nicht nur aus wirtschaftlichen, sondern auch aus sozialen und Reputationsgründen unwahrscheinlich, dass private Einrichtungen die faktische Ausgrenzung eines erheblichen Teils der Bevölkerung betreiben werden. Auch haben die vergangenen Monate gezeigt, dass solche Versuche direkt mit einer negativen Verurteilung durch Medien, Politik und der Öffentlichkeit verbunden waren. Ferner wäre es einem CWA-Nutzer, der die CWA App nur aufgrund eines empfundenen sozialen Zwangs nutzt, möglich, die CWA App auf einem (alten) Smartphone oder nur temporär zu installieren.

Die Verarbeitung im EFGS und die nachfolgenden Verarbeitungen durch die Verantwortlichen der am EFGS angeschlossenen nationalen Corona-Apps sind ebenfalls angemessen.

Die Entscheidungsfreiheit darüber, ob personenbezogene Daten im länderübergreifenden Kontext überhaupt verarbeitet werden dürfen, bleibt bestehen, da die Nutzung der nationalen Corona-Apps freiwillig ist. Bei einer Verarbeitung, bei der eine Einwilligung als Rechtsgrundlage dient, muss diese Einwilligung freiwillig gegeben werden.

Bei einer Verarbeitung, deren Rechtsgrundlage ein Gesetz ist, muss die Übermittlung der personenbezogenen Daten durch die betroffene Person ebenfalls freiwillig erfolgen und darf durch das Gesetz nicht zwingend vorgeschrieben werden. Im Rahmen des Antragsverfahrens wird entsprechend die Freiwilligkeit der Nutzung durch die gemeinsam verantwortlichen, am EFSG teilnehmenden Mitgliedstaaten geprüft und dokumentiert. Diese Entscheidungsfreiheit der Nutzer der nationalen Corona-Apps beinhaltet auch eine freie Entscheidung in Bezug auf die für die Verarbeitung Verantwortlichen. Da jeder Nutzer selbst entscheiden kann, ob er der Bereitstellung der Positivschlüssel im Falle eines positiven Tests und damit der Übermittlung personenbezogener Gesundheitsdaten zustimmt oder nicht, kann er auch darüber bestimmen, wem er die Verarbeitung seiner Daten ermöglicht. Eine weitere Option bezüglich der Weitergabe personenbezogener Daten nur an bestimmte Verantwortliche im Sinne von bestimmten Mitgliedstaaten oder der Ausschluss einzelner Verantwortlicher würden der Verfolgung des legitimen Zwecks entgegenstehen, da weder das Recht auf Mobilität noch das Recht auf Gesundheit sich speziell auf bestimmte Teile der Europäischen Union beschränkt. Aufgrund der hohen Ansteckungsgefahr können sich Infektionsketten über Grenzen hinweg bilden, ohne bestimmte Mitgliedstaaten zu verschonen. Es wäre daher mit dem Zweck des EFSG unvereinbar, wenn man es nur auf eine ausgewählte Gruppe von Mitgliedstaaten anwenden wollte, denn es liegt in der Natur der Sache, dass alle EFSG-Teilnehmerländer erfasst werden müssen. Die Möglichkeit des Datenaustauschs zwischen den für die nationalen Corona-Apps Verantwortlichen in Bezug auf die länderübergreifenden Warnungen trägt zur schnelleren Wiederherstellung eines Zustands bei, der das Reisen und grenzüberschreitende Arbeiten zwischen den teilnehmenden Ländern ohne Einschränkungen wie Selbstisolierung oder soziale Distanzierung ermöglicht, dem Schutz der Gesundheit aller Nutzer dient und eine länderübergreifende Unterbrechung von Infektionsketten ermöglicht.

Die Verarbeitung des Namens und der Telefonnummer im Rahmen der Verifikations-Hotline ist ebenfalls angemessen. Mit Blick auf die oben beschriebenen erheblichen Auswirkungen 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 CWA-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.

8.2 Zweck 2 (Testergebnisabruf)

8.2.1 Legitimer Zweck

Die Datenverarbeitung bezweckt die zeitnahe Benachrichtigung der CWA-Nutzer über ihr (positives) Testergebnis. Damit wird der legitime Zweck des Schutzes der Gesundheit der Nutzer sowie die frühzeitige Unterbrechung von Infektionsketten verfolgt.

8.2.2 Eignung

Die Verarbeitungstätigkeit ist zur zeitnahen Mitteilung von Testergebnissen an **Testpersonen** geeignet, so dass Infektionsketten früher unterbrochen werden können. Die Verarbeitung des QR-Codes und der darin enthaltenen GUID durch das Labor und das Backend der CWA sowie des Registration Tokens ermöglicht die automatisierte eindeutige Zuordnung der CWA-App-Instanz, über die der Test registriert worden ist, zu dem vom Labor übermittelten Testergebnis, so dass die Verarbeitung zur ausreichend zuverlässigen und schnellen Mitteilung des Testergebnisses nur an einen berechtigten CWA-Nutzer geeignet ist.

8.2.3 Erforderlichkeit

Mit Hilfe der CWA App können Personen, die CWA-Nutzer sind, deutlich schneller über Infektionsrisiken informiert werden als auf „traditionelle“ Weise (z. B. telefonisch durch die Gesundheitsämter). Dies gilt insbesondere dann, wenn der CWA-Nutzer die Mitteilungsfunktion aktiviert. Denn in diesem Fall wird der CWA-Nutzer automatisch informiert, sobald das Testergebnis vorliegt, auch wenn er die CWA App nicht aktiv nutzt (Push-Verfahren). Ein milderer Mittel als die CWA App zur schnellen Bekanntgabe des Testergebnisses ist nicht ersichtlich, da ein Anwender eines Smartphones sein Gerät in der Regel mit sich führt, so dass eine zeitnahe Kenntnisnahme des Testergebnisses wahrscheinlich ist. Bei Verwendung anderer Online-Kanäle (z. B. eine Website oder E-Mail) könnten möglicherweise zwar datensparsame und vertraulichere Lösungen entwickelt werden. Sie würden jedoch keine zeitnahe Information der Testperson gewährleisten, da der Testergebnisabruft von der Testperson aktiv gestartet werden müsste (durch Besuchen einer Website und Eingabe von Zugangsdaten bzw. Sichtung des Postfachs) und sind daher nicht gleichgeeignet.

Die zur Zuordnung der Testergebnisse zu der CWA App des CWA-Nutzers verwendeten Merkmale sind stark pseudonyme Kennungen. Die Verwendung von starken und faktisch nicht zuordenbaren Pseudonymen stellt somit das am wenigsten belastende Zuordnungsdatum zur Ermöglichung des Testabrufts durch die tatsächliche Testperson dar. Ein vollständiger alterner Testergebnisabruft ist aufgrund der technisch zwingend notwendigen Verarbeitung der IP-Adresse und weiterer bei jedem Internetzugriff anfallenden Daten des CWA-Nutzers praktisch oder nur mit unverhältnismäßigem Aufwand realisierbar (dazu sogleich). Durch die automatisierte und für das RKI unauflösbar pseudonymisierte Bereitstellung von Testergebnissen in der CWA App wird die Datenverarbeitung zwischen Labor, Arztpraxis bzw. Testcenter und getesterter Person auf das minimal erforderliche Maß reduziert und ein Missbrauch oder falsche Bekanntgabe von Testergebnissen deutlich unwahrscheinlicher.

Somit kann die Erforderlichkeit der Verarbeitungstätigkeit zum Testergebnisabruft bejaht werden.

8.2.4 Angemessenheit

Die Verarbeitung der Daten zur Authentifizierung sowie des Tests im Rahmen für die Zwecke des Testabrufs sind auch angemessen. Durch die automatisierte und für die beteiligten Akteure faktisch anonyme Bekanntgabe von Testergebnissen in der CWA App wird die Datenverarbeitung zwischen Labor, Arztpraxis und Testperson auf das minimal erforderliche Maß reduziert und ein Missbrauch oder falsche Bekanntgabe von Testergebnissen deutlich unwahrscheinlicher. Zwar wird auch hier durch die personenbezogene Verarbeitung durch das RKI in das Grundrecht der Testperson auf Datenschutz eingegriffen, doch erfolgt diese Beeinträchtigung unter Verwendung von Pseudonymen, die faktisch nicht mehr entschlüsselt werden können. Die Pseudonyme, die verwendet werden, enthalten nur so viele Angaben wie nötig, um der tatsächlichen Testperson ihr Testergebnis mitzuteilen. Die Entscheidungsfreiheit darüber, ob personenbezogene Daten überhaupt verarbeitet werden, bleibt jederzeit gewahrt, da die Nutzung des Testergebnisabrufs und insoweit die diesbezüglich eingeholte Einwilligung freiwillig ist. Die Testregistrierung in der CWA App kann auch durch eine entsprechende Funktion gelöscht werden und führt dazu, dass das bereitgestellte Testergebnis keiner CWA App mehr zugeordnet werden kann und somit praktisch anonym wird.

Vor diesem Hintergrund und mit Blick auf den durch die Testregistrierung ermöglichten erheblichen Zeitgewinn bei der Bekanntgabe des Testergebnisses und die dadurch wegen der Zeikritikalität des Zwecks entstehende Chance zur früheren Unterbrechung von Infektionsketten ist die Verarbeitung für den Testergebnisabruf angemessen.

9 Risikoanalyse

9.1 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 Gesamtverfahren der CWA wird jeweils eine Risikobewertung zum einen gemeinsam für die VT 1, 2 und 4, für VT 3 sowie den Verifikations-Hotline-Prozess durchgeführt.

Die zusätzliche gemeinsame Verarbeitung für die Interoperabilität wird einer gesonderten Risikoanalyse unter Verwendung der Vorlage der EU-Kommission unterzogen, soweit die Risiken in die gemeinsame Verantwortlichkeit der am EFSG beteiligten nationalen Behörden oder Stellen fallen. Gleichwohl können sich aus der Interoperabilität auch Risiken in Bezug auf die vorherige oder anschließende Datenverarbeitung im alleinigen Verantwortungsbereich des RKI ergeben. Risiken aus der EFGS-Risikomatrix, die bei der Anbindung der CWA an den EFSG zu betrachten sind bzw. Risiken, denen (nur) mit Maßnahmen durch die nationale CWA begegnet werden kann, sind ergänzend in die „Risikomatrix VT_1_2_4“ eingeflossen und werden als neue Version mit dem Namen „Risikomatrix VT_1_2_4_V1.5_mit_EFGS“ zur Verfügung gestellt. Die EFGS-bedingten Ergänzungen sind blau hinterlegt. Es handelt sich dabei um folgende Zeilen: 5, 7, 15, 55 – 59, 75, 92 – 97, 109, 110, 121 – 123, 137 – 141, 157, 158, 165.

9.1.1 Änderungshistorie

Die Änderungen der Risikomatrizen und Begründungen zu den dort angepassten oder ergänzten Bedrohungen oder Bewertungen werden in dem Vorbericht zur Anpassung der Risikomatrizen (Anlage 7) dokumentiert.

9.2 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 angelehnt⁴¹ – in folgenden Schritten vorgegangen:

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

9.3 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 bezeichnen, können ein Risiko darstellen.

⁴¹ Martin/Friedewald/Schiering/Mester/Hallinan: „Die Datenschutzfolgenabschätzung nach Art. 35 DSGVO – Ein Handbuch für die Praxis“, Frauenhofer Verlag, 2020.

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

- CWA App-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 und somit ein bestimmtes Bedrohungsszenario für verschiedene Risikoquellen betrachtet werden.)

9.3.1 Bedrohungen/Risiken

Die Bedrohungen/Risiken werden, ausgehend von den Schutzz Zielen 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 an sich, 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;
- Risikobetrachtungen durch die Projektbeteiligten;
- Ergebnisse der Workstreams;

- Ergebnisse aus dem Threat Modelling für die Komponenten CWA App, CWA Server, Verifikation Server, Portal Server, Lab Server sowie EFGS.

9.3.2 Zuordnung der Risiken zu Betroffenengruppen

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

Vorliegend sind die von den Risiken betroffenen Personen überwiegend die Nutzer. Die potenziellen Betroffenengruppen entsprechen insoweit den verschiedenen Nutzergruppen.

Beispiele sind:

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

In bestimmten Bedrohungsszenarien wurden auch andere Personengruppen als potenziell Betroffene identifiziert (z. B. Personen im Umfeld der Nutzer).

9.3.3 Bewertung der Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit (Wahrscheinlichkeit im Sinne der ISO 27005) ist ein Schätzwert 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 Angreifern werden im Rahmen der DSFA auch weitere Akteure betrachtet, denen Angriffsszenarien zugetraut werden.⁴²

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

Auch werden die Arten von Angriffen beschrieben:

A	B	C	D
Arten des Angriffes	Beschreibung	X	
Passiv	Passive Angreife betreffen die unautorisierte Informationsgewinnung und Zielen auf den Verlust der Vertraulichkeit ab. Hier wird hauptsächlich auf die Informationsbeschaffung abgesehen. Der Angreifer sendet selbst keine 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 Netzwerks durchzuführen und somit einen Einblick über die Struktur eines Netzwerkes zu bekommen. Sämtliche abgehängten Informationen können ihm als Ausgangsbasis für einen aktiven Angriff dienen.	1	
Aktiv	Aktive Angreife betreiben die unautorisierte Modifikation von Datenobjekten und richten sich somit gegen die Dateneingabe oder Verarbeitung eines Systems. Aktive Angreife gehen daher über ein passives Beobachten hinaus und beinhalten aktive Eingriffe in die Kommunikation, um Daten, IT-Systeme oder Benutzer zu manipulieren. Diese Art von Angreifen benötigt folglich die nicht autorisierte Modifikation von Daten undrichtet sich somit in erster Linie gegen die Dateneingabe und die Verarbeitung. Nach der erfolgreichen Durchführung eines aktiven Angriffes hat der Angreifer direkten Zugang zu fremden Betriebsmitteln und kann diese aktiv missbrauchen. So kann er durch Vieldurchlaufer, Verzögerung, Verfälschung, Modifikation und Lösung bestimmter Daten eine falsche Identität vorspielen und eventuell Rechte und Attribute modifizieren.	2	
Regional	Ein regionaler Angreifer ist in seinem Handlungsspielraum auf einige wenige in seine Gewalt gebrachte Geräte oder Infrastruktursysteme beschränkt.	1	
Überregional	Ein überregionaler Angreifer hat dagegen die Kontrolle über mehrere Geräte oder Infrastruktursysteme, die über ein überregionales Netzwerk verteilt sind.	2	
Rational	Ein rationaler Angreifer strebt nach persönlichem Profit und ist daher vorhersehbar in Bezug auf Angreifsziele und Angreifsmittel.	1	
Bös willig	Ein bös williger 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 unautorisierte Einbindung 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	
Indirekt	Ein indirekter 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	
Einstufig	Bereikt ein Angriff nur einen einzelnen Schritt, um das geplante Ziel anzusteuern, so handelt es sich um einstufigen Angriff.	1	
Mehrstufig	Mehrstufige Angriffe kombinieren verschiedene Angriffsschritte, 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 anzugehen. Dazu noch ein Beispiel: Ein Angreifer nutzt eine einfache, unsichere Applikation, um zweitens ins Internet zu gelangen. Im zweiten Schritt kann wird versucht, dort auf die datenträfferen Systeme zu erlangen.	2	
Arten des Angriffs Schadenskategorien Eintrittswahrscheinlichkeiten Maßnahmenplanung 4			

Abbildung 19: Risiko-Matrix

9.3.4 Bewertung der Schadenshöhe

Der potentielle Schaden für betroffene Personen wird anhand der zu betrachtenden Gewährleistungsziele Datenminimierung, Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Resilienz, Intervenierbarkeit, Transparenz, Zweckbindung/Nichtverkettung geschätzt:

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 offenbart werden. Sie sind vor unbefugter Veränderung zu schützen.

⁴² 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 (zuletzt abgerufen am 15.10.2020).

Integrität	Integrität von Daten ist die Abwesenheit von korrumptierten 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 Personen 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 die betroffenen Personen 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)
Schadensausmaß von	Gesellschaftliche und soziale Nachteile (Pfuschdägungen, Aussehenverluste)	Kein oder unbedeutender Verlust	geringfügige, vorübergehende Peinlichkeit	Vorstöße erheblichen Konsequenzen Beschädigung gesellschaftlicher Teilhabe, Mobbing, erheblicher Gesichtsverlust, über mit Anstrengung überwindbar	Fundamentalsler Verstoß gegen Vorschriften und Gesetze gesellschaftliche Diskriminierung, schwer öffentlich Bloßstellung mit fundamentalscher irreversiblen Folgen
	Einschüchterungseffekt (vor Angst vor negativer Folgen nicht Betroffener davon ab Rechte aussüßen oder sich persönlich zu enthalten (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 (Befreiung, Lokalisierung...) überwindbar	Ein erheblicher, dauernder und örtlich nicht mehr begrenzbarer Einschüchterungseffekt, eventuell sogar existenzgefährdender Art, ist denkbar.
	Beschädigung 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 entschuldigenden Schwierigkeiten	Erhebliche bis irreversible Folgen, nicht überwindbar
	Beeinträchtigung der persönlichen Unversehrtheit (falsche medizinische Behandlung, Vorschreiblisten 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 Akzeptanzsteigerung erfordern	Akzeptanzverlust der App sinkt nicht nur kurzfristig auf ####/ Komplettausfall
wirtschaftliche Auswirkungen / materielle Schäden (Jobverlust durch berufliche Nachteile durch Leistungs- und Verhältniskontrolle, Beschädigung staatlicher Leistungen, höheres KV-Beträge)		≤1.000.000 I	finanziell 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 20: 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 mitgelgenden Dokumenten beschrieben werden, soweit dies geboten erscheint. Dies betrifft insbesondere die Risiken hinsichtlich der verwendeten Rechtsgrundlagen, da die Risiken für betroffene Personen hier nicht nur auf einzelne Schutzziele wirken, sondern vielmehr auch grundsätzliche Fragen der Rechtmäßigkeit der Datenverarbeitung und Akzeptanz betreffen können.

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 Schadenzahl gebildet wird.

Kategorie	Risikoklasse	Beschreibung
Niedrig	0-4	<p>Die Auswirkungen des Schadens für betroffene Personen sind begrenzt und beherrschbar.</p> <p>Das Eintreten einer zu berücksichtigten Schadenssituation erscheint unmöglich.</p>
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	<p>Signifikante Schäden können nicht komplett ausgeschlossen werden, aber eine existenzbedrohende Situation erscheint unwahrscheinlich.</p> <p>Technische und organisatorische Maßnahmen MÜSSEN vorgeschlagen und innerhalb einer festgelegten Frist umgesetzt werden (siehe hierzu Tabellenblatt „Maßnahmenplanung“).</p> <p>Die Reduktion von Risiken durch technische und organisatorische Maßnahmen und/oder Kontrollen ist notwendig. Eine Risikoakzeptanz basierend auf einer Kosten-Nutzen-Betrachtung der geplanten Handlungen bedarf einer besonderen Managementbetrachtung.</p> <p>Die zuständige Aufsichtsbehörde SOLL konsultiert werden.</p>
Hoch	11-16	<p>Schadenseffekte können katastrophale oder existenzbedrohende Ausmaße annehmen. Das Eintreten des Risikos hat signifikante negative Auswirkungen.</p> <p>Dieses Risiko bedarf sofortiger Aufmerksamkeit. Eine Akzeptanz dieses Risikos ist ausgeschlossen. Eine Reduktion des Risikos durch hierauf abgestimmte technische und organisatorische Maßnahmen ist notwendig; die Berücksichtigung systematischer und strategischer Maßnahmen wird empfohlen.</p> <p>Die Aufsichtsbehörde MUSS konsultiert werden.</p>

Die Maßnahmen können dem Katalog der Referenzmaßnahmen des Standard-Datenschutzmodells⁴³ (SDM) zugeordnet werden, die im Tabellenblatt „Maßnahmen“ hinterlegt sind. Nach dem SDM werden jedem Gewährleistungsziel spezifische technische und organisatorische Abhilfemaßnahmen zugeordnet, mittels derer das Ziel und die dahinterstehenden Anforderungen der DSGVO gewährleistet und der Eintritt des Schadensereignisses verhindert werden können.

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.

⁴³ DSK, Das Standard-Datenschutzmodell Version 2.0b, abrufbar unter: <https://www.datenschutzzentrum.de/sdm/> (zuletzt abgerufen am 15.10.2020).

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

Abbildung 21: Darstellung der Risikobewertung (Inhalt nur beispielhaft).

9.4 Maßnahmen zur Risikobehandlung

Nachfolgend werden stichwortartig zentrale technische und organisatorische Maßnahmen aufgeführt, die vom RKI getroffen wurden, um die identifizierten Risiken für die betroffenen Personen zu reduzieren:

1. Pseudonymisierung, soweit möglich;
2. Trennung von Teilprozessen/Diensten durch Verwendung verschiedener Server (CWA Server, Verifikationsserver, Lab Server);
3. Restriktive Berechtigungskonzepte und Autorisierungsprozesse für alle CWA-Serverkomponenten zur Beschränkung der Zugriffsmöglichkeiten von Mitarbeitern der an der Datenverarbeitung beteiligten Unternehmen (auch als Bestandteil von Pseudonymisierungsmaßnahmen);
4. Verschlüsselte Datenübertragung zwischen CWA App und CWA Server sowie zwischen CWA Server und EFGS. Die Speicherung der Daten auf allen CWA- und EFGS-Serverkomponenten erfolgt verschlüsselt;
5. Implementierung von Betriebs-, Sicherheits- und Datenschutzkonzepten für die CWA- und EFGS-Komponenten zur Minimierung von Ausfallzeiten und zur Gewährleistung von Sicherheits- und Datenschutzanforderungen;
6. Etablierung eines Datenschutz-Managementsystems (DSMS; PDCA-Zyklus).

Ergänzend wird hinsichtlich der nationalen CWA-Komponenten auf die Liste der mit TSI vereinbarten technisch-organisatorischen Maßnahmen Bezug genommen, die an den Vorgaben des BSI ausgerichtet sind (Anlage 2).

Die konkreten vom RKI und hinsichtlich des EFGS von den gemeinsam Verantwortlichen ergriffenen oder geplanten Maßnahmen zur Risikobehandlung/-minimierung werden in den Risikomatrizen der jeweiligen Verarbeitungstätigkeiten beschrieben, die als Anlagen 3, 4, 5 (nationale CWA) und 6 (EFGS) beigefügt sind. Ergänzend wird zur Beschreibung der Maßnahmen auch auf die Dokumente zu den „Designentscheidungen“ (Anlage 1) Bezug genommen. In diesen Dokumenten finden sich nähere Beschreibungen der identifizierten Risiken und der diesbezüglich von den jeweiligen Verantwortlichen ergriffenen Risikobehandlungsmaßnahmen.

Weitere Informationen (insbesondere in Form von Quellcode) zu bei der Durchführung der Risikoanalyse berücksichtigten technischen Maßnahmen hinsichtlich einzelner CWA-Komponenten können teilweise auch der bis zum jeweiligen Berichtszeitraum der Risikoanalyse (siehe hierzu Anlage 7) versionierten GitHub-Projektdokumentation entnommen werden.⁴⁴

9.5 Bewertung von hohen Restrisiken

Die identifizierten Risiken und die diesbezüglich ergriffenen bzw. geplanten Risikobehandlungsmaßnahmen wurden im Rahmen der Durchführung, Weiterentwicklung und Aktualisierung der DSFA ausführlich behandelt und nach Möglichkeit im Projektverlauf berücksichtigt. In den Risikomatrizen und im Dokument „Designentscheidungen“ werden die Ergebnisse der Risikoanalyse dokumentiert. Die nach Umsetzung der Risikobehandlungsmaßnahmen noch verbleibenden Risiken (sog. Restrisiken) werden von den jeweils Verantwortlich als zurzeit akzeptabel bewertet. Das RKI muss jedoch fortlaufend beobachten, ob Umstände eintreten, die eine Neubewertung der Ergebnisse der Risikoanalyse notwendig erscheinen lassen.

Nachfolgend werden die im Rahmen der Risikoanalyse identifizierten hohen Restrisiken und die wesentlichen Gründe, weshalb diese akzeptiert werden, zusammenfassend dargestellt. Alle identifizierten Risiken und die diesbezüglichen Risikobehandlungsmaßnahmen werden in den Designentscheidungen, den Risikomatrizen und den Datenschutzkonzepten dokumentiert.

Die Darstellung erfolgt getrennt nach den Risiken der nationalen Verarbeitungsvorgänge (nationale CWA) einerseits (Abschnitt 9.5.1) und der Interoperabilität (EFGS) andererseits (Abschnitt 9.5.2). Da eine eindeutige Zuordnung der identifizierten Risiken in diese Kategorien nicht immer möglich ist, wird ggf. darauf eingegangen. Die Zuordnung ist teilweise auch unter praktischen Gesichtspunkten erfolgt, sodass in der Zuordnung keine Aussage zur Verantwortlichkeit für die jeweilige Datenverarbeitung bzw. Risikobehandlung getroffen werden soll.

⁴⁴ Vgl. Dokumentation auf github, abrufbar unter <https://github.com/corona-warn-app/> (zuletzt abgerufen am 15.10.2020).

9.5.1 Hohe Restrisiken der nationalen CWA

9.5.1.1 Risiken durch die Verwendung von Dritt-Technologien

→ Risiko-Matrix VT 1, 2, 4, dort Zeilen 20, 42, 43, 68, 98

Der Umstand, dass die CWA App die Konnektivitäten und das ENF von Google und Apple verwendet, stellt ein erhebliches Datenschutzrisiko dar, welches durch das RKI jedoch praktisch nicht beseitigt und auf technischer Ebene auch nicht reduziert werden kann. Gleichermaßen gilt hinsichtlich des Angewiesenseins der CWA App auf den BLE-Standard sowie die Hardwarekomponenten des Smartphones, die sich außerhalb des Wirkbereichs des RKI befinden. Aus den von Apple und Google veröffentlichten Quellcode-Auszügen des ENF ergibt sich kein vollständiges Bild⁴⁵, so dass die Aussagen von Apple und Google zur Funktionsweise und den Datenschutzaspekten des ENF nicht umfassend überprüft werden können.

Die genaue technische Umsetzung und Funktionsweise aller betriebssystem- und hardwareseitigen Funktionalitäten ist der Kontrolle des RKI entzogen. Es liegt nahe anzunehmen, dass Apple und Google – entgegen ihren öffentlichkeitswirksamen Bekundungen und Zusicherungen – durch eine Änderung des ENF 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) auf technischer Ebene leicht in der Lage wären. Derartige Risiken bestehen allerdings für jeden App-Anbieter, der die Schnittstellen des Betriebssystems bzw. der Google Play-Dienste oder technische Komponenten des Smartphones eines anderen Herstellers 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 oder Betriebssystems dieser Hersteller für persönliche Zwecke einhergehen, akzeptiert oder andernfalls ihr Nutzungsverhalten entsprechend angepasst haben (z. B. durch Deaktivierung von Systemfunktionen oder Bluetooth). Es ist damit zu rechnen, dass die Bluetooth-Technologie auch bisher nicht bekannte Schwachstellen aufweist, die infolge zu Fehlern oder zur Ermöglichung einer unbefugten Datenverarbeitung hinsichtlich der Daten der CWA ausgenutzt werden könnten.

Derartige Risiken, die auf technisch zwingend notwendige Abhängigkeiten der CWA von Dritt-Technologien und teilweise auch auf das individuelle Nutzungsverhalten des Nutzers zurückgehen, müssen und dürfen daher – soweit sie vom RKI wie vorliegend nicht durch angemessene Maßnahmen reduziert werden können – hingenommen werden. Andernfalls wären die CWA oder andere von Dritt-Technologie abhängige öffentliche Apps nicht realisierbar.

⁴⁵ Vgl. Dokumentation auf github, abrufbar unter <https://github.com/google/exposure-notifications-android> (zuletzt abgerufen am 15.10.2020).

9.5.1.2 Risiken durch Verhalten oder Technikfehler auf Seiten des Nutzers

→ Risiko-Matrix VT 1, 2, 4, dort Zeile 77

Risiken, die auf typische oder faktisch unvermeidbare Fehlbedienungen, nicht ordnungsgemäßes oder nicht sachgerechtes Nutzungsverhalten des CWA-Nutzers (z. B. falsche Konfigurationseinstellungen, Unterlassen von Sicherheitsupdates, Verzicht auf Passwortschutz- oder sonstige Datenschutzmaßnahmen) oder 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 wie vorliegend nicht durch angemessene Maßnahmen weiter reduziert werden können – hingenommen werden. Andernfalls wären die CWA oder andere von Dritt-Technologie abhängige öffentliche Apps nicht realisierbar. Eine zwischenzeitlich durch das BSI vorgelegte Stellungnahme geht nicht von zusätzlichen Sicherheitsrisiken durch den Einsatz der Bluetooth-Komponenten aus.

9.5.1.3 Risiken durch den Einsatz von Auftragsverarbeitern

→ Risiko-Matrix VT 1, 2, 4, dort Zeile 104

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 wurde, der die Überprüfung des Vorliegens einer tragenden Rechtsgrundlage für das Herausgabeverlangen juristisch sicherstellt. Mit TSI wurde zudem ein Auftragsverarbeitungsvertrag abgeschlossen, der die Verarbeitung von Daten ausschließlich zu den vom RKI festgelegten Zwecken der CWA vorgibt, soweit eine abweichende Datenverarbeitung nicht gesetzlich verpflichtend vorgeschrieben ist.

Durch den Einsatz von Auftragsverarbeiten wird zwangsläufig ein eigenes 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 Auftragsverarbeitern 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 sowie der Umsetzung angemessener technisch-organisatorischer Maßnahmen; zudem muss sichergestellt werden, dass die betroffenen Personen das Risiko durch die Beauftragung eines Auftragsverarbeiters zutreffend einschätzen können.

Das RKI hat mit seinen Auftragsverarbeitern angemessene technisch-organisatorische Maßnahmen vereinbart und auch tatsächlich umgesetzt. Sachgerechte und effektive Kontrollrechte des RKI sowie der zuständigen Aufsichtsbehörde gegenüber den Auftragsverarbeitern sind vertraglich sichergestellt. Die Nutzer werden über die Auftragsverarbeitung und Mitwirkung der zentralen Dienstleister SAP und TSI unter anderem in der Datenschutzerklärung der CWA App informiert, so dass das verbleibende Restrisiko – soweit es vom RKI wie vorliegend nicht durch angemessene und auch überobligatorische Maßnahmen weiter reduziert werden kann – hingenommen werden.

9.5.1.4 Risiken durch Cyberkriminalität / Sabotageversuche

- Risiko-Matrix VT 1, 2, 4, dort Zeilen 42, 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 richten) oder Gegnern der CWA (z. B. durch Versuche, die Akzeptanz der CWA App durch Verursachen von Fehlalarmen zu schädigen) ausgehen, können nicht vollständig verhindert werden. Sie müssen und dürfen daher – soweit sie vom RKI wie vorliegend nicht durch angemessene Maßnahmen weiter reduziert werden können – hingenommen werden. Andernfalls wären die CWA oder andere öffentliche App-Angebote nicht realisierbar.

Angemessene Maßnahmen für einen sicheren Regelbetrieb der CWA-Komponenten wurden von dem technischen Dienstleister TSI für das RKI aufgesetzt und dokumentiert. Die IT-Sicherheitsrisiken werden kontrolliert und jährlich aktualisiert. Das entsprechende Sicherheitsrahmenkonzept liegt dem BSI derzeit zur Abnahme vor. Aus IT-Sicherheitsgründen wurden die konkreten Sicherheitsmaßnahmen für den sicheren Betrieb der CWA bislang nicht veröffentlicht. Bisher (Stand: 6.10.2020) hat die TSI auf die CWA Infrastruktur noch keinen Cyber-Angriff detektiert.

Das Risiko von sog. Spoofing-Apps, mit deren Hilfe böswillige Angreifer unter Verschleierung ihrer Identität versuchen könnten, einen CWA-Nutzer davon zu überzeugen, eine andere App mit einem der CWA App gleichen oder ähnlichen Titel und/oder App-Icon zu verwenden, um bösartige Inhalte und/oder Funktionalitäten zu verbreiten (siehe Zeile 124 der Risikomatrix in Anlage 3), hat sich nach Einschätzung der Dienstleister SAP und TSI bislang nicht realisiert.

Der Hotline-Prozess verlief nach Aussagen der zuständigen Dienstleister bisher ohne Auffälligkeiten. Dies auch mit Blick auf das in Zeile 15 der Risikomatrix beschriebene Risiko. Das Risiko von Brute Force Attacken auf die teleTAN durch Hacker könnte potentiell zu einem Missbrauch der CWA führen. Im Hinblick auf die getroffenen IT-Sicherheitsmaßnahmen, insbesondere die Festlegung der Schlüssellänge ist das gegenwärtige Risiko als akzeptabel einzustufen. Zukünftig soll die Schlüssellänge auf neuartige Risikoszenarien angepasst werden können.

Das Risiko des Vortäuschens einer falschen Identität oder falscher positiver Testergebnisse über die Hotline (Zeile 8 der Risikomatrix) wird dennoch unverändert als hoch, gleichwohl aber als akzeptabel eingeschätzt, da es gegenwärtig vom RKI nicht durch angemessene Maßnahmen weiter reduziert werden kann. Es sei an dieser Stelle angemerkt, dass die Häufigkeit des Hotline-Prozesses wegen der fortschreitenden Anbindung der Labore an den Test Result Server deutlich abgenommen hat und auch weiterhin noch abnehmen wird.

9.5.1.5 Risiken für Minderjährige

→ Risiko-Matrix VT 1, 2, 4, dort Zeile 12

→ 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 Minderjährige unter 16 Jahren entgegen dieser Vorgabe die CWA App trotzdem herunterladen und nutzen, ohne dass eine Einwilligung eines Erziehungsberechtigen vorliegt. Das RKI hat faktisch keine Möglichkeit, dies zu verhindern. Es kann nur durch entsprechende Informationsmaßnahmen darauf hinwirken, dass in der Öffentlichkeit ein Bewusstsein über diese Altersgrenze herrscht, um einer Nutzung durch unter 16-jährige Personen entgegenzuwirken.

Der Verstoß eines CWA-Nutzers gegen die Altersgrenze führt jedoch nicht zwangsläufig zur Unwirksamkeit der Einwilligung und birgt insoweit nicht zwangsläufig das Risiko einer rechtswidrigen Datenverarbeitung. Weder dem RKI noch seinen Dienstleistern TSI sowie den Hotline-Dienstleistern sind Beschwerden bezüglich der Verarbeitung von Daten von Minderjährigen bekannt.

Das Risiko muss und darf – soweit es vom RKI wie vorliegend nicht durch angemessene Maßnahmen weiter reduziert werden kann – hingenommen werden.

9.5.1.6 Risiken durch Fehlfunktionen oder Unwirksamkeit der CWA App

→ Risiko-Matrix VT 1, 2, 4, dort Zeilen 25, 98, 119, 120

Der Einsatz einer Tracing-App zur Bekämpfung einer Virus-Pandemie ist weiterhin technisches „Neuland“. Daher können Risiken durch Fehlfunktionen oder fehlende epidemiologische Wirksamkeit der CWA App naturgemäß nicht ausgeschlossen werden. Bislang gibt es jedoch keine Hinweise auf fehlende Wirksamkeit. Die insbesondere in der Anfangsphase identifizierten technischen Fehler wurden durch Updates behoben. Über das Ausmaß von eventuellen durch diese Fehler bedingte Schäden liegen keine Erkenntnisse vor, so dass anzunehmen ist, dass möglicherweise zwar gewisse Unbequemlichkeiten oder Irritationen bei den betroffenen CWA-Nutzern, jedoch keine schwerwiegenden Schäden eingetreten sind.

Die Risiken können daher zurzeit akzeptiert werden.

Eine angemessene Bewertung der Wirksamkeit der CWA ist unter Verhältnismäßigkeitsgesichtspunkten nach einer gewissen Zeit jedoch erforderlich, auch wenn eine Nutzungsanalyse in der CWA App aus Datenschutzgründen gerade nicht vorgesehen ist. Das RKI plant daher eine Untersuchung zur Evaluierung der epidemiologischen Wirksamkeit der CWA, wobei die Gefahr einer Aufhebung der faktischen Anonymität der App-Nutzung auf ein Mindestmaß reduziert werden muss (z. B. durch Erhebung lediglich von Stichproben, die durch freiwillige Befragungen außerhalb der CWA App gewonnen werden).

9.5.1.7 Risiken durch missbräuchliche Nutzung des Hotline-Verfahrens

→ Risiko-Matrix Verifikations-Hotline, dort Zeile 8, 15

Der Einsatz der Verifikations-Hotline 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, alle Labore schnellstmöglich an den digitalen Prozess (QR-Code-Verfahren) anzuschließen.

Bis alle Labore angeschlossen sind, wird die Verifikations-Hotline erforderlich sein, um eine möglichst hohe Nutzbarkeit der CWA App zu gewährleisten. Vorschläge zur datenschutzfreundlichen Ausgestaltung der Verifikations-Hotline 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 Verifikations-Hotline wurden bereits mit dem BfDI vorsorglich weitere Schritte abgestimmt, um einem konkreten Verdacht missbräuchlicher Nutzung zügig zu begegnen. Das Risiko einer missbräuchlichen Nutzung hat sich nach bisherigen Erkenntnissen indes nicht realisiert.

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 (Plausibilitätsfragen und Rückruf beim Anrufer) 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.

9.5.1.8 Risiken durch Anbindung des CWA Servers an den EFGS

→ Risiko-Matrix VT 1, 2, 4, dort Zeile 7 (neu)

Das Risiko besteht darin, dass der CWA Server oder das entsprechende Serversystem einer anderen nationalen Corona-App die über den EFGS bereitgestellten Daten eines anderen Nutzers auf der Basis der Einwilligung des betreffenden Nutzers nicht nur einmalig von dort herunterladen, um sie dann an die eigenen Nutzer zu verteilen, sondern diese Daten im Rahmen der eigenen Positivschlüssel-Pakete (erneut) an den EFGS übermittelt, insbesondere weil nicht festgestellt werden kann, aus welchem Land die Daten übermittelt worden sind. Sofern im Fall einer Einwilligung des betreffenden Nutzers als Rechtsgrundlage diese (erneute) Verarbeitung nicht erlaubt ist, würde es an einer Rechtsgrundlage für die nochmalige Übermittlung fehlen. Dieses Risiko geht mit der Interoperabilität einher, wurde im Rahmen der Risikoanalyse jedoch bei den Risiken der nationalen CWA behandelt, da die primäre Risikobehandlung im alleinigen Verantwortungsbereich des RKI erfolgen muss.

Zur Behandlung des Risikos für andere Nutzer wird der CWA Server so konfiguriert, dass er die vom EFGS heruntergeladenen Schlüssel nicht erneut an das EFGS übermittelt. Hinsichtlich des Risikos für CWA-Nutzer wird der CWA Server so konfiguriert, dass die an den EFGS übermittelten Positivschlüssel-Pakete mit der zwischen den gemeinsamen Verantwortlichen abgestimmten Länderkennung "DE" versehen werden, so dass die anderen Verantwortlichen diese Information nutzen können, um die von CWA-Nutzern bereitgestellten Daten vor dem Hochladen herauszufiltern.

Zur technischen Mitigation des Risikos auf Seiten der anderen nationale Serversysteme der nationalen Corona-Apps setzt sich das RKI zurzeit dafür ein, dass im Rahmen der Paketierung der Positivschlüssel der Parameter "rolling_start_interval_number" der Schlüssel überprüft und somit veraltete Schlüssel verworfen werden. Hierdurch würde das Risiko umgangen, ausländische Positivschlüssel erneut zu verteilen, wenn sie nur auf Grund eines unzulässigen Wiederhochladens in nationalen Serversystemen der nationalen Corona-Apps und im EFGS verarbeitet werden.

Das identifizierte Restrisiko wird zurzeit als akzeptabel bewertet, muss nach Einführung der Interoperabilität jedoch beobachtet und ggf. in Zusammenarbeit mit den anderen Verantwortlichen weiter mitgiert werden.

9.6 Hohe Restrisiken der Interoperabilität

9.6.1 Risiken durch fehlende Rechtsgrundlage

→ Risiko-Matrix EFGS, dort Zeilen 6 und 8

Jeder Verantwortliche trägt die Verantwortung für die Verarbeitung personenbezogener Daten im EFGS⁴⁶. Es besteht somit das Risiko, dass ein für eine nationale Corona-App Verantwortlicher keine wirksame Rechtsgrundlage für die Verarbeitung zur Ermöglichung der Interoperabilität geschaffen hat. Verarbeitet einer der gemeinsam Verantwortlichen Daten unter Zu widerhandlung gegen verpflichtende EU-Gesetze oder entsprechende nationale Vorschriften bzw. ohne eine ausreichende Einwilligung der betroffenen Person, ist auch die Rechtmäßigkeit aller nachfolgenden Verarbeitungsschritte der anderen Verantwortlichen nicht gewährleistet. Es muss daher sichergestellt sein, dass die Wirksamkeit der Rechtsgrundlage für die Verarbeitung personenbezogener Daten im EFGS gegeben ist.

Damit eine nationale Corona-App an das EFGS angeschlossen wird, muss der jeweils Verantwortliche einen entsprechenden Antrag stellen. In diesem Antrag werden auch Angaben zur Rechtsgrundlage für die Datenverarbeitung in Zusammenhang mit der Interoperabilität gemacht.

Die gemeinsamen Verantwortlichen haben sich darauf verständigt, die jeweils verwendeten Rechtsgrundlagen im Rahmen des formalisierten Antragsverfahrens im Hinblick auf die Maßgaben des Durchführungsbeschlusses zu bewerten sowie insbesondere die Vorgaben des EDSA hierzu zu beachten, um Rechtssicherheit und Rechtskonformität im Hinblick auf die gemeinsame Verarbeitung zu gewährleisten. Gegenwärtig gibt es keinen Anlass zu der Annahme, dass das formalisierte Antragsverfahren diese Anforderungen nicht gewährleisten wird.

9.6.2 Risiken durch Verarbeitung veralteter oder nicht erforderlicher Daten

→ Risiko-Matrix EFGS, dort Zeile 96

Die Interoperabilität erfordert die Speicherung von Kopien der an das EFGS übermittelten Daten auf den nationalen Serversystemen der nationalen Corona-Apps. Ohne ein hohes Maß an Koordination und klar definierten einheitlichen Prozessen besteht daher das Risiko einer übermäßigen Erzeugung und Speicherung von personenbezogenen Daten, die für die Zwecke der gemeinsamen Verarbeitung nicht erforderlich ist. Daher müssen sich die gemeinsamen

⁴⁶ Durchführungsbeschluss der Kommission (EU) 2020/1023, 15. Juli 2020, Anhang II, Artikel 1 (2) (2), abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32020D1023&from=DE> (zuletzt aberufen am 15.10.2020).

Verantwortlichen auf einheitliche Standards, Prozesse und Datenstrukturen einigen und diese auch tatsächlich anwenden.

Zur Eindämmung des Risikos haben die gemeinsam Verantwortlichen unter anderem folgende Maßnahmen ergriffen bzw. festgelegt:

- Nationale Corona-Apps kommunizieren ausschließlich mit dem jeweiligen nationalen Serversystem (für die CWA also der CWA Server) und nicht direkt mit dem EFGS.
- Implementierung eines gemeinsamen Löschkonzepts, das die maximal zulässige Speicherdauer für die von den jeweils anderen bereitgestellten Daten auf die aus epidemiologischer Sicht erforderliche Dauer beschränkt.
- Bezuglich weiterer Designentscheidungen und Festlegungen in Bezug auf den EFGS, die insbesondere der Datenminimierung und Zweckbestimmtheit dienen, siehe das Dokument "Designentscheidungen" (Anlage 7) sowie den gemeinsamen Verarbeitung zugrundeliegenden Durchführungsbeschluss (EU) 2020/1023 (einschließlich Anhänge).

Da zum jetzigen Zeitpunkt nicht von Zuwiderhandlungen einzelner Verantwortlicher gegen die gemeinsam festgelegten bzw. noch festzulegenden Maßnahmen ausgegangen werden muss, wird das Restrisiko derzeit als akzeptabel bewertet.

9.6.3 Risiken durch Verwendung und technische Einschränkungen des ENF

→ Risiko-Matrix EFGS, dort Zeilen 6, 8, 20, 32, 47, 82

Die Verarbeitung nach dem Widerruf der Einwilligung und die von Apple und Google festgelegten technischen Begrenzungen des ENF betreffen beide die faktische Anonymität der Positivschlüssel für die gemeinsam Verantwortlichen, die als nicht zuordenbare Pseudonyme dienen sollen.

Weil eine Identifizierung einzelner Nutzer durch die Verantwortlichen der nationalen Corona-Apps aufgrund der Systemarchitektur der Serversysteme der nationalen Corona-Apps auch mit zusätzlichen identifizierenden Informationen zu den betroffenen Nutzern regelmäßig ausgeschlossen ist, kann ein Widerruf einer Einwilligung in die länderübergreifende Warnung mangels Zuordenbarkeit die weitere Verteilung der Daten des Widerrufenden an andere Nutzer nicht verhindern.

Diese technischen Einschränkungen können auch insoweit ein Risiko darstellen, als dass Apple und Google als Anbieter des ENF jederzeit technische Änderungen vornehmen könnten, die eine Identifizierbarkeit ermöglichen oder die von den Verantwortlichen ergriffenen eigenen Pseudonymisierungsmaßnahmen abschwächen oder gar aufheben können.

Der Umstand, dass die nationalen Corona-Apps das ENF von Google und Apple verwenden, stellt insoweit ein erhebliches Risiko für die gemeinsam verarbeiteten Daten dar, welchem

jedoch in erster Linie nur auf nationaler Ebene begegnet werden kann, da das ENF selbst keine Schnittstelle zum EFGS hat.

Das Risiko wird im Hinblick auf den verfolgten Zweck sowie die praktische Notwendigkeit des ENF zur Zweckerreichung derzeit im Ergebnis als akzeptabel bewertet. Jedoch sollten die gemeinsamen Verantwortlichen im Rahmen einer gemeinsamen Strategie den Dialog mit den ENF-Herstellern suchen, um Einfluss auf deren zukünftige Designentscheidungen nehmen zu können.

10 Nachhaltige Sicherung des Datenschutzes

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

10.1 Evaluierung

Sollte die Dringlichkeit der Zwecke der CWA nicht mehr im jetzigen Ausmaß gegeben sein, also etwa die Corona-Pandemie abflauen oder sich die Wirksamkeit der CWA als unzureichend erweisen, so müssen die Experten des RKI entscheiden, ob die CWA 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 einer solchen Entscheidung ist eine regelmäßige Evaluierung der Corona-Pandemie-Lage sowie der Wirksamkeit der CWA 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 erfolgt und welche Kriterien hierzu herangezogen werden.

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

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

10.2 Nächster Prüfungstermin

Die nächste Aktualisierung der DSFA erfolgt innerhalb von zwei Monaten nach Inbetriebnahme des EFGS, spätestens aber innerhalb von 6 Monaten nach Freigabe dieses DSFA-Berichts.

10.2.1.1 Anlagen

- Anlage 1: Designentscheidungen bei der Entwicklung der Corona-Warn-App der Bundesrepublik Deutschland (Version 1.5) und bei der Entwicklung des European Federation Gateway Service (EFGS) (Version 1.2)
- Anlage 2: Technisch-Organisatorische Maßnahmen (Version 1.1)
- Anlage 3: Risikomatrix VT 1, 2, 4 mit EFGS (Version 1.5)
- Anlage 4: Risikomatrix VT 3 Testing mit Laborschnittstelle (Version 1.5)
- Anlage 5: Risikomatrix Verification Hotline (Version 1.5)
- Anlage 6: Risikomatrix VT 5 EFGS (Version 1.4)
- Anlage 7: Vorbericht zur Anpassung der DSFA-Risikomatrizen (Anlage 3-5 zum DSFA-Bericht) für die Version 1.5
- Anlage 8: Glossar (Version 1.5)