

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 2.00 des öffentlichen¹ Berichts zur Datenschutz-Folgenabschätzung (DSFA)² 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 aktualisiert und die Ergebnisse werden jeweils in einer neuen Version des DSFA-Berichts veröffentlicht. Alle bisher veröffentlichten Versionen des DSFA-Berichts stellt das RKI auf der offiziellen Website der CWA (www.coronawarn.app) kostenlos zur Verfügung.

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

¹ Auf die Unterschiede zur internen (nicht-öffentlichen) Version des DSFA-Berichts wird unter Abschnitt 3.1 eingegangen.

² 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 V1.5	15.10.2020	Final
5	25.11.2020	1.2	Neue Funktionen des App-Releases V1.7		Final
6	09.12.2020	1.3	Berücksichtigung des App-Releases V1.8		Final
7	15.12.2020	1.4	Berücksichtigung des App-Releases V1.9		Final
8	17.12.2020	1.5	Berücksichtigung des App-Releases V1.10	08.01.2021	Final
9	28.01.2021	1.6	Berücksichtigung der App-Releases V1.11 und V1.12		Final
10	23.02.2021	1.7	Berücksichtigung des App-Releases V1.13		Final
11	12.03.2021	1.8	Berücksichtigung des App-Releases V1.14		Final
12	12.04.2021	1.9	Berücksichtigung des App-Releases V1.15		Final
13	14.04.2021	1.10	Berücksichtigung des App-Releases V2.00		Final
14	29.04.2021	1.11	Berücksichtigung des App-Releases V2.1		Final
15	11.05.2021	1.12	Berücksichtigung des App-Releases V2.2		Final

16	07.06.2021	1.13	Berücksichtigung des App-Releases V2.3		Final
17	25.06.2021	1.14	Berücksichtigung des App-Releases V2.4		Final
18	12.07.2021	1.15	Berücksichtigung des App-Releases V2.5		Final
19	26.07.2021	1.16	Berücksichtigung des App-Releases V2.6		Final
20	30.08.2021	1.17	Berücksichtigung der App-Releases V2.7 und V2.8		Final
21	18.09.2021	1.18	Berücksichtigung des App-Releases V2.9		Final
22	01.10.2021	1.19	Berücksichtigung des App-Releases V2.10		Final
23	09.12.2021	1.20	Berücksichtigung der App-Releases V2.11, V2.12, V2.13, V2.14 und V2.15		Final
24	11.10.2022	2.0	Berücksichtigung der App-Releases bis V2.25 einschließlich		Laufend

2 Inhalt

1	Vorausgehende Hinweise	2
2	Inhalt	5
3	Über diesen DSFA-Bericht.....	11
3.1	Gegenstand und Adressaten	11
3.2	Zusammensetzung und Vorgehensweise des DSFA-Teams	12
3.3	Name und Kontaktdaten des Verantwortlichen	14
3.4	Glossar	14
3.5	Abkürzungsverzeichnis	15
4	Notwendigkeit der DSFA.....	16
5	Beschreibung der CWA (Prüfgegenstand).....	18
5.1	Hintergrund und Release-Historie	18
5.2	Anwendungsphasen der CWA.....	22
5.3	Zwecke der Verarbeitung.....	23
5.3.1	Zweckdefinitionen	23
5.3.2	Abgrenzung zu anderen Zwecken	24
5.4	Ablauf aus Sicht eines CWA-Nutzers	24
5.4.1	Download und Installation der CWA App	24
5.4.2	Start der CWA App	25
5.4.3	Home-Bildschirm	26
5.4.4	Risiko-Ermittlung	26
5.4.5	Risikodetails	26
5.4.6	Statistik-Kacheln	27
5.4.7	Kontakt-Tagebuch / Begegnungshistorie	27
5.4.8	Testregistrierung	29
5.4.9	Namentlicher Schnelltest-Nachweis	31
5.4.10	Verifikations-Hotline	32
5.4.11	Erinnerung an das Warnen	32
5.4.12	Auslösen einer Warnung	33
5.4.13	Event-Registrierung	34
5.4.14	Zertifikats-Wallet	39
5.4.15	Weitere Funktionen	46
5.5	Systemarchitektur	50
5.5.1	Smartphone	51

5.5.2	CWA Server.....	52
5.5.3	CDN-Magenta.....	52
5.5.4	Verifikationsserver	53
5.5.5	Portalserver	53
5.5.6	Test Result Server.....	54
5.5.7	Data Donation Server	54
5.5.8	Log Storage Server	55
5.5.9	DCC Server	55
5.5.10	European Federation Gateway Service (EFGS)	55
5.5.11	Schweizer Gateway Service (CHGS)	57
5.5.12	Validierungsdienste	58
5.6	Datenflüsse und Prozesse	58
5.6.1	Risiko-Ermittlung	59
5.6.2	Berechnung des Infektionsrisikos.....	63
5.6.3	Testregistrierung.....	64
5.6.4	Verifikations-Hotline.....	67
5.6.5	Auslösen einer Warnung	68
5.6.6	Verwenden des Kontakt-Tagebuchs	74
5.6.7	Event-Registrierung.....	75
5.6.8	Anlegen eines Schnelltest-Profil.....	76
5.6.9	Fehlerberichte.....	76
5.6.10	Datenspende	77
5.6.11	Einladung zu Befragungen	80
5.6.12	Zertifikats-Wallet.....	80
5.6.13	Deinstallation der CWA App	88
5.7	Kategorien von Daten	89
5.7.1	Zugriffsdaten.....	89
5.7.2	Tagesschlüssel (TEK)	89
5.7.3	RPI.....	91
5.7.4	RPI-Metadaten (ENF V1)	91
5.7.5	Exposure-Window-Daten (ENF V2).....	92
5.7.6	Positivschlüssel (Diagnoseschlüssel).....	93
5.7.7	Metadaten zu Positivschlüsseln (CWA Server)	96
5.7.8	Bewertungseinstellungen (BWE).....	97
5.7.9	TAN	105

5.7.10	Registration Token	106
5.7.11	QR-Codes / GUID.....	106
5.7.12	Risikowert (Total Risk Score)	107
5.7.13	Risikostatus	107
5.7.14	Name und Telefonnummer (Verifikations-Hotline)	108
5.7.15	Antworten auf Plausibilitätsfragen (Verifikations-Hotline).....	108
5.7.16	Angaben zum Symptombeginn	108
5.7.17	Coronastatistik-Daten	108
5.7.18	Schnelltest-Nachweis (Datenkategorie)	109
5.7.19	Schnelltest-Profil (Datenkategorie).....	110
5.7.20	Kontakt-Tagebuch-Einträge.....	110
5.7.21	Event-Daten.....	111
5.7.22	Anwendungsdaten (Fehlerberichte)	112
5.7.23	Zertifikatsaussage	113
5.7.24	Eindeutige Zertifikatskennung	116
5.7.25	COVID-Zertifikate	117
5.7.26	Online-Validierungsdaten	117
5.7.27	Nutzungsdaten (Datenspende).....	120
5.8	Lösung der Daten	122
5.8.1	Daten der Risiko-Ermittlung.....	122
5.8.2	Daten der Testregistrierung	123
5.8.3	Daten der Warnfunktion.....	123
5.8.4	Schnelltest-Profile.....	124
5.8.5	Testergebnisse und Schnelltest-Nachweise.....	124
5.8.6	Kontakt-Tagebuch-Einträge.....	124
5.8.7	Event-Daten.....	125
5.8.8	Zugriffsdaten.....	125
5.8.9	Anwendungsdaten / Fehlerberichte	125
5.8.10	COVID-Zertifikate	126
5.8.11	Nutzungsdaten (Datenspende).....	126
5.8.12	Daten der Echtheitsprüfung (Token)	126
5.9	Akteure und betroffene Personen.....	126
5.9.1	RKI.....	126
5.9.2	Entwickler und Betreiber.....	127
5.9.3	Bundesregierung	128

5.9.4	BfDI	129
5.9.5	BSI	129
5.9.6	Teststellen / Testeinrichtungen	129
5.9.7	Labore	130
5.9.8	Öffentlicher Gesundheitsdienst der Länder	130
5.9.9	Hotline-Betreiber	130
5.9.10	Dienstleister für Support- und Pflegeleistungen	131
5.9.11	Hersteller der Smartphones / Betriebssysteme	132
5.9.12	Akteure des EFGS	132
5.9.13	Akteure des CHGS	132
5.9.14	Prüfer von COVID-Zertifikaten / Leistungsanbieter	133
5.9.15	Betreiber von Validierungsdiensten (Prüfpartner)	133
5.9.16	Betroffene Personen	133
5.10	Begleitdokumente zur Beschreibung des Prüfgegenstands	134
6	Einholung des Standpunktes der betroffenen Personen	134
7	Datenschutzrechtliche Bewertung	135
7.1	Personenbezug der Daten	136
7.1.1	Verarbeitung durch zentrale CWA-Dienste (Serversystem der CWA)	136
7.1.2	Verarbeitung für die Online-Validierung	138
7.1.3	Lokale Verarbeitung auf dem Smartphone	138
7.2	Gesundheitsdaten	139
7.3	Verantwortlichkeit	141
7.3.1	Verarbeitung durch zentrale CWA-Dienste	141
7.3.2	Lokale Verarbeitung durch die CWA App	141
7.3.3	Lokale Verarbeitung durch das ENF	146
7.3.4	Verarbeitung durch den EFGS	147
7.3.5	Verarbeitung durch den CHGS	147
7.3.6	Verarbeitung durch Lab Server / Teststellen-Informationssysteme	147
7.3.7	Verarbeitung durch Prüfsysteme	147
7.3.8	Verarbeitung durch Validierungsdienste	147
7.4	Auftragsverarbeiter	148
7.5	Rechtsgrundlagen	148
7.5.1	Anforderungen an eine Rechtsgrundlage	148
7.5.2	Rechtsgrundlagen der CWA	149
7.5.3	Begründung der Einwilligung als Rechtsgrundlage	152

7.6	Bewertung der Drittlandübermittlung	164
7.7	Rechte der betroffenen Personen.....	166
7.7.1	Rechte der CWA-Nutzer.....	167
7.7.2	Rechte anderer Nutzer	171
7.7.3	Rechte von Dritten.....	172
7.8	Data Protection by Design and by Default.....	172
7.9	Weitere datenschutzrechtliche Anforderungen	172
8	Bewertung der Notwendigkeit und Verhältnismäßigkeit	174
8.1	Zweck 1	174
8.1.1	Legitimer Zweck	174
8.1.2	Eignung	174
8.1.3	Erforderlichkeit.....	176
8.1.4	Angemessenheit.....	178
8.2	Zweck 2	181
8.2.1	Legitimer Zweck	181
8.2.2	Eignung	182
8.2.3	Erforderlichkeit.....	183
8.2.4	Angemessenheit.....	184
8.3	Zweck 3	185
8.3.1	Legitimer Zweck	185
8.3.2	Eignung	185
8.3.3	Erforderlichkeit.....	185
8.3.4	Angemessenheit.....	186
8.4	Zweck 4	186
8.4.1	Legitimer Zweck	186
8.4.2	Eignung	186
8.4.3	Erforderlichkeit.....	187
8.4.4	Angemessenheit.....	189
8.5	Zweck 5	190
8.5.1	Legitimer Zweck	190
8.5.2	Eignung	190
8.5.3	Erforderlichkeit.....	191
8.5.4	Angemessenheit.....	191
9	Risikoanalyse.....	191
9.1	Methodik	191

9.1.1	Änderungshistorie.....	192
9.2	Risiko-Identifikation.....	193
9.3	Risikoquellen	193
9.3.1	Bedrohungen/Risiken	194
9.3.2	Zuordnung der Risiken zu Betroffenengruppen.....	194
9.3.3	Bewertung der Eintrittswahrscheinlichkeit	195
9.3.4	Bewertung der Schadenshöhe	196
9.4	Maßnahmen zur Risikobehandlung	200
9.5	Bewertung von hohen Restrisiken	201
9.5.1	Hohe Restrisiken der CWA.....	202
9.6	Hohe Restrisiken der Interoperabilität	210
9.6.1	Fehlende Rechtsgrundlage	211
9.6.2	Verarbeitung veralteter oder nicht erforderlicher Daten	211
9.6.3	Verwendung und technische Einschränkungen des ENF	212
9.7	Zertifikats-Wallet	213
10	Nachhaltige Sicherung des Datenschutzes.....	213
10.1	Evaluierung	213
10.2	Nächster Prüfungstermin	214
11	Anlagen	215

3 Über diesen DSFA-Bericht

3.1 Gegenstand und Adressaten

Dieser DSFA-Bericht dokumentiert in zusammengefasster Form die Ergebnisse der für die unter Abschnitt 5 beschriebenen Verarbeitungsvorgänge durchgeführten DSFA.

Der vom DSFA-Team im Auftrag der Behördenleitung erstellte DSFA-Bericht bildet den gemäß Art. 35 Abs. 7 DSGVO vorgegebenen Mindestinhalt der DSFA ab.

Zusätzlich enthält der DSFA-Bericht teilweise weitergehende Erläuterungen und Detaildarstellungen auf sprachlicher und inhaltlicher Ebene, die nicht zwingend in einen DSFA-Bericht aufzunehmen sind und üblicherweise auch nicht aufgenommen werden. Diese Maßnahme dient vor dem Hintergrund der Veröffentlichung des DSFA-Berichts der allgemeinen Verständlichkeit für die interessierte Öffentlichkeit und Nicht-Fachleser und der einfacheren Überprüfung der Ergebnisse durch unabhängige Dritte. Zugleich wird die Erfüllung von Informationspflichten bei Konsultationsverfahren nach Art. 36 DSGVO erleichtert.

Adressat des DSFA-Berichts ist das RKI als Verantwortlicher für die CWA im Sinne des Art. 4 Nr. 7 DSGVO. Nachgeordnet richtet sich der DSFA-Bericht aus den bereits genannten Gründen auch an die interessierte Öffentlichkeit sowie die Datenschutzaufsichtsbehörden des Bundes und der Länder, politische Entscheidungsträger und sonstige Stakeholder.

Mit der Veröffentlichung der vorliegenden öffentlichen Version des DSFA-Berichts, die gesetzlich nicht vorgeschrieben ist, möchte das RKI das Vertrauen der Bevölkerung in den Datenschutz der CWA stärken, Transparenz hinsichtlich der Funktionsweise und den Sicherheitsmaßnahmen der CWA schaffen und Anregungen für die öffentliche Diskussion geben.

Die öffentliche Version des DSFA-Berichts umfasst alle Elemente des internen DSFA-Berichts und gibt die Ergebnisse der Risikoanalyse vollständig wieder. Aus Datenschutzgründen enthält das vorliegende Dokument jedoch keine nicht öffentlich zugänglichen personenbezogenen Angaben zu den an der DSFA-Durchführung auf Seiten des RKI, anderer Behörden, der Umsetzungspartner oder anderer Dienstleister des RKI direkt oder indirekt beteiligten Personen. Aus Gründen des Datenschutzes, zur Wahrung von Vertraulichkeitspflichten oder zur Vermeidung von Gefahren für die Informationssicherheit wird von einer Veröffentlichung einzelner Begleitdokumente abgesehen. Um gleichwohl die Nachvollziehbarkeit der veröffentlichten Ergebnisse durch die interessierte Öffentlichkeit zu gewährleisten, enthält dieses Dokument sinngemäße Darstellungen von potenziell ergebnisrelevanten, aber nicht zur Veröffentlichung vorgesehenen Informationen. Dies erklärt neben den oben genannten Gründen den punktuell großen Umfang und hohen Detailgrad der Darstellung.

Damit der große Umfang des DSFA-Berichts angesichts der unterschiedlichen Transparenzbedarfe des breiten Adressatenkreises nicht selbst ein Transparenzhindernis darstellt, werden Zusammenfassungen der wesentlichen Designentscheidungen dem DSFA-Bericht als Begleitdokumente beigefügt. In diesen Zusammenfassungen werden in allgemein

verständlicher Form die von fachkundigen Organisationen für deutsche bzw. europäische Tracing-Apps identifizierten Risiken und die zur Risikobehandlung geforderten Datenschutzmaßnahmen genannt und den für die CWA umgesetzten Maßnahmen gegenübergestellt.

3.2 Zusammensetzung und Vorgehensweise des DSFA-Teams

Mit der Planung und praktischen Durchführung der DSFA hat die Behördenleitung am 12.05.2020 ein interdisziplinäres Team bestehend aus in verschiedenen federführenden Funktionen am CWA-Projekt beteiligten Personen beauftragt. Das Kernteam besteht aus Mitarbeiterinnen und Mitarbeitern der technischen Umsetzungspartner T-Systems International GmbH (TSI) und SAP Deutschland SE & CO. KG (SAP) sowie Rechtsanwältinnen und Rechtsanwälten der Kanzlei Schürmann Rosenthal Dreyer Partnerschaft von Rechtsanwälten mbB. Die Mitglieder des Kernteams üben in ihren jeweiligen Fachgebieten jeweils eine federführende Zuständigkeit im CWA-Projekt aus. Die Teammitglieder und die ihnen jeweils zugewiesenen Aufgaben decken die für die Identifikation, Bewertung und Entscheidung über Risikobehandlungsmaßnahmen erforderliche Bandbreite an Qualifikationen und Kompetenzen in den Bereichen Entwicklung, IT Security, Recht und Projektmanagement ab. Darüber hinaus erfolgte eine punktuelle Mitwirkung durch wissenschaftliche Projektbeteiligte auf Seiten des RKI, welche beispielsweise die für die DSFA-Durchführung erforderliche epidemiologische Expertise in das DSFA-Team eingebracht haben.

Die DSB steht dem DSFA-Team beratend zur Seite. Eine regelmäßige Einbindung der DSB in die Entscheidungsprozesse des DSFA-Teams erfolgt nicht, um die Unabhängigkeit der Prüfung und der Entscheidungsprozesse über gebotene Risikobehandlungsmaßnahmen zu wahren.

Auftragsgemäß erfolgte die federführende Durchführung der Risikoanalyse im Rahmen der DSFA durch die technischen Umsetzungspartner TSI und SAP. Beratend zur Seite standen dem TSI-/SAP-Team die Rechtanwältinnen und Rechtsanwälte der Kanzlei Schürmann Rosenthal Dreyer Partnerschaft von Rechtsanwälten mbB, die federführend für die Abstimmung von Beratungs- und Anhörungsthemen mit dem BfDI zuständig sind.

Ein wesentlicher Teil sowohl der Designentscheidungen als auch der DSFA-Durchführung erfolgt seit Projektbeginn im Rahmen des Workstreams „Datenschutz“, der seit dem 12.05.2020 besteht. Dem Workstream „Datenschutz“ gehören neben Mitgliedern des DSFA-Teams auch weitere Projektbeteiligte an. Er umfasst die parallellaufenden Arbeitsstränge „Datenschutzkonzept“ einerseits und „DSFA“ andererseits, die Hand in Hand arbeiten. Aufgrund der agilen Entwicklungsweise der CWA fließen seit Projektbeginn kontinuierlich Risikobetrachtungen und Zwischenergebnisse aus der DSFA in Architekturentscheidungen ein, die jeweils zu Änderungen des Datenschutzkonzepts führen und kurzfristig bei der Durchführung bzw. Aktualisierung der DSFA berücksichtigt werden müssen. Zudem wurde das Feedback der Entwicklungs-Community in den Workstreams berücksichtigt. Insgesamt stellt sich die Risikobetrachtung im Rahmen der DSFA 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.

Die Änderungen und Designentscheidungen im Rahmen des Datenschutzkonzepts sowie potenzielle Risikobehandlungsmaßnahmen und damit zusammenhängende organisatorische Themen einschließlich der Vorbereitung von Beratungs- und Anhörungsterminen mit dem BfDI wurden zwischen dem DSFA-Team, der DSB sowie ggf. Vertretern der jeweils zuständigen Workstreams laufend ausführlich erörtert. Zur Klärung von wesentlichen Fragen in Bezug auf neue Funktionen der CWA App wurden teilweise auch Vertreter des Bundesministeriums für Gesundheit (BMG) informatorisch hinzugezogen.

Vor dem Hintergrund der vom RKI mit der Veröffentlichung des DSFA-Berichts verfolgten Ziele hat das DSFA-Team bei der Durchführung der DSFA die öffentlichen Stellungnahmen und konkreten Forderungen von fachkundigen Organisationen zu den datenschutzrechtlichen Aspekten einer Corona-Tracing-App umfassend berücksichtigt und im Zusammenhang mit den ergriffenen technischen und organisatorischen Maßnahmen in diesem DSFA-Bericht dokumentiert. Ebenso wurden die Stellungnahmen und Forderungen von europäischen Datenschutzaufsichtsbehörden und Datenschutzgremien berücksichtigt³.

Die Durchführung der Risikoanalyse erfolgte in methodischer Hinsicht in Anlehnung an das von den Datenschutzbehörden des Bundes und der Länder empfohlene Standard-Datenschutzmodell⁴ (SDM), so dass die identifizierten Risiken den dem SDM zugrunde liegenden Gewährleistungszielen zugeordnet werden können. Die Gewährleistungsziele des SDM sind aus den in Art. 5 DSGVO festgelegten Verarbeitungsgrundsätzen abgeleitet, wobei jedem Gewährleistungsziel spezifische technische und organisatorische Abhilfemaßnahmen zugeordnet sind, mittels derer das jeweilige Ziel und die dahinterstehenden Anforderungen der DSGVO gewährleistet und der Eintritt von Schadensereignissen verhindert werden können. Zur Bewertung der identifizierten Risiken hat das DSFA-Team eine bewährte Risiko-Matrix für datenverarbeitungsintensive Vorhaben aus dem Gesundheitsbereich verwendet, die auf anerkannten Standards beruht und vom DSFA-Team an die spezifischen Anforderungen des CWA-Projekts angepasst worden ist. Als zentrales Hilfsmittel für die Planung und Dokumentation der Risikoanalyse hat das DSFA-Team eine von der Telekom entwickelte Excel-Arbeitsmappe verwendet, die in Abschnitt 9 näher beschrieben wird.

³ Datenschutzkonferenz, Kurzpapier Nr. 5 zur Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, Stand: 17.12.2018, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf (abgerufen am 11.10.2022) und Kurzpapier Nr. 18 zum Risiko für die Rechte und Freiheiten natürlicher Personen, Stand: 26.04.2018, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (abgerufen am 11.10.2022); 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 11.10.2022).

⁴ DSK, Das Standard-Datenschutzmodell Version 2.0b, abrufbar unter: <https://www.datenschutzzentrum.de/sdm/> (zuletzt abgerufen am 11.10.2022).

3.3 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

Leitung	Prof. Dr. Lothar H. Wieler (Präsident)
----------------	--

Datenschutzbeauftragte	Claudia Enge
E-Mail-Adresse der Datenschutzbeauftragten	datenschutz@rki.de

3.4 Glossar

Für die effektive Zusammenarbeit der zahlreichen am CWA-Projekt mitwirkenden Personen 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
CWA	O	Corona-Warn-App
DCC-VO	§	Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates vom 14. Juni 2021 über einen Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von COVID-19-Impfungen und -Tests sowie der Genesung von einer COVID-19-Infektion (digitales COVID-Zertifikat der EU) mit der Zielsetzung der Erleichterung der Freizügigkeit während der COVID-19-Pandemie
DSGVO	§	Datenschutz-Grundverordnung
EDSA	O	Europäischer Datenschutzausschuss
EGS	T	Eigenschlüssel (eigene Tagesschlüssel)
ENF	T	Exposure Notification Framework (Expositionenbenachrichtigungswerkzeug)
EPS	T	Empfangsschlüssel
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
SES	T	Sendeschlüssel
TAN	T	Transaktionsnummer
TEK	T	Temporary Exposure Keys (Tagesschlüssel)
TRL	T	TransmissionRiskLevel

4 Notwendigkeit der DSFA

Art. 35 Abs. 1 DSGVO regelt die Pflicht zur Durchführung einer DSFA und schreibt diese vor, wenn, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Zur weiteren Konkretisierung der gesetzlichen Anforderungen erstellen und veröffentlichen die Datenschutzaufsichtsbehörden gemäß Art. 35 Abs. 4 DSGVO Listen der Verarbeitungsvorgänge, für die auf jeden Fall eine DSFA durchzuführen ist („Muss-Listen“).

Für die CWA ergibt sich die Notwendigkeit einer DSFA bereits aus dem Regelbeispiel des Art. 35 Abs. 3 lit. b DSGVO, wonach vor einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO eine DSFA durchzuführen ist. Das gleiche Ergebnis folgt aus der Liste des BfDI⁵, denn die Merkmale der

⁵ 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/Muster/Liste_VerarbeitungsvorgaengeArt35.pdf;jsessionid=432AFB89A8301F333B53A6582084C3DD.intranet242?__blob=publicationFile&v=5 (abgerufen am 11.10.2022).

darin unter Nr. 4 a., 5, 7 c. und d. sowie 8 genannten Verarbeitungstätigkeiten treffen auf die CWA zu.

Auch nach der Auffassung des EDSA muss vor der Einführung einer Tracing-App eine DSFA durchgeführt werden, weil „die Verarbeitung als mit einem hohen Risiko (Gesundheitsdaten, voraussichtliche flächendeckende Einführung, systematische Überwachung, Einsatz neuer technologischer Lösungen) behaftet“ eingestuft wird.⁶ 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.⁷

Aufgrund des engen Zusammenhangs mit den Verarbeitungstätigkeiten der App-Komponente (CWA App) und den Diensten im Backend der CWA hat das DSFA-Team entschieden, dass auch Verarbeitungstätigkeiten der **Verifikations-Hotline** zum Prüfgegenstand der DSFA gehören. Die Verifikations-Hotline wirkt sich wesentlich auf die Zweckerreichung der CWA aus und ist daher eine notwendige Komponente des Gesamtverfahrens der CWA.

⁶ 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 11.10.2022).

⁷ 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 11.10.2022).

5 Beschreibung der CWA (Prüfgegenstand)

Gegenstand der vorliegenden DSFA sind die nachfolgend beschriebenen Verarbeitungsvorgänge der CWA. Die Darstellung bildet den Stand des App-Releases Version 2.25 ab.

Zur allgemeinen Verständlichkeit und Nachvollziehbarkeit der Ergebnisse der DSFA werden teilweise auch Verarbeitungsvorgänge beschrieben, die außerhalb des Prüfgegenstands oder des Verantwortungsbereichs des RKI liegen. An entsprechender Stelle wird ggf. darauf hingewiesen.

5.1 Hintergrund und Release-Historie

Der Beginn der prüfgegenständlichen Verarbeitung erfolgte am 16.06.2020 mit dem Release der ersten Version der CWA App in den deutschen App Stores von Apple und Google durch das RKI.

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

Zu Beginn war die CWA App monofunktional ausgelegt. Ihre primäre Funktionalität war das Warnen anderer, daher enthielt die CWA App nur die für das Auslösen einer Warnung sowie dem Warnen vorgesetzten Tracing mittels der **Begegnungsaufzeichnung** und den **Testergebnisabruf** notwendigen Funktionen. Im Laufe der Zeit wurde die CWA App um weitere Funktionalitäten erweitert, die auch über das Warnen hinausgehende Nutzungsszenarien ermöglichen.

Da das Warnsystem der CWA auf einem dezentralen Tracingkonzept beruht, findet die Begegnungsaufzeichnung ausschließlich lokal, also auf dem Smartphone des CWA-Nutzers statt. Für den Testergebnisabruf und die gezielte Aussteuerung von Warnungen an potenzielle Kontaktpersonen muss die CWA App jedoch auf zentrale Fachdienste zurückgreifen. Diese werden von weiteren CWA-Komponenten – **CWA Server**, **Verifikationsserver**, Verifikations-Hotline und weiteren Diensten – bereitgestellt. Zudem werden von zentralen CWA-Komponenten auch Dienste für nachträglich eingeführte optionale Nebenfunktionen der CWA App bereitgestellt.

Die CWA App nutzt für die Begegnungsaufzeichnung das gemeinsam von Apple und Google für Corona-Tracing-Apps 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 zwingende Systemvoraussetzung der CWA App, d. h. für Smartphones mit

Betriebssystemen ohne Schnittstelle zum ENF kann die CWA App nicht angeboten werden, weshalb sie beispielsweise auch nicht in der Huawei AppGallery bzw. für Smartphones mit dem Betriebssystem Harminoy OS bereitgestellt werden kann.

Das ENF ermöglicht Smartphones mit den Betriebssystemen iOS und Android den kontinuierlichen, betriebssystemübergreifenden Austausch von **ZufallsCodes (Zufalls-IDs⁸)** zur Kontaktnachverfolgung per **Bluetooth Low Energy (BLE)**, ohne dass die Akkulaufzeit des Smartphones merklich darunter leidet. Die Datenverarbeitung durch das ENF findet auf Ebene des jeweiligen Betriebssystems statt und liegt daher außerhalb des direkten Einflussbereichs des RKI.

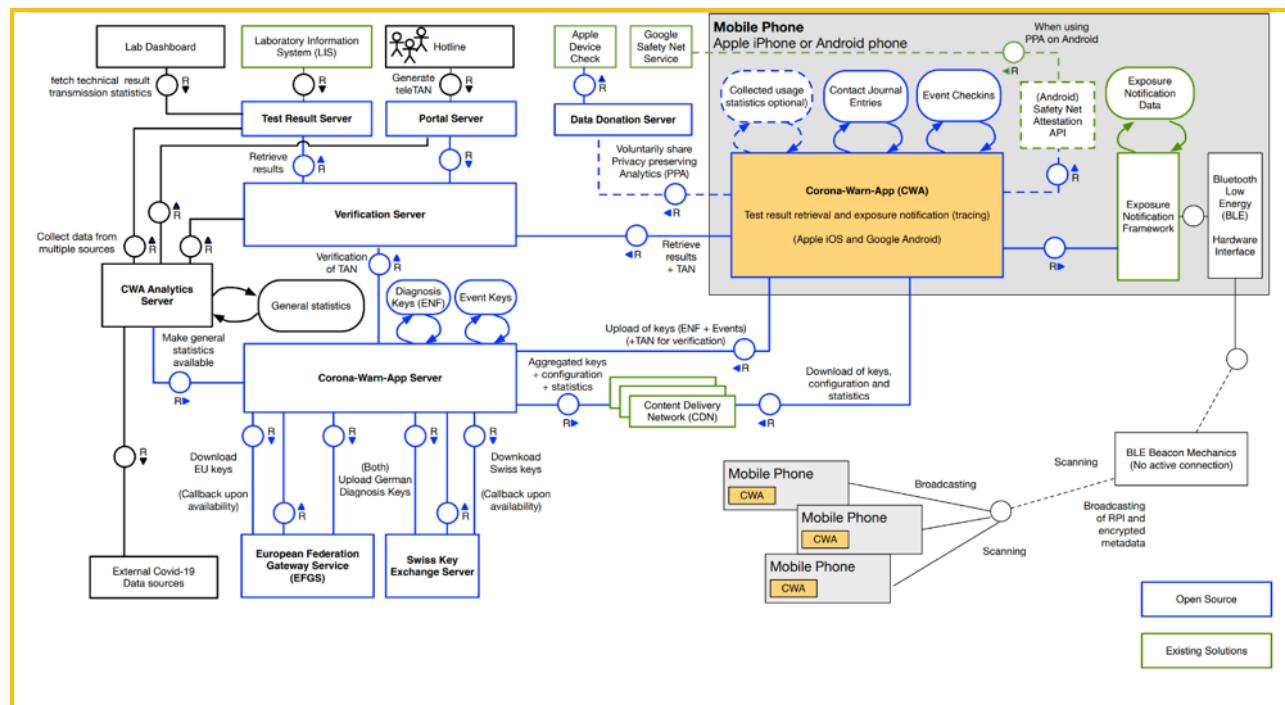


Abbildung 01: Überblick über die Gesamtarchitektur der CWA

Nach ihrer erstmaligen Veröffentlichung haben die Komponenten und Dienste der CWA mehrere Updates erhalten, mit denen Fehler behoben und die vorhandenen Funktionen optimiert und barrierefreier gestaltet worden sind.

Grundlegende Funktionserweiterungen wurden erstmals mit dem Release der CWA App Version 1.5 eingeführt:

⁸ Der Begriff „Zufalls-ID“ wird in der Datenschutzerklärung der CWA App 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. In diesem DSFA-Bericht wird der Begriff der Zufalls-ID in der Regel nur im Zusammenhang mit Einwilligungserklärungen verwendet.

- Die Warnfunktion wurde um eine Symptomabfrage erweitert, sodass ein **positiv getesteter CWA-Nutzer** beim Auslösen einer Warnung angeben kann, wann eventuelle typische Corona-Symptome (Fieber, Husten, Geschmacksverlust usw.) erstmals aufgetreten sind. Diese Angabe wird genutzt, um das **Übertragungsrisiko** für **Kontaktpersonen** des CWA-Nutzers genauer zu berechnen. Eine Abfrage konkreter Symptome erfolgt nicht.
- Zudem wurde die länderübergreifende Funktionsweise der Risiko-Ermittlung und der Warnfunktion (Interoperabilität) eingeführt. Teilnehmende Länder in der Europäischen Union (bzw. potenziell dem Europäischen Wirtschaftsraum) betreiben hierfür einen gemeinsamen Austausch-Server⁹, den EFGS, über den Positivschlüssel zwischen den nationalen Corona-Apps ausgetauscht werden, um die jeweils eigenen Nutzer über Risiko-Begegnungen auch mit Nutzern anderer Apps informieren zu können.

Mit den folgenden Releases der CWA App wurden neben Fehlerbereinigungen und Detailverbesserungen von Bestandsfunktionen zahlreiche weitere Bestandsfunktionen erweitert und neue Funktionen ergänzt.¹⁰ Für die datenschutzrechtliche Bewertung des Prüfgegenstands sind insbesondere folgende Funktionserweiterungen bzw. -ergänzungen relevant und werden in der Risikoanalyse berücksichtigt:

- Mit dem Release der CWA App Version 1.10 wurde das Kontakt-Tagebuch und mit dem Release der CWA Version 1.11 wurde die Statistik-Kachel eingeführt. Diese Funktionen ermöglichen eine Nutzung der CWA App zu persönlichen Informationszwecken und stellen insoweit einen Bruch mit der zunächst monofunktionalen Auslegung der CWA App als reine Tracing- bzw. Warn-App dar.
- Mit dem Release der CWA App Version 1.12 wurde das Kontakt-Tagebuch um die sogenannte Begegnungshistorie erweitert werden. Die Begegnungshistorie führt den bisher auf der Risiko-Kachel auf dem Home-Screen angezeigten Risikostatus mit dem Kontakt-Tagebuch zusammen. Dies ermöglicht dem CWA-Nutzer, rückblickend nachzuvollziehen, an welchen Tagen die CWA App welches Risiko errechnet hat. Dies verbessert die Aussagekraft und den Nutzen der Risiko-Ermittlung insofern, als dass nun nicht mehr nur der aktuelle, sondern auch vergangene Risikostatus an spezifischen Tagen einsehbar sind.
- Mit dem Release der CWA App Version 1.13 wurde die Möglichkeit geschaffen, mit der CWA-Nutzer an Befragungen des RKI zur Nutzung der CWA App und über die CWA App erhaltenen Warnungen teilnehmen können. Zusätzlich wurde eine Datenspendefunktion eingeführt, über die CWA-Nutzer dem RKI Daten über das eigene Nutzungsverhalten für Analyticszwecke zur Verfügung stellen können.

⁹ Der Begriff Austausch-Server wird in der Datenschutzerklärung der CWA App 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 Glossarbegriff „European Federation Gateway Service“ (EFGS) verwendet.

¹⁰ Die vollständige Release-Übersicht kann auf den Projektseiten auf github eingesehen werden, abrufbar unter: <https://github.com/corona-warn-app/cwa-app-ios/releases> (zuletzt abgerufen am 25.10.2022). Releases, die in erster Linie für die datenschutzrechtliche Bewertung des Prüfgegenstands nicht relevante Bugfixes enthalten werden in der nachfolgenden Auflistung nicht erwähnt.

- Mit dem Release der CWA App Version 1.14 wurden die Funktionen des Kontakt-Tagebuchs erweitert. Zu den Stammdaten von gespeicherten Orten und Personen können CWA-Nutzer nun auch die E-Mail-Adresse sowie die Telefonnummer im Kontakt-Tagebuch sowie weitere Angaben zu den Umständen des Kontakts hinterlegen.
- Mit dem Release der CWA App Version 1.15 wurde die mit Release 1.5 eingeführte Interoperabilität auf EU-Ebene um die Schweiz erweitert. Hierfür wurde vom RKI zusammen mit dem Betreiber der Schweizer Corona-App, dem Bundesamt für Gesundheit (BAG), nach dem Vorbild des EFGS ein weiterer gemeinsamer Austausch-Server, der CHGS, eingerichtet.
- Mit dem Release der CWA App Version 2.0 wurde vor dem Hintergrund neuer Forschungsergebnisse über die Verbreitungswege des Corona-Virus die Event-Registrierung eingeführt. Diese ermöglicht unabhängig von der Begegnungsaufzeichnung bzw. dem ENF die Warnung von CWA-Nutzern, die sich während eines gemeinsamen Zeitintervalls am gleichen Ort oder auf derselben Veranstaltung aufgehalten haben. Damit wird dem Umstand Rechnung getragen, dass insbesondere in Innenräumen durch hohe Aerosolkonzentrationen auch bei größeren Abständen ein erhebliches Infektionsrisiko bestehen kann, welches mit der ENF-basierten Begegnungsaufzeichnung aber nicht abgebildet werden kann.
- Seit dem Release der CWA App Version 2.1 können in teilnehmenden Teststellen durchgeführte Antigen-Schnelltests in der CWA App registriert und positive Schnelltest-Ergebnisse können genutzt werden, um andere zu warnen. Wenn der CWA-Nutzer gegenüber der Teststelle eine entsprechende Einwilligung erklärt hat, können die in der CWA App angezeigten Schnelltest-Ergebnisse als namentliche Schnelltest-Nachweise gegenüber Dritten verwendet werden.
- Seit dem Release der CWA App Version 2.2 können CWA-Nutzer in der App sogenannte Schnelltest-Profile anlegen. Diese können verwendet werden, um im Rahmen der Anmeldung zum Test in einer Teststelle dieser die erforderlichen Daten schnell per QR-Code zur Verfügung zu stellen. Die Verwendung des Schnelltest-Profiles ersetzt dann die händische Eingabe in das datenführende System der Teststelle. Zusätzlich kann der CWA-Nutzer in der CWA App ab dem Release 2.2 auch einen Fehlerbericht zu Supportzwecken erstellen.
- Seit dem Release der CWA App Version 2.3 verfügt die CWA App über eine vollwertige Wallet-Funktionalität für COVID-19-Impfzertifikate. Als Wallet für COVID-19-Testzertifikate kann die CWA App seit den Release 2.4 und für COVID-19-Genesenenzertifikate seit Release 2.5 genutzt werden. Zudem wurde mit Release 2.5 die Funktion für Familienzertifikate eingeführt, so dass der CWA-Nutzer die CWA App auch als Wallet für COVID-Zertifikate von Familienmitgliedern nutzen kann.
- Seit dem Release der CWA App Version 2.6 können CWA-Nutzer die Gültigkeit von COVID-Zertifikaten anhand der aktuell geltenden nationalen Gültigkeitsregelungen der teilnehmenden EU-Mitgliedsländer prüfen. Diese inhaltliche („fachliche“) Gültigkeitsprüfung wurde mit Release 2.7 um eine technische Gültigkeitsprüfung anhand technischer Faktoren (Signaturprüfung) erweitert.
- Mit dem Release der CWA App Version 2.9 wurde die Event-Registrierung um die Funktion „In Vertretung warnen“ erweitert, so dass Warnungen an Event-Teilnehmer

auch dann ausgelöst werden können, wenn die Person, von der das Infektionsrisiko ausgeht, kein CWA-Nutzer ist.

- Seit dem Release der CWA App Version 2.10 können lokale Push-Mitteilungen zur Erinnerung an notwendige Auffrischimpfungen genutzt werden. Zudem wurde die Wallet der CWA App um eine Funktion zum Drucken und Exportieren von COVID-19-Zertifikaten ergänzt.
- Mit dem Release der CWA App Version 2.15 wurde die Wallet der CWA App um eine Funktion für den Nachweis von COVID-Zertifikaten im Rahmen von Online-Validierungsverfahren bei Drittanbietern (z. B. Reise- und Veranstaltungsunternehmen) ergänzt.¹¹
- Mit dem Release der CWA App Version 2.18 wurde eine Funktion zur Prüfung und Anzeige des G-Status zu COVID-Zertifikaten ergänzt. Die Prüfung erfolgt gegen die Statusregelungen des Bundes und der Länder, die dynamisch, also tagesaktuell, geladen werden.
- Mit den Releases der CWA App Versionen 2.19, 2.21 und 2.22 wurden die Funktionen zur Verwaltung von Familienzertifikaten sowie zur Zuordnung zu COVID-Zertifikaten zu Personen verbessert.
- Mit dem Release der CWA App Version 2.23 wurden die Funktionen zur Erneuerung von technisch abgelaufenen COVID-Zertifikaten ergänzt.
- Mit dem Release der CWA App Version 2.24 wurde die Exportfunktion für COVID-Zertifikate dahingehend erweitert, dass nunmehr alle gespeicherten Zertifikate in einer zusammenhängenden PDF-Datei exportiert werden können.

5.2 Anwendungsphasen der CWA

In der öffentlichen CWA-Dokumentation und in den Designentscheidungen der CWA wird die Nutzung der CWA App aus der Perspektive eines CWA-Nutzers in vier Phasen eingeteilt (User Journey):¹²

- Phase Idee
- Phase Installation
- Phase Anwendung
- Phase Deinstallation

Die Phase „Anwendung“ wird nochmals in vier Unterabschnitte (jeweils als eine „Anwendungsphase“ bezeichnet) unterteilt:

- Anwendungsphase 1: Hintergrund
- Anwendungsphase 2: Kontaktfall
- Anwendungsphase 3: Testing

¹¹ Diese Funktion wurde parallel auch mit der CovPass-App Version 1.14 bereitgestellt.

¹² Siehe z. B. im Scoping-Dokument unter https://github.com/corona-warn-app/cwa-documentation/blob/88150d82ece4a5f5d1eaa7f7320ef177ee3c6109/translations/scoping_document.de.md (zuletzt abgerufen: 11.10.2022).

- Anwendungsphase 4: Infektfall

Soweit in diesem DSFA-Bericht eine Zuordnung von Funktionen, Datenflüssen oder Prozessen zu den vorgenannten Phasen vorgenommen wird, dient dies dazu, dem Leser die Herstellung von Bezügen zu anderen Bestandteilen der Dokumentation zu erleichtern.¹³

5.3 Zwecke der Verarbeitung

5.3.1 Zweckdefinitionen

Das RKI hat die Zwecke der Verarbeitung im Rahmen der CWA wie folgt definiert:¹⁴

- (1) Einzelpersonen sollen darüber informiert bzw. gewarnt werden, dass ein erhöhtes Infektionsrisiko besteht, weil sie sich in unmittelbarer Nähe zu einer Corona-infizierten Person¹⁵ 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.
- (3) Bürgerinnen und Bürger sollen sich jederzeit niedrigschwellig über tagesaktuelle Statistiken zum Infektionsgeschehen informieren können.
- (4) Personen, für die bestimmte Erleichterungen oder Ausnahmen von Schutzmaßnahmen des Bundes, der Länder oder in anderen EU-Mitgliedsstaaten zur Eindämmung der Corona-Pandemie gelten, soll eine einfache und EU-weit anerkannte Möglichkeit an die Hand gegeben werden, um nachweisen zu können, dass sie von diesen Erleichterungen oder Ausnahmen erfasst sind.

¹³ Die genannten Phasen wurden zu Beginn der Entwicklung der CWA festgelegt. Zu diesem Zeitpunkt war die CWA App als reine Tracing-App konzipiert, d. h. die User Journey war vorhersehbar. Wegen des nachträglich erheblich erweiterten Funktionsumfangs ist eine klare Einteilung der User Journey in Phasen nicht immer praktikabel und wird in der neueren Dokumentation ggf. nicht mehr vorgenommen.

¹⁴ Die Zweckdefinition wurden seit Projektbeginn teilweise sprachlich und inhaltlich angepasst, um sprachliche Klarstellungen vorzunehmen. Zudem wurden vor der Einführung neuer Funktionen in einigen Fällen neue Zwecke definiert oder bestehende Zwecke erweitert, um dem geänderten Funktionsumfang der CWA abbilden zu können.

¹⁵ 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.

- (5) Bürgerinnen und Bürger sollen bei der niedrigschweligen Inanspruchnahme von präventiven Corona-Tests unterstützt werden.

5.3.2 Abgrenzung zu anderen Zwecken

Folgende 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)
- Behandlung von COVID-19-Erkrankten

Die unter Abschnitt 5.3.1 genannten Zweckdefinitionen umfassen diese Zwecke nicht und werden vom RKI im Zusammenhang mit der CWA auch nicht angestrebt. Falls personenbezogene Daten von CWA-Nutzern im Zusammenhang mit dem Prüfgegenstand für die vorgenannten weiteren Zwecke genutzt werden sollen, muss die DSFA um eine Betrachtung der jeweiligen 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.¹⁶

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-

¹⁶ 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 7.5.3.2.1 ausgeführt.

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-Beschreibungsseite der CWA App kann der CWA-Nutzer vor dem Download der CWA App die Datenschutzerklärung und die Nutzungsbedingungen der CWA App aufrufen. Das RKI hat keinen Einfluss auf die Datenverarbeitung durch die App-Store-Betreiber.

5.4.2 Start der CWA App

5.4.2.1 Onboarding

Wenn der CWA-Nutzer die CWA App nach ihrer Installation zum ersten Mal startet, fragt die CWA App die Systemsprache ab, um die Benutzeroberfläche der CWA App in der Systemsprache anzuzeigen. Wenn die CWA App nicht in der Systemsprache angezeigt werden kann, wird die englische Sprachfassung angezeigt.

Nach dem initialen Start der CWA App erhält der CWA-Nutzer eine Einführung in die Funktionsweise der CWA App. Im Rahmen des Onboardings wird der CWA-Nutzer in allgemeiner Form über die wesentlichen Zwecke und die technische Funktionsweise der CWA App informiert und die 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 die **Einwilligung** des CWA-Nutzers und ist daher zunächst deaktiviert. Die Aktivierung der Risiko-Ermittlung erfolgt durch Antippen des Buttons „Risikoermittlung aktivieren“. 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. Wenn der CWA-Nutzer das ENF aktiviert, ist auch die Risiko-Ermittlung der CWA App aktiviert.

Nutzer eines iPhones werden vom iOS-Betriebssystem mit einem Systemdialog 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 Mitteilungseinstellungen können in den Einstellungen der CWA App verwaltet werden.

5.4.2.2 Information nach Updates

Wird die CWA App nach einem Update erstmals gestartet, wird der CWA-Nutzer über neue oder geänderte Funktionen einmalig informiert. Diese Information kann innerhalb der CWA App jederzeit erneut im Bereich „App-Informationen“ → „Neue Funktionen“ angezeigt werden.

Nach erstmaligem Start nach dem Update auf eine Version seit 1.5 erhält der CWA-Nutzer zudem einmalig eine Einführung über die mit Version 1.5 eingeführte länderübergreifende Risiko-Ermittlung. Die Informationen erklären die Funktionsweise sowie den Zweck der Interoperabilität. Zudem werden die Länder, die gegenwärtig über eine am EFGS oder CHGS angeschlossene **nationale Corona-App** verfügen, mit ihren Nationalflaggen 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 Risiko-Ermittlung (aktiv/inaktiv), der für den CWA-Nutzer ermittelte **Risikostatus** (z. B. „niedriges Risiko“), aktuelle Statistiken sowie die weiteren Funktionen angezeigt. Über das Menüband am unteren Rand sind die für den alltäglichen Gebrauch konzipierten Funktionen (Kontakt-Tagebuch, QR-Code-Scanner, Check-in und Zertifikats-Wallet) erreichbar.

5.4.4 Risiko-Ermittlung

Auf diesem Bildschirm wird die Funktionsweise der länderübergreifenden Risiko-Ermittlung erläutert und unter dem Unterpunkt „Länderübergreifende Risiko-Ermittlung“ die Liste der gegenwärtig teilnehmenden Länder angezeigt. Über einen Schalter kann die länderübergreifende Risiko-Ermittlung aktiviert bzw. deaktiviert werden.

Im Falle einer Störung der Risiko-Ermittlung (z. B. weil die **Bluetooth**-Schnittstelle des Smartphones deaktiviert ist) wird ein Störungshinweis angezeigt und eine mögliche Lösung vorgeschlagen.

5.4.5 Risikodetails

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 Risikostatus an. Zudem wird erklärt, wie und

wann der Risikostatus ermittelt wurde, etwa durch Anzeige der Anzahl der Risiko-Begegnungen und des Zeitpunkts der letzten Aktualisierung des Risikostatus.

Der Risikostatus wird einer der folgenden Stufen zugeordnet:

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

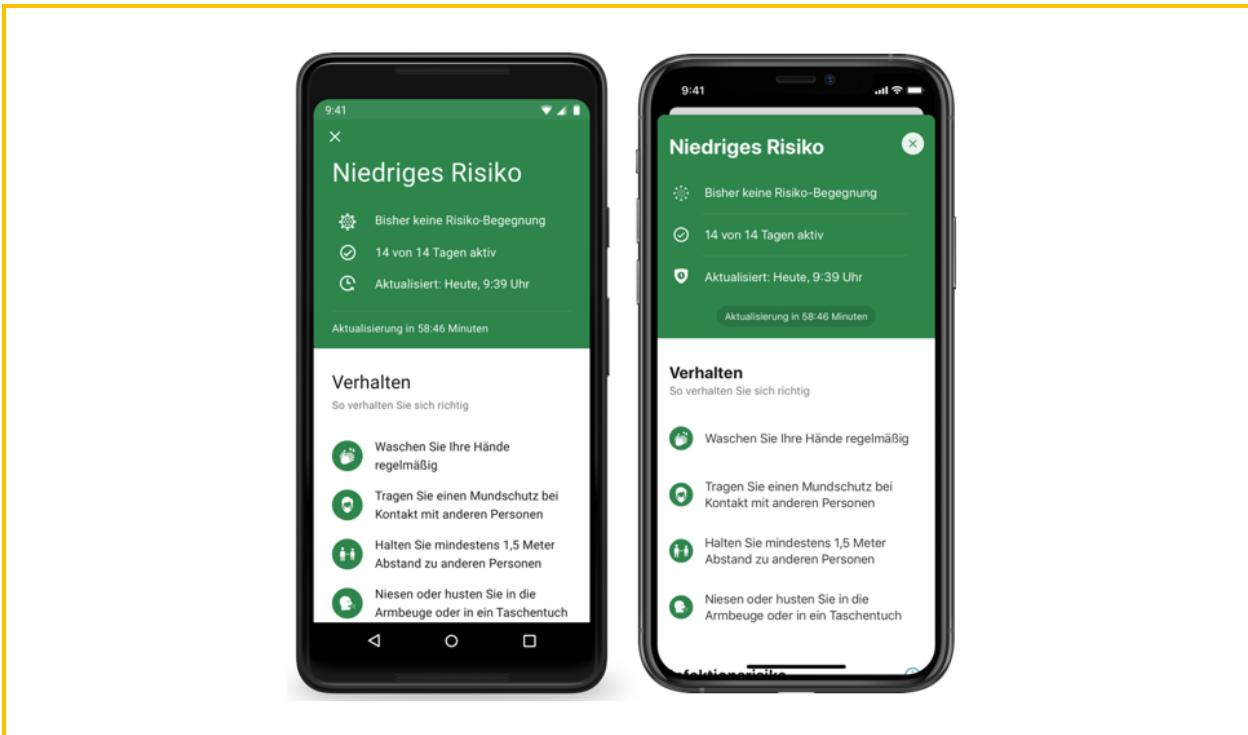


Abbildung 02: Anzeige der Risikodetails bei "niedrigem Risiko" (links Android, rechts iOS)

Im Fall eines niedrigen Risikos ist der Risikostatus mit der Signalfarbe Grün und im Fall eines erhöhten Risikos mit der Signalfarbe Rot hinterlegt.

5.4.6 Statistik-Kacheln

Auf dem Home-Screen werden tagesaktuelle Statistiken des RKI zum Pandemiegeschehen (z. B. Inzidenzzahlen) sowie Kennzahlen zur CWA angezeigt, etwa die Anzahl der über die CWA App ausgelösten Warnungen. Die Statistiken zur 7-Tage-Inzidenz können auch auf regionaler Ebene angezeigt werden, wobei der CWA-Nutzer bis zu fünf Regionen (auf Bundesländer-, Landkreis-/Bezirksebene) auswählen kann.

5.4.7 Kontakt-Tagebuch / Begegnungshistorie

Das Kontakt-Tagebuch ermöglicht die Erfassung von Personen und Orten, die der CWA-Nutzer in den letzten zwei Wochen aufgesucht hat. Das Kontakt-Tagebuch dient damit als Gedächtnissstütze und ermöglicht im Falle eines positiven Corona-Tests, dem zuständigen

Gesundheitsamt im Rahmen der Kontaktpersonennachverfolgung genauere und verlässlichere Angaben zur Ermittlung von Neuinfektionen mitzuteilen oder eigene Maßnahmen zur Unterbrechung von potenziellen Infektionsketten zu ergreifen (z. B. kurzfristige Benachrichtigung von Kontaktpersonen, die dem CWA-Nutzers persönlich bekannt sind).

Es können im Kontakt-Tagebuch auch Informationen zu Personen hinterlegt werden, die die CWA App nicht nutzen. Die gespeicherten Daten werden lokal gespeichert. CWA-Nutzer können die Einträge mittels einer Export-Funktion im Textformat exportieren. Da die CWA App keine Schnittstellen zu anderen Apps für die Datenübernahme hat und auch keine sonstige Import-Funktion bietet, müssen alle Kontaktpersonen und Begegnungsorte innerhalb des Kontakt-Tagebuchs manuell angelegt werden, auch wenn die Informationen bereits auf dem Smartphone des CWA-Nutzers gespeichert sind (z. B. in Form eines Adressbucheintrags).

CWA-Nutzer werden beim erstmaligen Öffnen der Kontakt-Tagebuch-Funktion im Rahmen eines Informationstextes auf die Funktionsweise, die Freiwilligkeit der Nutzung, die automatisierten Löschungen sowie darauf hingewiesen, es zu respektieren, wenn jemand nicht im Kontakt-Tagebuch erfasst werden möchte.

Durch Antippen eines Tageseintrags können CWA-Nutzer Orte und Personen zu den jeweiligen Tageseinträgen im Kontakt-Tagebuch abspeichern, editieren und wieder löschen.

Die Tageseinträge werden um die Angabe ergänzt, ob an dem betreffenden Tag eine Risikobegegnung oder eine Begegnung mit niedrigem Risiko ermittelt worden ist (Begegnungshistorie). Im Zusammenhang mit der Kalenderdarstellung und den dort erfassten Kontakt-Tagebuch-Einträgen (Besuch bestimmter Orte, Begegnungen mit bestimmten Personen) wird den CWA-Nutzern auf diese Weise ein Anreiz gegeben, um eigene Verhaltensweisen im Hinblick auf Infektionsrisiken zu hinterfragen und ggf. gebotene Vorsorgemaßnahmen (z. B. Vermeiden bestimmter Orte) zu ergreifen. Zudem erfahren CWA-Nutzer auf diese Weise, an welchen Tagen weitere Begegnungen mit niedrigem Risiko ermittelt worden sind. Im Zusammenhang mit der Kontaktnachverfolgung können Mitarbeiterinnen und Mitarbeiter des Gesundheitsamtes gezielt auf die Ereignisse im Zusammenhang mit festgestellten Risikobegegnungen und das Aufeinandertreffen mit mehreren Personen oder den Besuch bestimmter Orte eingehen und die Identifikation von Kontaktpersonen potenziell beschleunigen.

Beim erstmaligen Öffnen des Kontakt-Tagebuchs wird ein Informationsscreen mit Erläuterungen zur Begegnungshistorie angezeigt. Dieser Informationsscreen kann im Kontakt-Tagebuch jederzeit wieder über das Kontextmenü geöffnet werden. Auch der Einleitungstext im Kopfteil des Kontakt-Tagebuchs enthält einen deutlichen Hinweis auf den Zweck und Nutzen der Begegnungshistorie. Sofern für einen Tag eine Risikobegegnung oder eine Begegnung mit niedrigem Risiko festgestellt wurde, wird der ausdrückliche Hinweis bei dem jeweiligen Eintrag eingeblendet, dass der Risikostatus nicht in direktem Zusammenhang mit den erfassten Personen oder Orten im Kontakt-Tagebuch stehen muss. Mittels der deutlichen Hinweise wird dem Risiko vorgebeugt, dass die Darstellung der Begegnungshistorie zu Missverständnissen führt (im Sinne einer falschen Verdächtigung einer im Kontakt-Tagebuch eingetragenen Begegnung als Risikoquelle).

In der Datenschutzerklärung wird dieser Hinweis ebenfalls erteilt. Dort wird zudem auf das im Einzelfall bestehende De-Pseudonymisierungsrisiko im Zusammenhang mit der Darstellung der Begegnungshistorie im Kontakt-Tagebuch hingewiesen.¹⁷

5.4.8 Testregistrierung

Corona-Tests (PCR-Tests und Antigen-Schnelltests) können in der CWA App „registriert“ werden, um den digitalen Testinformationsprozess zu starten. Dies ermöglicht die Anzeige des Status des Tests bzw. des Testergebnisses in der CWA App. Es können eigene und Corona-Tests von anderen Personen registriert werden.

Bei einem positiven eigenen Testergebnis kann der CWA-Nutzer eine Warnung auslösen. Wenn es sich um das positive Testergebnisses einer anderen Person handelt, ist dies nicht möglich. Für den Fall eines abgerufenen eigenen oder eines negativen Testergebnisses einer anderen Person kann über die CWA App ein Testzertifikat angefordert werden, sofern die Teststelle an den Zertifikatsservice angeschlossen ist (siehe Abschnitt 5.4.14.2).

Ist das **Labor** oder die Teststelle an die Systeme zum Testergebnisabruf angeschlossen, wird die getestete Person bei der Durchführung des Tests vor Ort gefragt, ob sie ihr Testergebnis über die CWA App erhalten möchte und ob sie mit einer entsprechenden Übermittlung des Testergebnisses an die dafür vorgesehene Serverinfrastruktur der CWA (Test Result Server) einverstanden ist.

Bei PCR-Tests wird die Einwilligung zur Übermittlung an den CWA Test Result Server auf dem Proben-Formular notiert und der getesteten Person in einem Begleitdokument (Probenbegleitschein) der **QR-Code** bereitgestellt, der zur Testregistrierung in der CWA App benötigt wird. Mittels des QR-Codes, der eine eindeutige Test-spezifische Kennzahl (**GUID**) enthält, kann die Zuordnung der Proben sowie der Testergebnisse erfolgen.

Die Testregistrierung erfolgt durch Scannen des QR-Codes in der CWA App. Die CWA App liest dann die GUID aus dem QR-Code aus und generiert einen Hash, der zur Abfrage des Testergebnisses genutzt wird. Im Fall eines PCR-Tests wird ein zweiter Hash aus der GUID und zusätzlich dem Geburtsdatum der getesteten Person generiert (siehe hierzu Abschnitt 5.6.3).

Bei Schnelltests wird die Einwilligung von der Teststelle im Teststellen-System (PoC-Backend) erfasst. Zusätzlich sind die Teststellen angewiesen, die getestete Person auf die Möglichkeit der namentlichen Anzeige des negativen Schnelltest-Ergebnisses in der CWA App hinzuweisen. Wenn sie dies wünscht und darin einwilligt, wird diese Einwilligung im Teststellen-System erfasst. Die Teststelle erzeugt dann im Teststellen-System einen individuellen QR-Code oder Link, den die getestete Person mit der CWA App scannen kann.

¹⁷ Dieses Risiko besteht dann, wenn eine Warnung ausgelöst wird, die eine Person im persönlichen Umfeld erreicht und diese an dem fraglichen Tag keinerlei weitere Kontakte hatte und diese Informationen gemeinsam im Kontakt-Tagebuch dargestellt werden. Die Bewertung dieses Risikos ist Gegenstand der Risikoanalyse.

Der QR-Code enthält in kodierter Form die GUID sowie den Testzeitpunkt des Schnelltests. Sofern die getestete Person die namentliche Anzeige des Schnelltest-Ergebnisses gewählt hat, enthält der QR-Code auch den Namen sowie das Geburtsdatum in kodierter Form, damit die CWA App diese von dort auslesen und im Fall eines negativen Testergebnisses anzeigen kann.

Nach dem Scannen des QR-Codes muss der CWA-Nutzer zunächst auswählen, ob er den Test für sich oder ein Familienmitglied registriert. Sollte es sich um den Test eines Familienmitglieds handeln, muss der CWA-Nutzer einen (beliebig wählbaren) Namen eingeben, unter dem der Test von der CWA App (lokal auf dem Smartphone) verwaltet wird.

Sollte es sich um einen eigenen Test des CWA-Nutzers handeln, wird er für den Fall eines positiven Testergebnisses vorab um seine Einwilligung in die Übermittlung seiner freigegebenen Tagesschlüssel der letzten 14 Tage und etwaiger optionaler Angaben zum Symptombeginn an den CWA Server durch Tippen auf den Button „Einverstanden“ gebeten, so dass andere Nutzer vor einer möglichen Ansteckung länderübergreifend (im Fall eines positiven PCR-Testergebnisses) bzw. deutschlandweit¹⁸ (im Fall eines positiven Schnelltest-Ergebnisses) gewarnt werden können. In diesem Zusammenhang wird dem CWA-Nutzer nochmals die Funktionsweise der länderübergreifenden Warnung erläutert und die Liste der teilnehmenden Länder angezeigt, wie dies bereits auf dem Bildschirm „Risiko-Ermittlung“ geschehen ist. Nach Antippen des Buttons „Einverstanden“ wird der CWA-Nutzer über den Systemdialog des Betriebssystems aufgefordert, die Freigabe zur lokalen Weitergabe seiner Tagesschlüssel durch das ENF an die CWA App zu erteilen („Andere über positiven Test informieren?“). Diese Freigabe („Einmal erlauben“) hat eine Gültigkeit von fünf Tagen, sie kann während dieses Zeitraums über die Systemeinstellungen des Betriebssystems für das ENF zurückgenommen werden. Sobald sein eigenes Testergebnis bereitsteht, wird der CWA-Nutzer auf seine zuvor erteilte Einwilligung zur Warnung anderer Nutzer hingewiesen, so dass er seine Entscheidung überdenken und seine Einwilligung bei Bedarf widerrufen kann. Erfolgt der Abruf des Testergebnisses innerhalb von fünf Tagen nach der Freigabe der Tagesschlüssel, wird der Systemdialog nicht erneut angezeigt. Im Fall eines positiven Testergebnisses werden die Tagesschlüssel dann vom ENF automatisch an die CWA App übergeben. Erfolgt der Testergebnisabruf erst zu einem späteren Zeitpunkt, d. h. die technische Freigabe der Tagesschlüssel liegt länger als fünf Tage zurück, wird der Systemdialog erneut angezeigt.

Liegen sowohl die Einwilligung als auch die technische Freigabe vor, hat der CWA-Nutzer vor dem Anzeigen seines eigenen Testergebnisses im Screen „Check-ins teilen“ die Möglichkeit die Events und Orte auszuwählen, bei denen er in den letzten 14 Tagen eingekennzeichnet war und die in seine Warnung aufgenommen werden sollen. Die zeitgleich an diesen Events und Orten eingekennzeichneten CWA-Nutzer werden dann ggf. über eine mögliche Risiko-Begegnung gewarnt. Der CWA-Nutzer kann alle oder auch nur einzelne Check-ins hinzufügen. Die Check-ins sind

¹⁸ „Deutschlandweit“ ist nicht geographisch zu verstehen, sondern meint, dass bei einer Warnung aufgrund eines positiven Schnelltest-Ergebnisses keine Weitergabe der Tagesschlüssel an den EFGS und CHGS erfolgt. Es werden somit nur diejenigen Kontakte des CWA-Nutzers gewarnt, die ebenfalls die CWA App nutzen.

nicht vorausgewählt. Der CWA-Nutzer kann sich auch dafür entscheiden, keinen Check-in auszuwählen.

Unabhängig davon, ob der CWA-Nutzer die Einwilligung, die technische Freigabe der Tagesschlüssel erteilt und Check-ins ausgewählt hat, wird das Testergebnis abschließend angezeigt.

Der Prozess zum Abruf eines Testergebnisses erfolgt über eine zyklische Abfrage von Statusänderungen durch die CWA App, die sich auf das Vorliegen des Testergebnisses eines zuvor registrierten Corona-Tests beziehen. Sofern das Testergebnis vorliegt, wird dieses gelesen und auf dem Home-Bildschirm der CWA App angezeigt. Wenn ein Corona-Test eines Familienmitglieds registriert worden ist, wird auf dem Home-Bildschirm der Bereich „Tests von Familienmitgliedern“ angezeigt, über den die Corona-Tests der Familienmitglieder sowie deren Testergebnisse verwaltet und eingesehen werden können.

Über die lokale Mitteilungsfunktion des Betriebssystems wird der CWA-Nutzer über das Vorliegen eines neuen Testergebnisses in der CWA App informiert. Voraussetzung ist, dass die CWA App zum Versand von Push-Mitteilungen berechtigt ist (siehe unter Ziffer 5.4.15.3). Die Push-Mitteilung selbst enthält keine Information über das konkrete Ergebnis des Tests, sondern weist lediglich auf den geänderten Status, also auf das Vorliegen eines Testergebnisses hin. Erst nach dem Öffnen der CWA App wird dem CWA-Nutzer das Testergebnis innerhalb der CWA App angezeigt.

5.4.9 Namentlicher Schnelltest-Nachweis

Falls die getestete Person, deren Schnelltest in der CWA App registriert worden ist, gegenüber der Teststelle in die namentliche Anzeige seines Schnelltest-Ergebnisses eingewilligt hat, kann sie sich – sofern das Ergebnis des Schnelltests negativ ist – eine Detailansicht der Ergebnisanzeige anzeigen lassen. In der Detailansicht wird das (negative) Testergebnis zusammen mit dem gegenüber der Teststelle angegebenen Vor- und Nachnamen und Geburtsdatum sowie dem Zeitpunkt, an dem das Schnelltestergebnis übermittelt wurde, angezeigt. In der Detailansicht finden sich zudem Hinweise zur sachgerechten Verwendung der Detailansicht als Schnelltest-Nachweis. Der namentliche Testnachweis wird erst in der CWA App zusammengestellt und anschließend angezeigt. Es wird weiterhin lediglich das Testergebnis am Server abgefragt (siehe unter Ziffer 5.4.8). Der angezeigte Name und das Geburtsdatum der getesteten Person werden bei der Testregistrierung aus dem QR-Code ausgelesen und in der CWA App gespeichert.

5.4.10 Verifikations-Hotline

Die Verifikations-Hotline ermöglicht nach Erhalt eines positiven PCR-Tests¹⁹ das Auslösen einer Warnung ohne vorherigen Testergebnisabruf durch die CWA App, etwa weil das Labor oder die testende ärztliche Praxis nicht an die Systeme zur Bereitstellung der Testergebnisse angeschlossen sind, der QR-Code aufgrund von Beschädigungen nicht lesbar ist oder kein QR-Code ausgegeben wurde.

In diesem Fall kann sich der CWA-Nutzer an die **Hotline** (Verifikations-Hotline) wenden. Gemäß einem abgestimmten Skript stellt der Mitarbeiter der Hotline dann zunächst Plausibilitätsfragen, 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 einstuft, 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 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.

5.4.11 Erinnerung an das Warnen

Wenn ein CWA-Nutzer innerhalb von vier Stunden nach dem Abruf eines eigenen positiven Testergebnisses in der CWA App keine Warnung auslöst, wird er von der CWA App erstmals nach zwei Stunden und ein zweites Mal nach vier Stunden mit einer lokalen Push-Mitteilung an das Teilen seines Testergebnisses erinnert (Erinnerungsfunktion). Voraussetzung ist, dass die CWA App zum Versand von Mitteilungen berechtigt ist (siehe unter Ziffer 5.4.15.3). Die Erinnerungs-Mitteilung lautet „Helfen Sie mit! Bitte warnen Sie andere und teilen Sie Ihr Testergebnis.“

¹⁹ Die Verifikations-Hotline steht nicht für Ergebnisse von (positiven) Antigen-Schnelltests zur Verfügung.

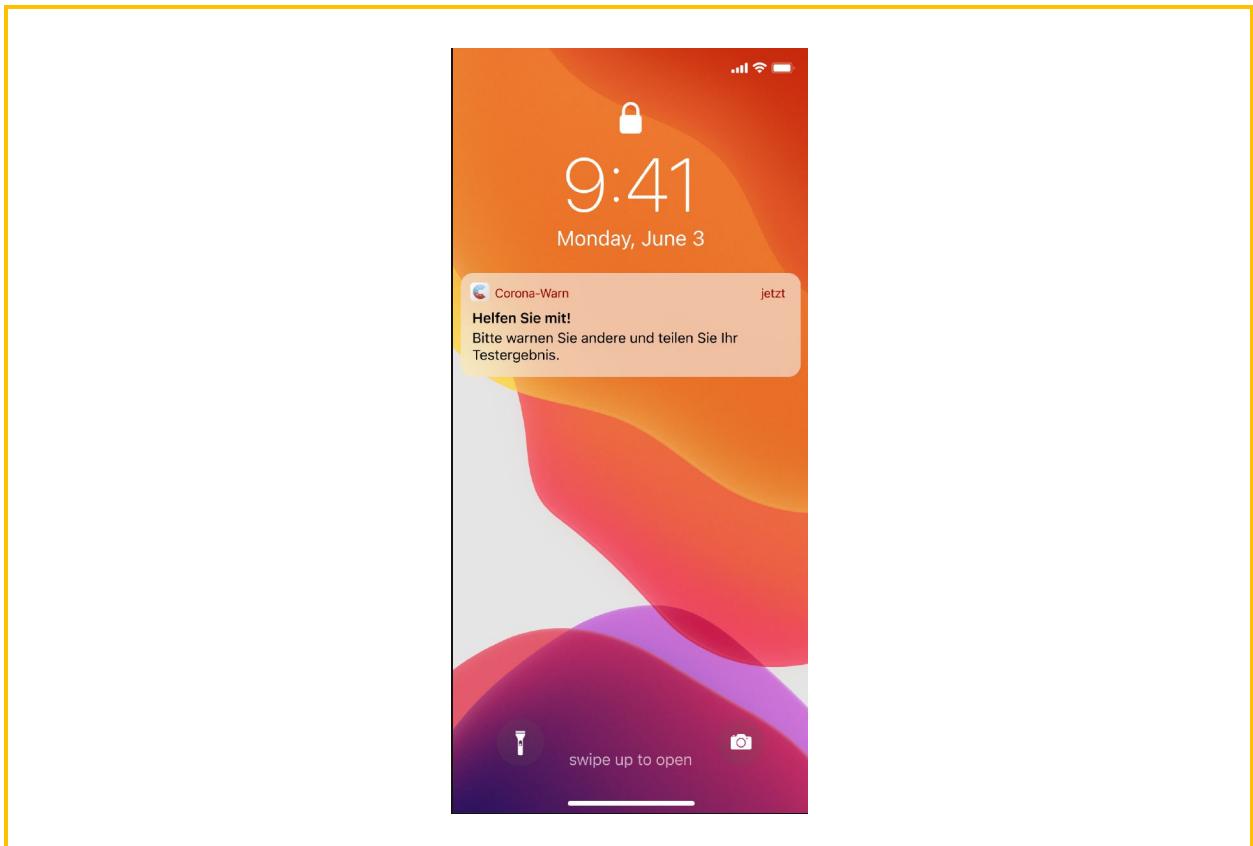


Abbildung 03: Erinnerungs-Mitteilung auf dem Sperrbildschirm (Beispiel-Screenshot iOS)

5.4.12 Auslösen einer Warnung

Bei einem positiven eigenen Testergebnis kann der CWA-Nutzer mit der Warnfunktion sein Testergebnis mit Kontaktpersonen teilen und somit vor einer möglichen Ansteckung warnen, sofern die Kontaktpersonen Nutzer der CWA App oder einer anderen nationalen Corona-App sind.²⁰ Die Warnung kann nur ausgelöst werden, wenn der CWA-Nutzer seine Einwilligung erteilt hat. Auf Grundlage eines in der CWA App erhaltenen positiven Testergebnisses eines Familienmitglieds kann sachgerechter Weise keine Warnung ausgelöst werden.

Vor dem finalen Absenden der Warnung kann der CWA-Nutzer optionale Angaben zum Symptombeginn machen. Nach der Verifikation des Testergebnisses kann der CWA-Nutzer entweder 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

²⁰ Im Falle von positiven Schnelltests werden nur CWA-Nutzer gewarnt. Kontaktpersonen können auch Personen sein, die zeitgleich mit dem positiv getesteten CWA-Nutzer das gleiche Event oder den gleichen Ort besucht haben und dort über die Funktion Event-Registrierung der CWA eingecheckt waren (siehe Abschnitt 5.6.7).

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.

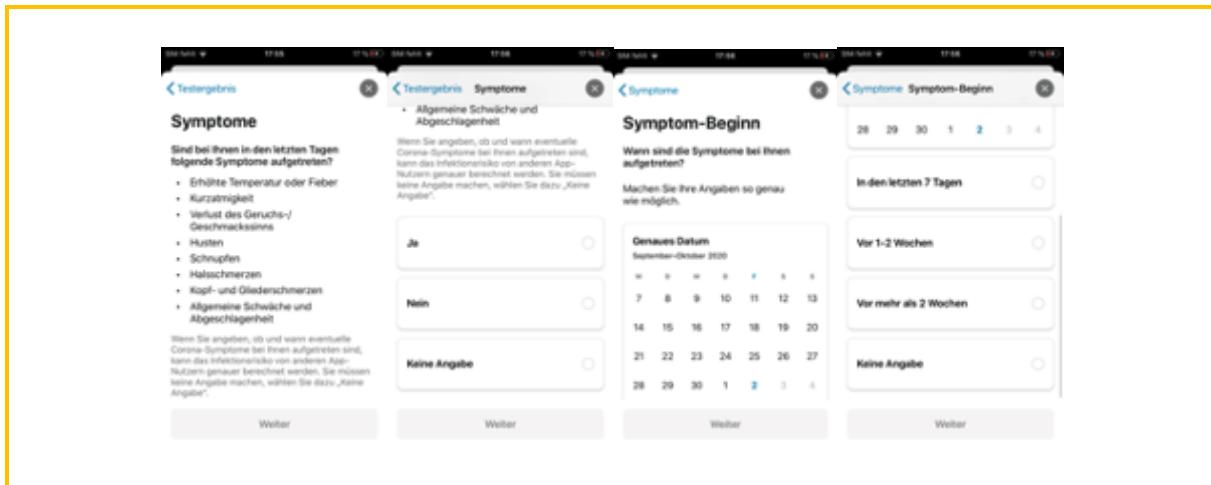


Abbildung 04: Abfrage zum Symptombeginn (Beispiel-Screenshot iOS)

Sofern der CWA-Nutzer im Rahmen der Testregistrierung keine Einwilligung erteilt hat bzw. die Einwilligung vor mehr als fünf Tagen erteilt worden ist, kann der gesamte Nutzerdialog der Warnfunktion jederzeit vom CWA-Nutzer abgebrochen werden. Zuletzt kann der Prozess durch die Verweigerung der Freigabe der Tagesschlüssel im Systemdialog des Betriebssystems abgebrochen werden.

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

5.4.13 Event-Registrierung

Mit der Event-Registrierung kann der CWA-Nutzer von anderen CWA-Nutzern vor einem möglichen Infektionsrisiko infolge des Besuchs einer Veranstaltung oder eines Ortes (Event) gewarnt werden. Umgekehrt kann der CWA-Nutzer im Fall eines positiven Testergebnisses nach dem Besuch eines Events andere CWA-Nutzer, die das gleiche Event besucht haben, warnen.

Die Event-Registrierung verwendet – anders als die Risiko-Ermittlungsfunktion – nicht das ENF zur automatischen Identifikation von Infektionsrisiken im Hintergrund, sondern setzt ein aktives Handeln des CWA-Nutzers, nämlich das Erzeugen und Auslegen bzw. das Einscannen eines QR-Codes voraus. Aus technologischer und Nutzersicht stellt die Event-Registrierung somit eine konzeptionelle Erweiterung der CWA App dar.

5.4.13.1 Event anlegen (als Veranstalter)

Um CWA-Nutzern, die zeitgleich ein Event besucht haben, das wechselseitige Erhalten und Auslösen von Warnungen zu ermöglichen, muss der Veranstalter des Events in seiner CWA App einen Event-spezifischen QR-Code herstellen. Die Besucher des Events können diesen QR-Code dann mit ihrer CWA App scannen und sich auf diese Weise bei dem Event „einchecken“.

Der CWA-Nutzer, der das Event anlegen will, findet hierzu die Kachel „Sie planen eine Veranstaltung?“ auf dem Home-Bildschirm vor. Dort kann er für sein geplantes Event einen „QR-Code erstellen“, der von anderen CWA-Nutzern bzw. Event-Besuchern für den Check-in genutzt werden kann.

Beim erstmaligen Anlegen eines Events wird dem CWA-Nutzer neben der Funktionsweise auch der Zweck der Event-Registrierung erläutert und darauf hingewiesen, den QR-Code regelmäßig auszutauschen, um das Risiko für einen Missbrauch des QR-Codes durch Dritte zu reduzieren.

Nach Antippen des Buttons „QR-Code erstellen“ werden dem CWA-Nutzer in einem Formular verschiedene Felder zur Beschreibung des geplanten Events angezeigt, wobei zwischen den Kategorien „Orten“ und „Events“ unterschieden wird.

Nach der Wahl eines „Orts“ oder „Events“ (zusammenfassend nachfolgend nur „Event“) müssen auf dem nächsten Screen genauere Angaben zum Event gemacht werden (Bezeichnung, Ort, Datum, Start- und Endzeitpunkt). Zudem kann der CWA-Nutzer angeben, wie lange Besucher voraussichtlich bzw. üblicherweise beim Event verbleiben werden. Sobald alle Angaben gemacht sind, wird das entsprechende Event in der App angelegt und der zugehörige QR-Code generiert.

Um Gästen das Einchecken durch Einscannen des QR-Codes zu ermöglichen, muss der CWA-Nutzer (als Veranstalter) den QR-Code auf seinem Smartphone in der CWA App vorzeigen oder ausdrucken und auslegen.

Events werden auf dem Screen „Meine QR-Codes“ verwaltet. Der CWA-Nutzer kann einen QR-Code erstellen bzw. ein Event anlegen, ein Event löschen und die QR-Codes zu bereits angelegten Events anzeigen, um anderen CWA-Nutzern das Einchecken durch Scannen des Bildschirms zu ermöglichen. Daneben kann eine „Druckversion“ angezeigt werden, die dann in einem weiteren Schritt über die entsprechende Funktion des Betriebssystems ausgedruckt werden kann.

Der CWA-Nutzer kann auch als Veranstalter bei einem von ihm angelegten Event selbst als regulärer Gast einchecken.

5.4.13.2 Einchecken bei Events (als Guest)

Als Guest eines Events muss der CWA-Nutzer die Funktion „Check-in“ aufrufen, um sich bei dem Event einzuchecken. Dort findet sich eine Übersicht über alle Veranstaltungen, bei denen

er eingekennet war oder ist, sowie den QR-Code-Scanner. Falls der CWA-Nutzer der CWA App noch nicht die Berechtigung für die Kamera erteilt hat, wird er zunächst um die entsprechende Freigabe gebeten.

Eine weitere Möglichkeit zum Einchecken besteht im Scannen des QR-Codes mit der „normalen“ Kamera-App des Smartphones, welche heute in der Regel einen QR-Code-Scanner umfasst. In diesem Fall kann die CWA App nach dem Einlesen der im QR-Code enthaltenen Informationen aus der Foto-App heraus gestartet werden und die ausgelesenen Informationen werden vom Betriebssystem an die CWA App weitergegeben.

Nachdem der CWA-Nutzer den QR-Code eingescannt hat, werden ihm die darin enthaltenen Details zum Event angezeigt, so dass er prüfen kann, ob es sich um das richtige, d. h. das tatsächlich von ihm besuchte Event handelt. Der CWA-Nutzer kann hier auch eine Zeit für automatisches Auschecken einstellen. Zudem kann der CWA-Nutzer wählen, ob das Event nach dem Auschecken in das Kontakt-Tagebuch eingetragen werden soll. Mit Antippen des Buttons „Einchecken“ kann der Eincheckprozess schließlich abgeschlossen werden.

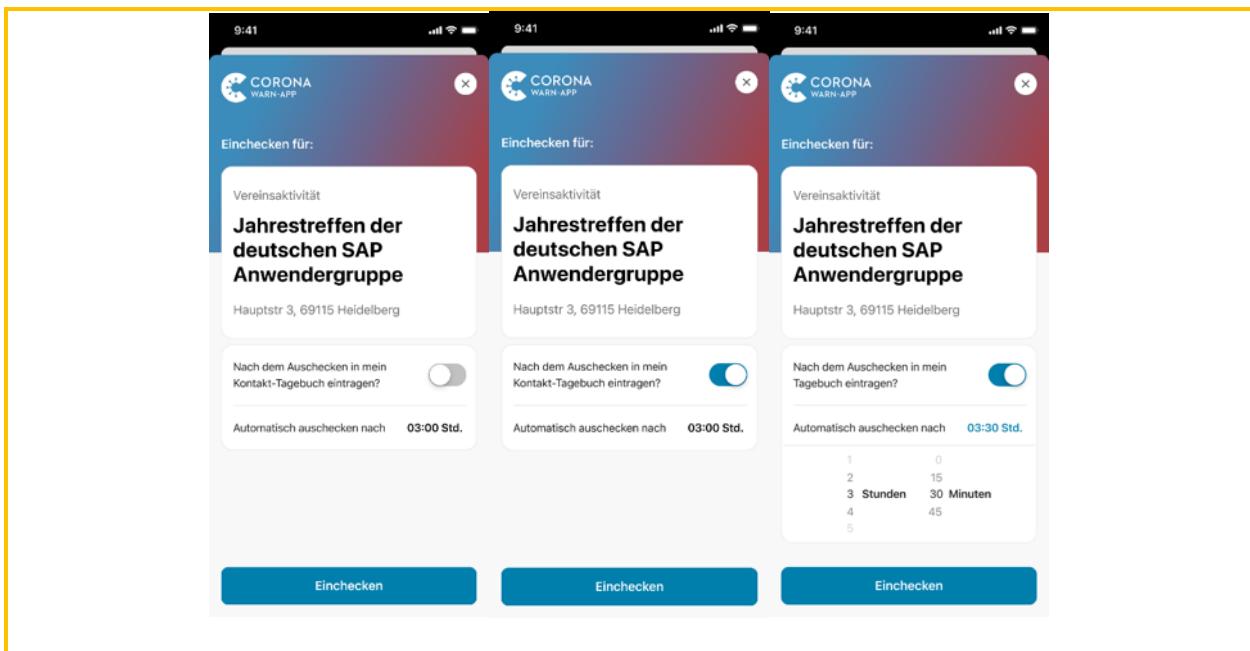


Abbildung 05: Einchecken zu einer Veranstaltung

Ebenso wie die vom CWA-Nutzer angelegten Events werden auch die besuchten Events auf dem Screen „Meine QR-Codes“ verwaltet (z. B. Löschen von gespeicherten Events).

Wenn der CWA-Nutzer ein laufendes eingekennetes Event verlässt, kann er sich über den Button „Jetzt auschecken“ jederzeit manuell auschecken.

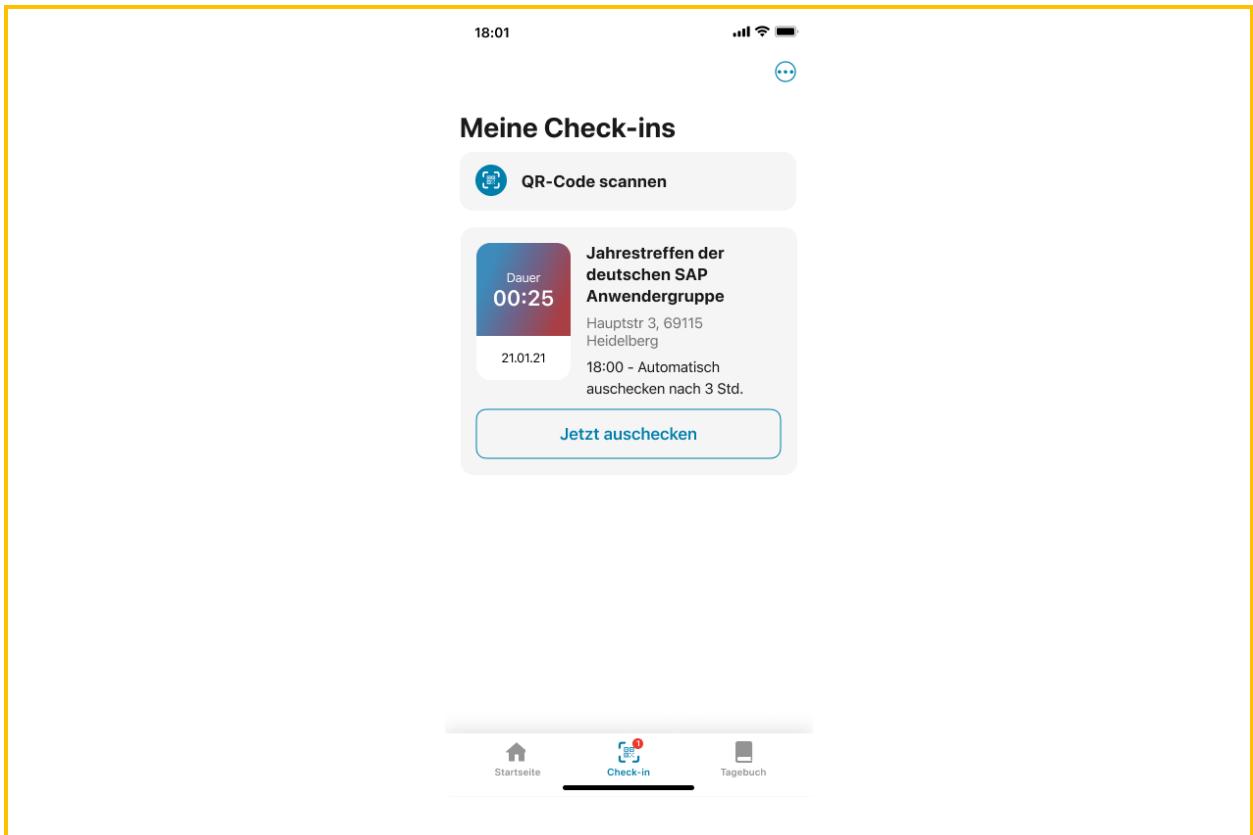


Abbildung 06: Meine Check-ins

5.4.13.3 Übernahme in das Kontakt-Tagebuch

Wenn der CWA-Nutzer beim Einchecken die Übertragung in das Kontakt-Tagebuch aktiviert hat, erfolgt beim Auschecken aus dem Event ein Eintrag im Kontakt-Tagebuch. In der Kontakt-Tagebuch-Historie wird dem CWA-Nutzer dann auch angezeigt, welchem Infektionsrisiko der CWA-Nutzer bei dem Besuch des Events ausgesetzt war.

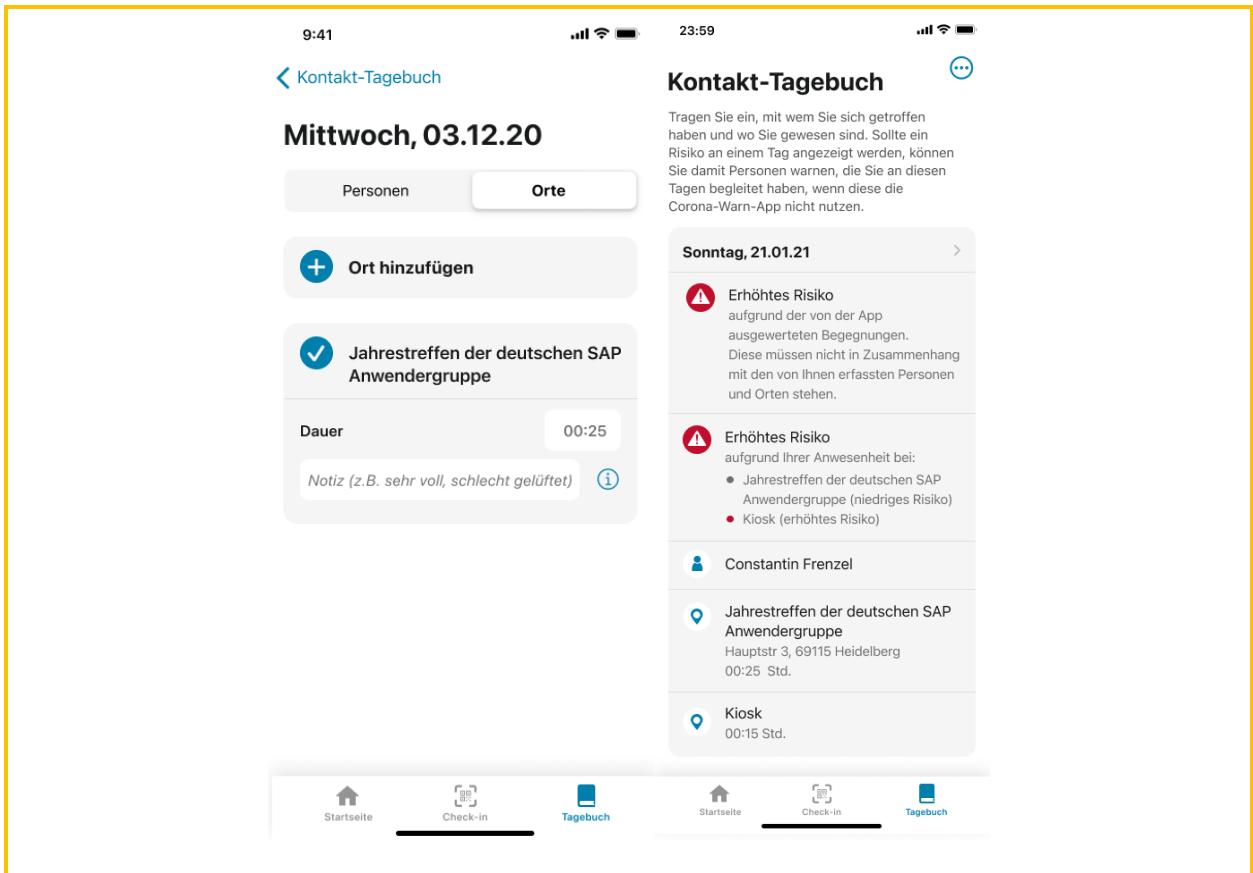


Abbildung 07: Screens Kontakt-Tagebuch

5.4.13.4 In Vertretung warnen

In Situationen, in denen eingekochte CWA-Nutzer (Gäste) nicht von einem positiv getesteten anderen Gast gewarnt werden können, etwa weil der betreffende Guest nicht eingekochte war oder kein CWA-Nutzer ist, kann eine Warnung „stellvertretend“ für den positiv getesteten Guest durch das Gesundheitsamt (Option 1) oder den Veranstalter (Option 2) ausgelöst werden. Hierfür benötigt der vertretend Warnende eine sogenannte PIW-TAN (Public Health Authority Initiated Warning TAN), die analog der teleTAN generiert wird.

Die Funktion „In Vertretung warnen“ richtet sich ausschließlich an Veranstalter. Veranstalter, die ein Event angelegt haben, können die Funktion nutzen, um „in Vertretung“ eines später positiv getesteten Gastes eine Warnung auszulösen und somit ihre Gäste vor potenziellen Gesundheitsrisiken zu schützen. Die stellvertretende Warnung kann nur ausgelöst werden, nachdem der Veranstalter von einem Gesundheitsamt kontaktiert und ihm von diesem die PIW-TAN und ggf. der Aufenthaltszeitraum des positiv getesteten Gastes auf dem Event (Beginn/Ankunft und Ende) mitgeteilt wurde. Alternativ kann das Gesundheitsamt auch selbst die Warnung auslösen, sofern dem Gesundheitsamt der QR-Code des Events bekannt ist.

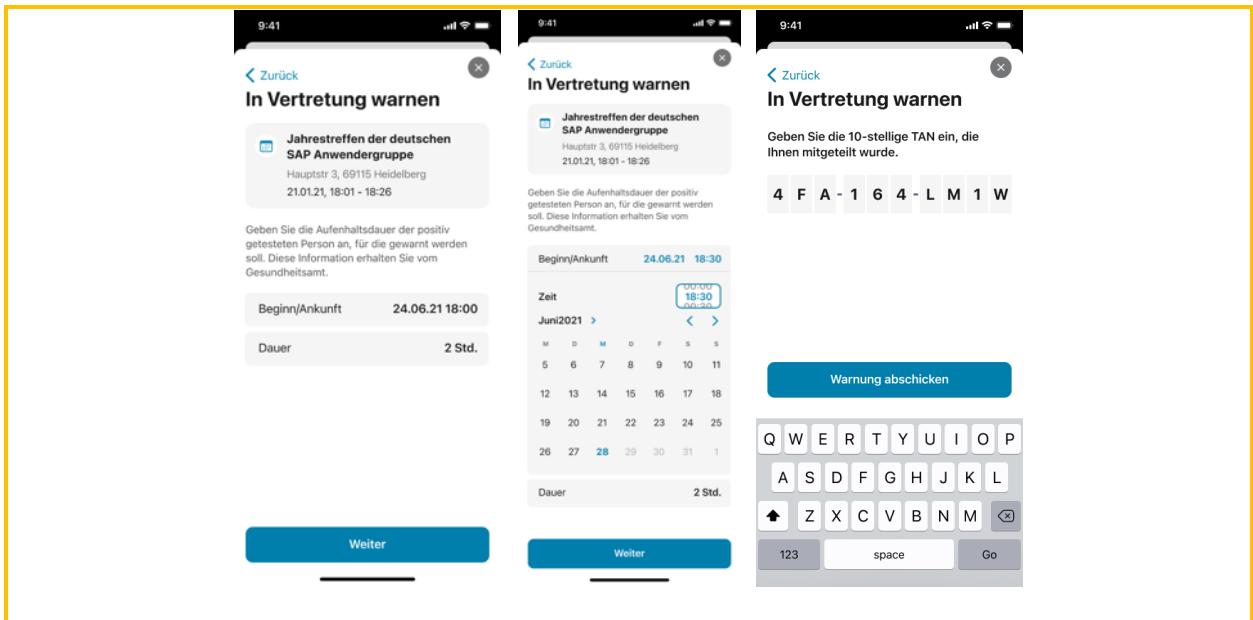


Abbildung 08: Screens „In Vertretung warnen“

5.4.14 Zertifikats-Wallet

Die CWA App ermöglicht die elektronische Nutzung der zum 01.06.2021 mit dem novellierten § 22a IfSG²¹ eingeführten COVID-Zertifikate und kann dadurch als vollwertige Wallet-App für alle in Deutschland gesetzlich anerkannten COVID-Zertifikatskategorien dienen.²² Zu den Wallet-Funktionen gelangt der CWA-Nutzer über die Menüleiste durch Antippen des Menüpunkts „Zertifikate“.

Ein COVID-Zertifikat enthält einen QR-Code, der in maschinenlesbarer Form die Angaben zum Impf-/Geneseneten-/Teststatus (Zertifikatsaussage, siehe Abschnitt 5.7.23) sowie den Namen und das Geburtsdatum des Zertifikatsinhabers enthält. Der CWA-Nutzer kann ein COVID-Zertifikat in Papierform sowie in elektronischer Form mit einer Wallet-App verwenden. Die offiziellen Wallet-Apps der Bundesrepublik Deutschland für COVID-Zertifikate sind die CWA App und die ebenfalls vom RKI herausgegebene CovPass-App.

²¹ § 22 IfSG in der Fassung des Artikels 1 des Zweiten Gesetzes zur Änderung des Infektionsschutzgesetzes und weiterer Gesetze vom 28.05.2021 (BGBl. I S. 1174); (jetzt § 22a IfSG).

²² Hinweis zum Prüfgegenstand: Die Datenverarbeitung im Zusammenhang mit der Ausstellung und Prüfung von COVID-Zertifikaten ist nicht vom Prüfgegenstand dieser DSFA umfasst, da sie technisch und organisatorisch unabhängig von der CWA erfolgt. Gegenstand der vorliegenden DSFA sind ausschließlich die Verarbeitungstätigkeiten in Bezug auf die von einem CWA-Nutzer mit der CWA App gespeicherten COVID-Zertifikate.

5.4.14.1 Verwalten von COVID-Zertifikaten

Um ein COVID-Zertifikat elektronisch mit der CWA App zu nutzen, muss der QR-Code des COVID-Zertifikats mit dem QR-Code-Scanner der CWA App gescannt werden. Nach dem Auslesen des QR-Codes wird das von ihm repräsentierte COVID-Zertifikat sofort in elektronischer Form in der Wallet der CWA App hinterlegt.

In der Übersichtsdarstellung wird jedes COVID-Zertifikat durch eine Kachel repräsentiert, die lediglich den Namen des Zertifikatsinhabers und den QR-Code des COVID-Zertifikats angezeigt. Die Zertifikatskategorie (z.B. Impf- oder Genesenenzertifikat) wird in dieser neutralen Ansicht nicht angezeigt. Der Titel beschreibt nur die Kategorie „Digitales COVID-Zertifikat der EU“. Sofern das COVID-Zertifikat zum Nachweis von bestimmten Statuskriterien wie 2G oder 2G+ verwendet werden kann, wird zudem ein entsprechender „Status-Nachweis“ über dem QR-Code angezeigt.

Durch Antippen einer Kachel gelangt der CWA-Nutzer zur Detailansicht des betreffenden COVID-Zertifikats. Die Detailansicht zeigt gesamte Zertifikatsaussage im Klartext. Bei Impfzertifikaten wird zusätzlich angezeigt, ob der Impfschutz vollständig ist und wie viele Tage seit der Impfung vergangen sind. Zudem können hier die Zertifikats-spezifischen Funktionen (Druckversion anzeigen, Gültigkeitsprüfung) aufgerufen und das COVID-Zertifikat entfernt werden.

Die Übersichtsdarstellung und die Detailansichten enthalten jeweils einen leicht erkennbaren Hinweis darauf, dass eine verlässliche Überprüfung der Zertifikate mit der CovPassCheck-App möglich ist. Damit sollen CWA-Nutzer dafür sensibilisiert werden, in Überprüfungssituationen auf den sachgerechten Umgang der Prüfperson mit ihrem COVID-Zertifikat zu achten und somit beispielsweise eine „Prüfung“ durch Abfotografieren oder Einlesen des COVID-Zertifikats in die eigene Wallet-App der Prüfperson zu vermeiden.

Wenn ein COVID-Zertifikat ungültig bzw. widerrufen worden ist oder ein Impfzertifikat noch keinen vollständigen Impfschutz nachweist, wird die Detailansicht des betreffenden COVID-Zertifikats grau hinterlegt und auf die Ungültigkeit bzw. den „unvollständigen Impfschutz“ hingewiesen. Ebenso wird bei Statusänderungen aufgrund geänderter gesetzlicher Vorgaben in den Ländern hingewiesen. Bei Impfzertifikaten fällt der Hinweis auf den unvollständigen Impfschutz weg, nachdem das letzte (bzw. im Fall einer Einmalimpfung: das einzige) Impfzertifikat der Impfserie gescannt worden ist und 14 Tage seit dem im QR-Code genannten Impftermin vergangen sind, da ab diesem Zeitpunkt von einem vollständigen bzw. ausreichenden Impfschutz ausgegangen wird (§ 2 Nr. 3 lit. a der COVID-19-Schutzmaßnahmen-Ausnahmenverordnung). Bei Impfzertifikaten zu Impfungen von Genesenen, die aus einer einzigen Impfdosis bestehen („Genesenenzimpfung“), wird gemäß

§ 2 Nr. 3 lit. b der COVID-19-Schutzmaßnahmen-Ausnahmenverordnung sofort der vollständige Impfschutz angezeigt.²³

Die Entfernung eines COVID-Zertifikats aus der Zertifikatsübersicht führt nicht zur sofortigen Löschung des COVID-Zertifikats. Stattdessen wird das entfernte COVID-Zertifikat zunächst in den „Papierkorb“ der CWA App verschoben. Von dort kann es zunächst durch den CWA-Nutzer wieder hergestellt werden. Die endgültige Löschung der COVID-Zertifikate im Papierkorb erfolgt automatisch nach 30 Tagen, sofern nicht zuvor eine manuelle Löschung angestoßen wird. Der Papierkorb kann auf dem Home-Bildschirm aufgerufen werden und zeigt das Löschdatum der darin enthaltenen COVID-Zertifikate an. Nach der endgültigen Löschung ist das COVID-Zertifikat unwiederbringlich aus dem App-Speicher gelöscht. Zur erneuten Aufnahme in die CWA App muss es neu eingelesen werden.

Neben eigenen COVID-Zertifikaten kann der CWA-Nutzer auch Familienzertifikate in der CWA App speichern. Als Familienzertifikate werden reguläre COVID-Zertifikate von Angehörigen des CWA-Nutzers (beispielsweise Kinder oder Ehe-/Lebenspartner) bezeichnet, die – zusätzlich zu den eigenen COVID-Zertifikaten des CWA-Nutzers – ebenfalls in der CWA App nach den verschiedenen Zertifikatsinhabern gruppiert gespeichert und angezeigt werden können. Durch Aktivierung eines Schiebereglers in der Detailansicht der COVID-Zertifikate unter seinem Namen kann der CWA-Nutzer der CWA App signalisieren, dass er der Besitzer bzw. Hauptnutzer der CWA App ist, so dass seine eigenen COVID-Zertifikate zuerst in der Liste erscheinen.

Zur leichteren Übersicht werden die COVID-Zertifikate nach Zertifikatsinhabern gegliedert angezeigt. Um kleinere Abweichungen bei der Schreibweise des Namens des Zertifikatsinhabers auszugleichen, ist die Zuordnungsfunktion der CWA App mit einer Fehlertoleranz ausgestattet. Mehrere COVID-Zertifikate werden daher auch dann der gleichen Person zugeordnet, wenn die Namen in den Zertifikatsaussagen nicht exakt übereinstimmen.

5.4.14.2 Testzertifikate zu registrierten Tests

Bis Release 2.5 konnten mit der CWA App nur Testzertifikate zu Tests gespeichert werden, die zuvor in der CWA App registriert worden sind (siehe Abschnitt 5.4.8), d. h. es war nicht möglich, Testzertifikate, die nur im Papierformat (mit QR-Code) vorliegen, nachträglich in der CWA App zu speichern und damit in das elektronische Format zu überführen. Diese Beschränkung wurde mit Release 2.5 beseitigt, so dass nunmehr auch im Papierformat vorliegende Testzertifikate in der CWA App gespeichert werden können.

²³ Bei einer Genesenenumimpfung mit dem Impfstoff von Johnson & Johnson wird der vollständige Impfschutz erst nach 14 Tagen angezeigt, da der im COVID-Zertifikat enthaltene Impfstatus keine Speicherung von Informationen zu einer eventuellen Genesung des Zertifikatsinhabers erlaubt. Bei den mRNA-Impfstoffen, die für einen vollständigen Impfschutz zwei Impfungen erfordern („2 von 2“), wird die Genesung des Zertifikatsinhabers durch die nur für Genesenenumimpfungen verwendete Nummerierung „1 von 1“ kenntlich gemacht. Diese Möglichkeit entfällt bei dem Impfstoff von Johnson & Johnson, da die Nummerierung „1 von 1“ auch bei Impfungen von nicht-genesenen Personen verwendet wird.

Sofern die Teststelle an den Zertifikatsservice angebunden ist, kann das Testzertifikat nach dem Einstellen des QR-Codes für die Testregistrierung für den Fall eines negativen Testergebnisses angefordert werden (siehe Abschnitt 5.4.8). Im Fall eines PCR-Tests muss der CWA-Nutzer für die Anforderung eines Testzertifikats zusätzlich das Geburtsdatum der jeweiligen getesteten Person in der CWA App eingegeben. Nachdem das (negative) Testergebnis vorliegt, wird das entsprechende Testzertifikat von der CWA App automatisch in der Zertifikats-Wallet der CWA App gespeichert. Da es sich bei den im Abrufverfahren übermittelten Testzertifikaten um reguläre Testzertifikate (im elektronischen Format) handelt, können sie in der CWA App ebenso wie mittels QR-Code-Scanner ausgelesene Testzertifikate verwendet werden.

5.4.14.3 Prüfung von COVID-Zertifikaten

Die Verwendung eines in der Zertifikats-Wallet gespeicherten COVID-Zertifikats kann in Präsenzsituationen durch Vorzeigen des QR-Codes und bei Online-Buchungen durch Übermittlung des COVID-Zertifikats an einen vom jeweiligen Leistungsanbieter (z. B. Reise- oder Veranstaltungsunternehmen) beauftragten Validierungsdienst (sog. Prüfpartner), der die Gültigkeit des Zertifikats für den Leistungsanbieter überprüft, erfolgen.²⁴

5.4.14.3.1 Präsenzsituationen

Um mittels eines COVID-Zertifikats den Impf-, Test- oder Genesenestatus gegenüber einem Dritten nachzuweisen, kann der CWA-Nutzer der Prüfperson den zugehörigen QR-Code mit der Übersichtsdarstellung oder der Detailansicht des COVID-Zertifikats vorzeigen, so dass die Prüfperson diesen mit der CovPassCheck-App oder einem anderen Prüfsystem auf Gültigkeit überprüfen kann.

Hinweis zum Prüfgegenstand: Die Datenverarbeitung im Zusammenhang mit der Prüfung von COVID-Zertifikaten durch Dritte ist unabhängig von der CWA und nicht vom Prüfgegenstand umfasst.

5.4.14.3.2 Online-Validierung

Um Zertifikatsinhaber bei der Buchung von Tickets und sonstigen Leistungen und vor der Inanspruchnahme solcher Leistungen über das Internet (z. B. Online-Check-In-Verfahren im Reiseverkehr) gegenüber dem jeweiligen Leistungsanbieter in die Lage zu versetzen, ihren Impf- oder Genesenestatus nachzuweisen, wurde die CWA App mit Release der Version 2.15 um eine Funktion für Online-Validierungen erweitert.²⁵ Dadurch kann der CWA-Nutzer ein

²⁴ Die Funktion für den Nachweis bei Online-Buchungen wurde mit Release der CWA App Version 2.15 eingeführt.

²⁵ Die CovPass-App wird ebenfalls die Online-Validierungsfunktion erhalten.

in seiner Zertifikats-Wallet gespeichertes COVID-Zertifikat an einen externen Validierungsdienst eines Drittanbieters (sog. „Prüfpartner“) übermitteln, der für eine prüfende Stelle (im Zusammenhang mit der Online-Validierung als „Leistungsanbieter“ bezeichnet) die Gültigkeit des COVID-Zertifikats überprüft und dem Leistungsanbieter sodann das Prüfungsergebnis mitteilt. Weder Leistungsanbieter noch Nutzer sind jedoch zur Nutzung des Online-Validierungsverfahrens verpflichtet. Voraussetzung für die Online-Validierung eines COVID-Zertifikats ist, dass der Leistungsanbieter den Validierungsdienst eines vom BMG anerkannten²⁶ Prüfpartners einsetzt und der CWA-Nutzer bei der Online-Buchung über das Buchungssystem des Leistungsanbieters (z. B. Webshop für Tickets) die Durchführung des Online-Validierungsverfahrens ausdrücklich gewünscht bzw. ausgewählt hat.²⁷

Zur Einleitung des Online-Validierungsverfahrens muss der Leistungsanbieter dem CWA-Nutzer im Rahmen des Buchungsvorgangs einen speziellen Initialisierungs-QR-Code aushändigen, was in der Regel durch Anzeige des QR-Codes im Webbrowser erfolgen wird. Nachdem der CWA-Nutzer den Initialisierungs-QR-Code mit dem QR-Code-Scanner der CWA App ausgelesen hat, wird in der CWA App zu Kontrollzwecken die Bezeichnung des Leistungsanbieters und die Beschreibung des Buchungsvorgangs angezeigt und über die für die Online-Validierung erforderliche Datenverarbeitung der CWA App informiert. Sofern der CWA-Nutzer in diese Datenverarbeitung einwilligt, werden die zur Durchführung der Online-Validierung benötigten Buchungsdaten vom Server des Leistungsanbieters abgerufen. Andernfalls wird das Online-Validierungsverfahren in der CWA App beendet.

Im nächsten Schritt prüft die CWA App anhand der vom Leistungsanbieter bereitgestellten Buchungsdaten lokal, ob der in den Buchungsdaten benannte Validierungsdienst in der vom BMG verwalteten Liste anerkannter Validierungsdienste aufgeführt ist. Ist das nicht der Fall, weist die CWA App den CWA-Nutzer darauf hin, dass der betreffende Validierungsdienst dem RKI nicht bekannt ist und die Online-Validierung daher nicht durchgeführt werden kann. Andernfalls wählt die CWA App anhand der Buchungsdaten ein geeignetes COVID-Zertifikat aus der Wallet aus. Falls weitere COVID-Zertifikate die Validierungskriterien des Leistungsanbieters erfüllen, werden diese als Liste angezeigt. Der Nutzer kann dann das vorgeschlagene COVID-Zertifikat bestätigen oder ein eventuelles anderes geeignetes Zertifikat für die Online-Validierung auswählen.

Nach der Zertifikatsauswahl zeigt die CWA App zu Kontrollzwecken nochmals das ausgewählte COVID-Zertifikat, die Bezeichnung des Leistungsanbieters und auch die Bezeichnung des Validierungsdienstes an und informiert den CWA-Nutzer über die weitere für die Online-Validierung erforderliche Datenverarbeitung der CWA App. Sofern der CWA-Nutzer in diese einwilligt, wird das ausgewählte COVID-Zertifikat von der CWA App an den Validierungsdienst übermittelt und dort nach Maßgabe der Validierungsanforderungen des

²⁶ Näheres zur Rolle des BMG siehe Abschnitt 5.9.3.

²⁷ Hinweis zum Prüfgegenstand: Die konkrete Datenverarbeitung auf Seiten des Leistungsanbieters, etwa durch seine Buchungssysteme, liegt nicht im Einflussbereich des RKI und ist nicht vom Prüfgegenstand umfasst. Für diese Datenverarbeitung ist der jeweilige Leistungsanbieter verantwortlich.

Leistungsanbieters überprüft und das Validierungsergebnis (also ob die Validierung erfolgreich oder nicht erfolgreich war) anschließend dem Leistungsanbieter bekanntgegeben.

Das Validierungsergebnis und im Fall einer nicht erfolgreichen Validierung auch der Grund des Fehlschlags (beispielsweise welche Validierungsanforderungen des Leistungsanbieters vom Validierungsdienst als nicht erfüllt bewertet worden sind) werden dem CWA-Nutzer direkt in der CWA App angezeigt.

5.4.14.4 Weitere Wallet-Funktionen

Neben den Kernfunktionen zur Speicherung, Verwaltung und Verwendung von COVID-Zertifikaten mit einem Smartphone umfasst die Zertifikats-Wallet auch weitere Funktionen, mit denen der spezifische Zweck der COVID-Zertifikate unterstützt wird.

5.4.14.4.1 Zertifikats-Gültigkeitsprüfung

Die CWA App kann verwendet werden, um die Gültigkeit von in der Wallet gespeicherten COVID-Zertifikaten anhand der aktuell geltenden Business Rules der teilnehmenden Mitgliedstaaten zu prüfen. Zum Verwenden der Gültigkeitsprüfungsfunktion muss der CWA-Nutzer in der Detailansicht des zu prüfenden COVID-Zertifikats auf den Button „Gültigkeit prüfen“ tippen und das Land auswählen, dessen Business Rules berücksichtigt werden sollen. Zusätzlich muss das Datum angegeben werden, für das die Gültigkeitsprüfung durchgeführt werden soll. Die CWA App lädt sodann die gegenwärtig gültigen Business Rules der Mitgliedstaaten vom Serversystem der CWA herunter. Es werden immer die Regelwerke sämtlicher Mitgliedsländer heruntergeladen. Die Prüfung der COVID-Zertifikate gegen die Business Rules des ausgewählten Mitgliedslandes findet lokal in der CWA App statt. Anschließend wird dem CWA-Nutzer angezeigt, ob das geprüfte Zertifikat dem Regelwerk des gewählten Mitgliedslandes entspricht. Ist das nicht der Fall, wird dem CWA-Nutzer außerdem mitgeteilt, welche Regeln nicht eingehalten werden bzw. welche Regeln nicht geprüft werden konnten.

5.4.14.4.2 Druckversion von Impfzertifikaten

Die CWA App kann eine PDF-Version („Druckversion“) eines in der Wallet gespeicherten Impfzertifikats erstellen und dieses über die Teilen-Schnittstelle des Betriebssystems exportieren, so dass die PDF-Version ausgedruckt oder an andere für die die Verwendung von PDF-Dateien geeigneten Apps oder Systemdienste übergeben werden kann. Nach dem Schließen des Teilen-Dialogs des Betriebssystems wird die PDF-Version des Impfzertifikats unabhängig davon, ob es tatsächlich gedruckt oder anderweitig geteilt worden ist, aus dem Speicher der CWA App gelöscht.

Zur Erstellung der Druckversion wird das offizielle Impfzertifikats-Template verwendet, mit dem auch die von den zur Ausgabe von Impfzertifikaten verpflichteten Stellen (z. B. Apotheken, ärztliche Praxen) ausgegebenen Impfzertifikate technisch generiert werden.

Es können nur Druckversionen von vom RKI selbst ausgestellten Impfzertifikaten erzeugt werden. Für andere digitale COVID-Zertifikate als Impfzertifikate können keine Druckversionen erzeugt werden.

Da das lokal erzeugte PDF-Dokument personenbezogene Gesundheitsdaten des Zertifikatsinhabers (Zertifikatsaussage) enthält, erfolgt in der CWA App vor der Erstellung der Druckversion vorsorglich ein Hinweis auf die Vertraulichkeitsrisiken bei einem Teilen des PDF-Dokuments mit Dritten. Zudem soll der CWA-Nutzer auch durch die Bezeichnung als „Druckversion“ daran erinnern werden, dass der Zweck der Funktion in erster Linie darin besteht, bei Bedarf die Herstellung einer Papierversion eines Impfzertifikats zu ermöglichen.

5.4.14.4.3 Mitteilungen über Auffrischimpfungen

Die CWA App weist CWA-Nutzer mit einem gültigen Impfzertifikat über die letzte Impfung einer abgeschlossenen Impfserie in der Wallet auf eine eventuell notwendige Auffrischimpfung des jeweiligen Zertifikatsinhabers hin, wenn seit der Impfung eine bestimmte Zeit verstrichen ist. Die Zeitspanne bis zur Erteilung eines Hinweises richtet sich nach den aktuellen Empfehlungen des RKI. Da über die Notwendigkeit und Durchführung einer Auffrischimpfung nur nach individueller ärztlicher Abwägung im Einzelfall entschieden werden kann, daher spricht der Hinweis in der CWA App ausdrücklich nur davon, dass eine Auffrischimpfung aufgrund des Zeitablaufs erforderlich sein „könnte“.

Der Hinweis wird dem CWA-Nutzer als lokale Push-Mitteilung sowie in der CWA App erteilt. Voraussetzung für den Erhalt einer lokalen Push-Mitteilung ist, dass die CWA App zum Versand von Push-Mitteilungen berechtigt ist (siehe unter Ziffer 5.4.15.3). Sie hat den generischen Inhalt „Es gibt Neuigkeiten von Ihrer Corona-Warn-App.“ Wenn der CWA-Nutzer daraufhin die CWA App öffnet, findet er mittels einer roten Markierung in der Navigationsleiste Informationen zu dem möglichen Auffrischungsbedarf und einen Link zur FAQ mit weiterführenden Hinweisen. Zudem wird das Impfzertifikat in der CWA App markiert, sodass der CWA-Nutzer den Hinweis zu dem entsprechenden Zertifikat auch dort einsehen kann.

5.4.14.4.4 Zertifikaterneuerung

Die CWA App informiert den CWA-Nutzer mit einer Vorlaufzeit von 28 Tagen über den bevorstehenden Ablauf der technischen Gültigkeit von gespeicherten Genesenen- und Impfzertifikaten. Er hat dann bis zu 90 Tage nach Ablauf der technischen Gültigkeit Zeit, das betreffende COVID-Zertifikat in der CWA App zu „erneuern“, indem er auf den Hinweis „Zertifikat erneuern“ tippt. Nachdem er sein Einverständnis gegeben hat, wird das neue COVID-Zertifikat vom Zertifikatsservice angefordert. Das „erneuerte“ COVID-Zertifikat ist aus technischer Sicht ein neu ausgestelltes weiteres COVID-Zertifikat und ersetzt nach Erhalt das

bald ablaufende COVID-Zertifikat. Letzteres wird automatisch in den Papierkorb verschoben und nach 30 Tagen automatisch gelöscht.

5.4.15 Weitere Funktionen

Neben den oben beschriebenen Funktionen, die im Mittelpunkt der CWA App stehen, umfasst die CWA App unter anderem diese weiteren Funktionen:

5.4.15.1 Teilen

Der CWA-Nutzer kann die CWA App mit anderen Personen „teilen“, indem er diesen einen Link zur offiziellen Homepage der CWA (www.corona-warn-app.de) sendet. Das eigentliche Teilen findet außerhalb der CWA App über die hierfür vorgesehene Teilen-Schnittstelle des Betriebssystems statt. Die CWA App erhält somit keinen Zugriff auf die Kontakte des CWA-Nutzers.

5.4.15.2 App-Informationen

Im Untermenü „App-Informationen“ werden die Datenschutzerklärung, das Impressum sowie weitere rechtliche und Service-Informationen im Zusammenhang mit der CWA bereitgestellt (z. B. Nutzungsbedingungen, Open-Source-Lizenzhinweise, Kontaktdataen der Hotline).

5.4.15.3 Einstellungen

Im Bereich „Einstellungen“ befinden sich alle Konfigurationsfunktionen der CWA App, etwa welche Push-Mitteilungen die CWA App dem CWA-Nutzer zusenden darf. Zudem wird eine Funktion zum **Rücksetzen auf Auslieferungszustand** bereitgestellt.

5.4.15.4 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.

5.4.15.5 Datenspende

Seit Release der CWA App Version 1.13 wird der CWA-Nutzer beim erstmaligen Start der (aktualisierten) CWA App gefragt, ob er dem RKI **Nutzungsdaten** über die Verwendung seiner

CWA App zu Auswertungszwecken freiwillig zur Verfügung stellen möchte (Datenspende). Die Teilnahme an der Datenspende ist freiwillig und einwilligungsbasiert. In der Einwilligungserklärung und über einen Verweis auf Detailinformationen kann sich der CWA-Nutzer über die Zwecke und die Datenverarbeitung im Zusammenhang mit der Datenspende informieren, bevor er die Einwilligung erteilt.

Im Menü „Einstellungen“ (Abschnitt 5.4.15.3) kann der CWA-Nutzer seine Einwilligung auch zu einem späteren Zeitpunkt erteilen oder widerrufen, sofern er an der Datenspende nicht mehr teilnehmen möchte.

Im Rahmen der Datenspende wird der CWA-Nutzer um die Angabe des Bundeslandes und der Region (Kreis/Bezirk) und die Angabe der Altersgruppe (bis 29 Jahre, 30 bis 59 Jahre, 60 Jahre oder älter) gebeten. Die Angabe dieser Daten ist optional. Für beide Auswahlfelder ist die Standardangabe „keine Angabe“ vorausgewählt. Diese weiteren Angaben helfen im Rahmen der metadatenbasierten statistischen Auswertung der Nutzung der CWA App auf regionale und altersgruppenspezifische Unterschiede einzugehen und auf regionale Vorkommnisse frühzeitig zu reagieren (z.B. den regionalen Ausfall eines spezifischen Testlabors, sobald die Datenbasis zeigt, dass in der Region keine Testergebnisse abgerufen werden).

Bei Aktivierung der Datenspende wird der Verifikations-Dienst zur Echtheitsprüfung des Endgerätes (Privacy-preserving Access Control, PPAC) des jeweiligen Betriebssystemherstellers Apple oder Google verwendet. Der Einsatz des Verifikations-Dienstes erfolgt nur mit Einwilligung des CWA-Nutzers.

5.4.15.6 Befragungen

Seit der CWA App Version 1.13 können CWA-Nutzer an situationsspezifischen Befragungen des RKI teilnehmen. Die Einladung zu einer freiwilligen Befragung wird in der CWA App im Fall der Anzeige eines erhöhten Risikostatus auf dem Home-Screen unter der Risiko-Kachel angezeigt. Sofern der CWA-Nutzer auf den Button „Zur Befragung“ tippt, werden ihm innerhalb der CWA App nähere Informationen über den Ablauf und den Zweck der „Befragung zur Bewertung und Verbesserung der Corona-Warn-App“ präsentiert. In der angezeigten Einwilligungserklärung und über einen Verweis auf Detailinformationen kann sich der CWA-Nutzer über die Zwecke und die Datenverarbeitung im Zusammenhang mit der Befragung informieren, bevor er die Einwilligung erteilt.

Die Befragung selbst findet außerhalb der CWA App auf einer Website des RKI statt. Vor der Anzeige des individuellen Links zur Befragungs-Website wird über den Verifikations-Dienst zur Echtheitsprüfung des Endgerätes (Privacy-preserving Access Control, PPAC) des jeweiligen Betriebssystemherstellers Apple oder Google ein Einmalpasswort (One-time-Password, OTP) erzeugt. Der Einsatz des Verifikations-Dienstes erfolgt nur mit Einwilligung des CWA-Nutzers.

5.4.15.7 Schnelltest-Profile

In der CWA App können mehrere Schnelltest-Profile angelegt werden. Dafür öffnet der CWA-Nutzer über den Home-Bildschirm den Bildschirm „Test registrieren“ und tippt auf die Kachel „Schnelltest-Profile“.

Bevor ein Schnelltest-Profil angelegt werden kann, wird auf die Funktionsweise des Schnelltest-Profils sowie diesbezügliche Datenschutzaspekte hingewiesen. Anschließend wird eine Eingabemaske angezeigt, in die der CWA-Nutzer seine Profildaten eintragen kann. Es müssen nicht alle Datenfelder ausgefüllt werden, worauf der CWA-Nutzer hingewiesen wird. Wenn der CWA-Nutzer auf „Speichern“ tippt, erzeugt die CWA App einen QR-Code, in dem die vom Nutzer eingegebenen Daten kodiert sind (Schnelltest-Profil, siehe Abschnitt 5.7.18). Anstelle der Kachel „Schnelltest-Profil anlegen“ wird sodann die Kachel „Schnelltest-Profil“ angezeigt.

Wenn der CWA-Nutzer künftig über den Home-Bildschirm die Funktion „Test registrieren“ aufruft und dort auf die Kachel „Schnelltest-Profile“ tippt, werden alle angelegten Schnelltest-Profile angezeigt. Nach Auswahl eines Schnelltest-Profils wird der zugehörige QR-Code zusammen mit dem Namen und Geburtsdatum der betreffenden Person angezeigt. Wenn der CWA-Nutzer den QR-Code vorzeigt, kann dieser gescannt werden und das enthaltene Schnelltest-Profil (siehe Abschnitt 5.7.18) durch die Teststelle ausgelesen werden. Bei Durchführung eines Antigen-Schnelltests kann dann auf eine manuelle Eingabe der Daten durch Mitarbeiter der Teststelle verzichtet werden.

5.4.15.8 Fehlerberichte

Seit Version 2.2 der CWA App können Fehlerberichte erstellt und geteilt werden. Diese Funktion soll dem CWA-Nutzer die Möglichkeit geben, bei Problemen während des Betriebs der CWA App, insbesondere solchen, die auf potenzielle Programmierfehler hinweisen (z. B. Abstürze, Fehlermeldungen, Darstellungsfehler) die Programmereignisse und -abläufe (z. B. Fehlermeldungen, Laufzeitinformationen) automatisch im Hintergrund von der CWA App in Form eines Logfiles aufzeichnen zu lassen, um die Entwickler der CWA App bei der Problembehebung zu unterstützen (Fehlerbericht). Nachdem die Ursache für das auftretende Problem gefunden wurde, können die Entwickler eine Lösung entwickeln, damit das Problem in zukünftigen Versionen der CWA App nicht mehr auftaucht. Die Aufzeichnung für den Fehlerbericht erfolgt erst nach einer ausdrücklichen Aktivierung dieser Funktion durch den CWA-Nutzer und kann jederzeit wieder gestoppt werden. Der CWA-Nutzer kann zu jedem Zeitpunkt entscheiden, ob und wann der Fehlerbericht aufgezeichnet wird und ob er seinen Fehlerbericht mit dem RKI teilen möchte.

Die Aktivierung der Fehlerberichts-Funktion erfolgt im Bereich „App-Einstellungen“ unter dem Menüpunkt „Fehlerberichte“. Standardmäßig ist die Funktion deaktiviert. Sie richtet sich primär an CWA-Nutzer aus der Entwicklungs-Community. Für den typischen CWA-Nutzer ist die Fehlerberichts-Funktion nicht von Interesse.

Der CWA-Nutzer wird zunächst über Zweck und Funktionsweise sowie die wichtigsten Datenschutzaspekte des Fehlerberichts informiert. Durch das Antippen des Buttons „Starten“ wird die Aufzeichnung des Fehlerberichts schließlich gestartet. Ab diesen Punkt werden verschiedene Daten von der CWA App erfasst und in einer Log-Datei gespeichert.

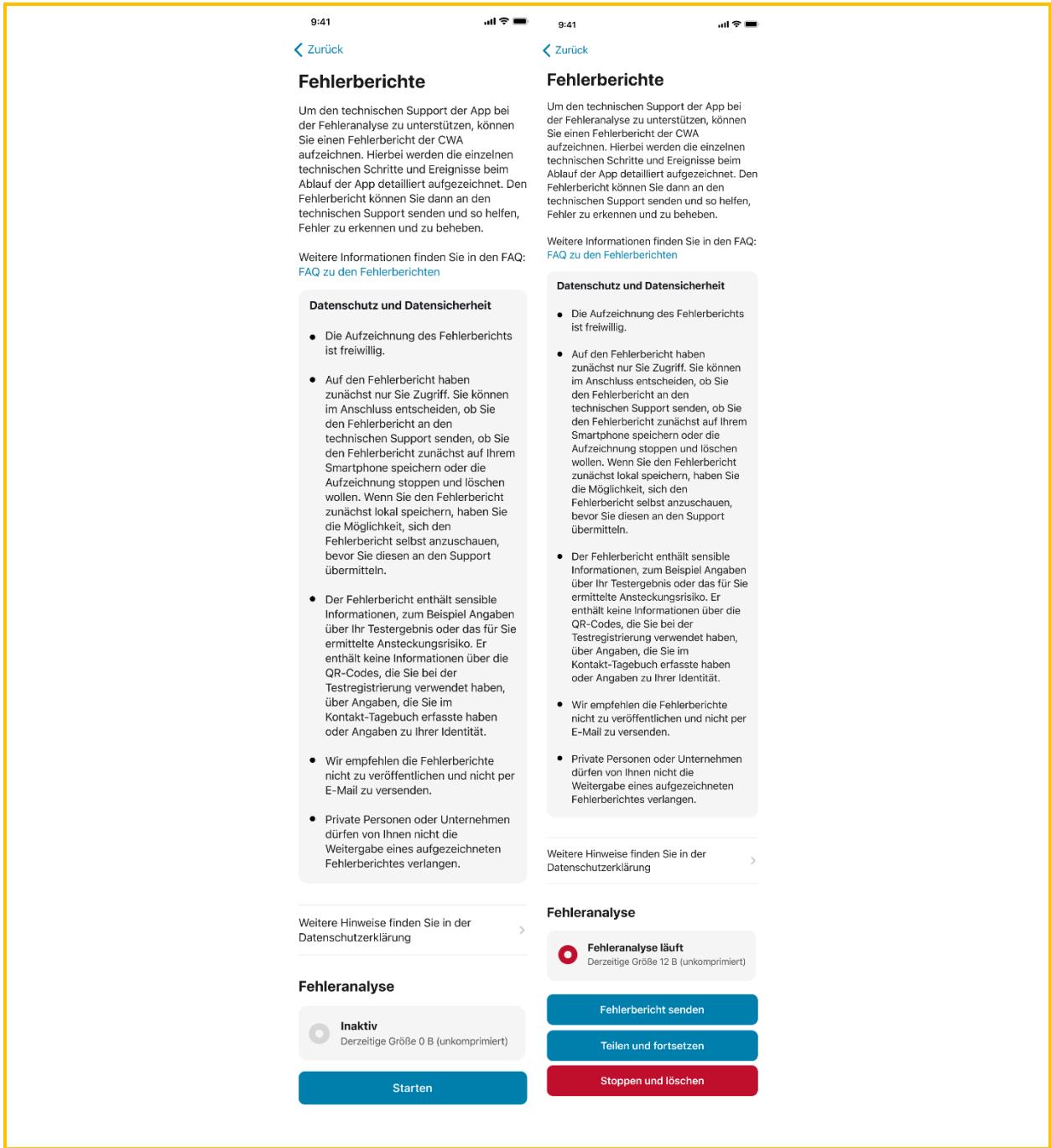


Abbildung 09: Aktivierung des Fehlerberichts (Beispiel-Screenshot iOS)

Sobald der Fehlerbericht aktiviert ist, stehen dem CWA-Nutzer folgende Funktionen zur Verfügung:

- Fehlerbericht senden: Der Fehlerbericht wird von der CWA App an das RKI übermittelt.

- Teilen und fortsetzen: Der Fehlerbericht kann als einfacher Text (plain text) über die Teilen-Schnittstelle des Betriebssystems mit geeigneten Apps und Systemdiensten geteilt werden.
- Stoppen und löschen: Die Aufzeichnung wird angehalten und das gespeicherte Logfile wird gelöscht.

Will der CWA-Nutzer die Funktion „Fehlerbericht senden“ nutzen, erscheint zunächst ein Informations-Screen, auf dem die Datenverarbeitung für die Zwecke dieser Funktion erläutert und der Nutzer hierfür um sein Einverständnis gebeten wird. Sofern der CWA-Nutzer dieses erteilt, wird der Fehlerbericht an das RKI gesendet.

Nach dem erfolgreichen Hochladen des Fehlerberichts wird diesem eine eindeutige ID zugewiesen und in der CWA App unter dem Menüpunkt „ID Historie“ angezeigt (Fehlerberichts-ID). Der CWA-Nutzer kann die Fehlerberichts-ID dann beispielsweise im Rahmen von Support-Anfragen gegenüber dem RKI angeben, falls er mit diesem in direkten Kontakt treten will.

5.4.15.9 QR-Code-Scanner

Die CWA App beinhaltet einen universellen QR-Code-Scanner, der über die Schnellstartleiste und aus verschiedenen Untermenüs der CWA App gestartet werden kann. Der QR-Code-Scanner kann alle mit der CWA App verwendbaren QR-Codes auslesen. Der CWA-Nutzer wird dann abhängig vom eingescannten QR-Code zu der für das jeweilige Dokument relevanten Funktion (z. B. Einchecken bei einem Event oder Speichern eines COVID-Zertifikats) geführt. Zudem besteht die Möglichkeit, einen QR-Code aus einer Bilddatei im Speicher bzw. in der Bildergalerie des Smartphones in die CWA App zu laden, sofern der CWA-Nutzer der CWA App die entsprechende Zugriffsberechtigung erteilt hat. Diese Funktion wurde eingeführt, nachdem eine erhebliche Zahl von CWA-Nutzern von Problemen mit dem QR-Code-Scanner berichtet hat. Diese konnten überwiegend auf eine zu geringere Auflösung/Qualität der in den Smartphones der betroffenen CWA-Nutzer verbauten Kameras zurückgeführt werden. Die Funktion zum Import eines (mit einer leistungsfähigeren) Kamera aufgenommenen Bildes des QR-Codes soll diesem Umstand Rechnung tragen.

5.5 Systemarchitektur

Für die technische Umsetzung der Infrastruktur der CWA wurde für das 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 unabsichtliche oder ungewollte Identifizierung einzelner Nutzer durch die an den Datenverarbeitungsvorgängen beteiligten Stellen und andere Nutzer zuverlässig ausgeschlossen werden kann. Die CWA verzichtet nach Möglichkeit 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.

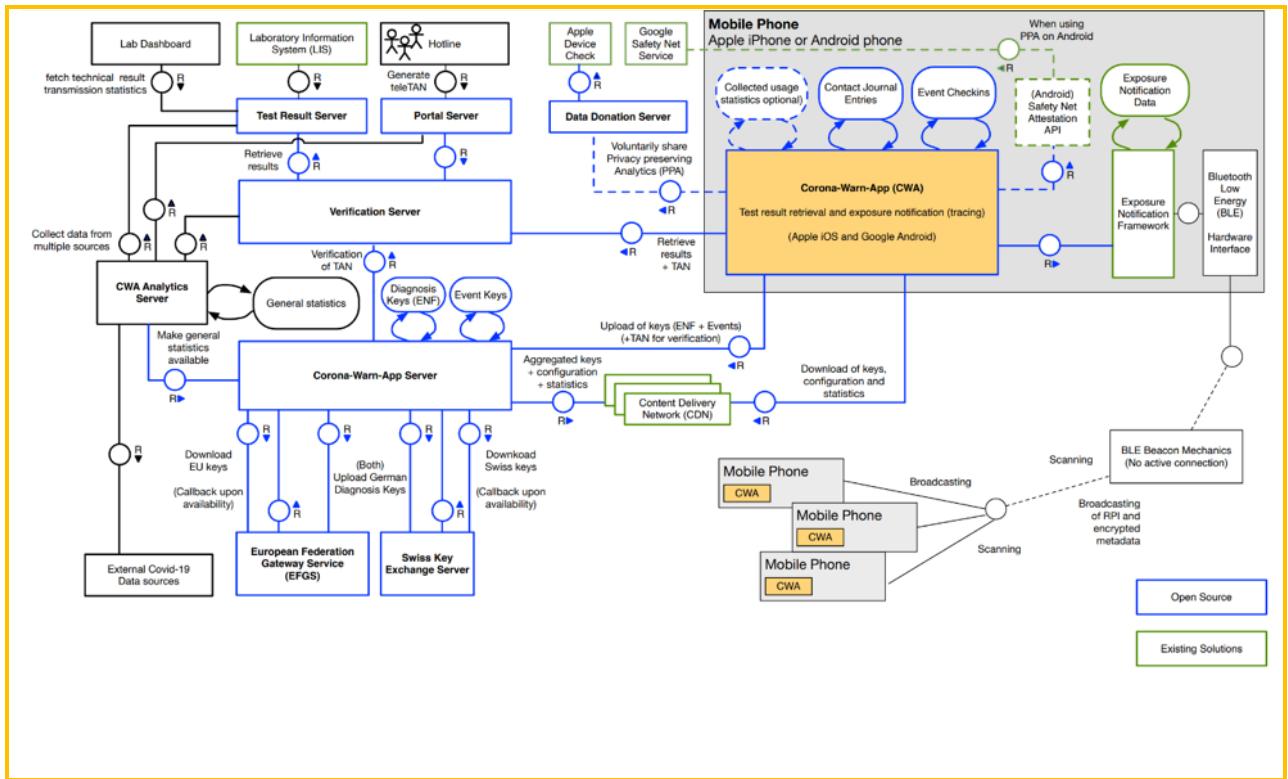


Abbildung 10: Überblick über die Architektur der CWA

Die 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 länderübergreifenden Funktionen bzw. Zwecke der CWA werden durch die Anbindung des CWA Servers an den EFGS und den CHGS und somit nicht direkt über die CWA App realisiert.

5.5.1 Smartphone

Das Smartphone einschließlich seines Betriebssystems stellt die für den Betrieb der CWA App notwendigen Funktionalitäten und Konnektivitäten bereit. Für den Betrieb der CWA App sind insbesondere die folgenden Komponenten und Hintergrunddienste von Bedeutung:

Internetkommunikation:

Die CWA App benötigt eine Internetverbindung, damit Funktionen, die nicht ausschließlich lokal funktionieren, auf die jeweilige Serverkomponente der CWA zugreifen und die jeweils benötigten Daten abrufen oder übertragen können.

Kamera:

Die Kamera wird für das Einscannen von QR-Codes benötigt.

ENF:

Das ENF ist ein Bluetooth-Low-Energy-basierter Dienst, der über eine Schnittstelle des Betriebssystems bereitgestellt wird. Er wurde von Apple und Google vor dem Hintergrund der Corona-Pandemie entwickelt, um Tracing-Apps die Annäherungserkennung und Aufzeichnung von Kontakten zwischen mobilen Endgeräten mit den Betriebssystem iOS und Android zur Berechnung eines Infektionsrisikos zu ermöglichen. Apple und Google erlauben bisher nur einer „offiziellen“ Corona-App pro Land die Nutzung der ENF-Schnittstelle, das heißt, dass die jeweilige Corona-App von einer Gesundheitsbehörde oder einer von einer zuständigen Behörde beauftragten anderen Stelle (bspw. Rotes Kreuz) angeboten werden muss. In der Bundesrepublik Deutschland ist die CWA App die offizielle nationale Corona-App und somit als einzige Anwendung hierzulande berechtigt, die ENF-Schnittstelle zu nutzen.

5.5.2 CWA Server

Der CWA Server wird für die Verteilung der Positivschlüssel im Rahmen der Warnfunktion benötigt. Wenn ein positiv getesteter 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 Widerrufslisten und Positivschlüssel vom und an den EFGS und den CHGS, um die länderübergreifende Warnung sowie den länderübergreifenden Zertifikatswiderruf zu ermöglichen.

Der CWA-Server lädt in regelmäßigen Abständen die aktuellen Business Rules vom Business Rules Service (erforderlich für die Gültigkeits- und Statusprüfung) und die aktuellen Value Sets (erforderlich für die korrekte Darstellung der Zertifikate aus unterschiedlichen Mitgliedstaaten) herunter. Die heruntergeladenen Daten werden auf dem CWA Server für die CWA App aufbereitet und über das CDN-Magenta zur Verfügung gestellt.

Beim Upload der Dateien auf das CDN-Magenta prüft der CWA Server, ob die Dateien der Business Rules und Value Sets aktualisiert worden sind. Nur wenn geänderte Dateien vorliegen und die dazugehörige Datei nicht leer ist, wird sie auf das CDN-Magenta gespielt und damit für die CWA App verfügbar gemacht.

5.5.3 CDN-Magenta

Das CDN-Magenta ist ein Content Delivery Network, über welches die von bestimmten CWA App-Funktionen benötigten Daten zum Herunterladen bereitgestellt werden. Sämtliche Server des CDN-Magenta werden in Deutschland betrieben.

Folgende Daten werden über das CDN-Magenta bereitgestellt:

- Liste mit den aktuellen Positivschlüsseln (Positivschlüssel-Pakete)
- Liste mit Event-IDs der von positiv getesteten CWA-Nutzern besuchten Veranstaltungen (Check-in-Pakete)
- **Bewertungseinstellungen (BWE)** (siehe Abschnitt 5.7.8)
- Statistikdaten für die Statistik-Kachel
- Value Sets für die Darstellung von COVID-Zertifikaten
- Business Rules für COVID-Zertifikate
- Widerrufslisten für COVID-Zertifikate

Beim Laden der Business Rules werden immer die Regelwerke sämtlicher Mitgliedstaaten und Länder heruntergeladen. Das Laden des Gesamtpaketes verhindert, dass anhand der Anfragen am CDN-Magenta Reiserouten einzelner CWA-Nutzer nachvollzogen werden können. Die Prüfung der Zertifikate gegen die Business Rules des vom CWA-Nutzer ausgewählten Mitgliedstaates findet lokal auf dem Smartphone statt.

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. Zur Echtheitsprüfung verarbeitet der Verifikationsserver die TAN. Das 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 Testergebnisses nicht in der CWA App erhalten hat und es sich um einen PCR-Test handelt (siehe hierzu auch Abschnitt 5.4.10), kann er 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. Nach dem gleichen Prinzip funktioniert die Funktion „In Vertretung warnen“, wobei in diesem Fall nicht von teleTAN, sondern PIW-TAN gesprochen wird.

5.5.5 Portalserver

Über den Portalserver steht den Mitarbeitern der Verifikations-Hotline eine Funktion zur Abfrage von teleTANs und PIW-TANs zur Verfügung. Über eine Weboberfläche, die mit dem Portalserver verbunden ist, kann der Mitarbeiter die jeweils benötigte TAN-Variante generieren lassen. 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 tele- oder PIW-TAN generiert. Sodann wird die tele- oder PIW-TAN 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 tele- oder PIW-TAN 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 und Teststellen die Testergebnisse der CWA-Nutzer ablegen können, die einer entsprechenden Übermittlung an die CWA zugestimmt haben. Die Labore und Teststellen greifen über eine eigene Software, den **Lab Client bzw. das Teststellen-System**, auf den Test Result Server zu. Diese Software ist nicht vom Prüfgegenstand umfasst und wird im Verantwortungsbereich der jeweiligen Labore bzw. Teststellen betrieben.

5.5.7 Data Donation Server

Auf dem **Data Donation Server** werden in den dafür vorgesehenen Datenbanken die von CWA-Nutzern im Rahmen der Datenspende zur Verfügung gestellten Nutzungsdaten gespeichert.

Über den Data Donation Server wird auch der Dienst für die Echtheitsprüfung realisiert, welcher das für bestimmte App-Funktionen erforderliche **One Time-Password (OTP)** validiert. Dazu werden die für die Validierung erforderlichen Prüfdaten (Token) empfangen und geprüft. Konkret betrifft dies die Funktionen für die Einladung zu Befragungen, die Datenspende und das Senden von Fehlerberichten.

Die Echtheitsprüfung kommt zum Einsatz, wenn im Hinblick auf die vorgenannten Funktionen zur Erreichung eines mit den von der CWA App übermittelten Daten verfolgten Zwecks eine bestimmte Datenqualität gewährleistet sein muss ist. Denn die Echtheitsprüfung erhöht die Wahrscheinlichkeit, dass es sich bei der Person, die die Daten übermittelt, tatsächlich um einen CWA-Nutzer handelt, der die CWA App in einer nicht-manipulierten Umgebung, also auf einem durch den jeweiligen Hersteller validierten Endgerät ausführt. Sie reduziert somit etwa das Risiko, dass die Befragungen oder die Datenerhebung mittels der Datenspende durch massenhaft übermittelte Daten (z. B. im Rahmen konzertierter Angriffe) manipuliert oder beeinträchtigt und die Auswertungsergebnisse damit unbrauchbar werden. Ohne eine Echtheitsprüfung könnte auch das Senden von unechten Fehlerberichten, d. h. gefälschte Fehlerberichte oder Fehlerberichte, die von einer manipulierten CWA App erzeugt wurden, nicht sicher festgestellt bzw. technisch verhindert werden. Die übermittelten Daten wären dann nicht belastbar und für die mit den genannten Funktionen verfolgten Zwecke nicht oder nur bedingt geeignet. Zudem bestünde die Gefahr, dass die Serversysteme der CWA mit künstlich generierten falschen Fehlerberichten überschwemmt werden.

5.5.8 Log Storage Server

Der Log Storage Server wird in der OTC betrieben und stellt den Dienst **Error Log Service (ELS)** bereit. Der ELS nimmt die mit der Fehlerberichtsfunktion der CWA App aufgezeichneten und an das RKI gesendeten Fehlerberichte entgegen, teilt diesen eine Fehlerberichts-ID zu und stellt die Fehlerberichte den CWA-Entwicklern über ein Webportal zur Verfügung (siehe Abschnitt 5.6.9).

5.5.9 DCC Server

Der DCC Server bildet die Schnittstelle zwischen dem CWA-System (Verifikationsserver und Test Result Server) und dem Zertifikatsservice des RKI. Er erzeugt auf Grundlage der im CWA-System vorliegenden Daten die eindeutige Zertifikatskennung für vom CWA-Nutzer per CWA App angeforderte COVID-Testzertifikate und fordert beim Zertifikatsservice des RKI die entsprechende elektronische Signatur für das COVID-Testzertifikat an.

5.5.10 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 diesen in Gestalt des EFGS umgesetzt²⁸.

Beim EFGS handelt es sich um eine technische Datenplattform, über die die Informationen zu Warnungen, die durch die nationalen Corona-Apps zur länderübergreifenden Risiko-Ermittlung und Warnung jeweils erfasst werden, zwischen den am EFGS teilnehmenden Mitgliedstaaten der Europäischen Union ausgetauscht werden. In der Folge können die Positivschlüssel eines Nutzers auch zur Warnung von Nutzern anderer nationaler Corona-Apps genutzt werden, da alle nationalen Corona-Apps das ENF verwenden und deshalb technisch zueinander kompatibel sind. So können Begegnungen zwischen Nutzern verschiedener nationaler Corona-Apps (z. B. auf Reisen) bei der Risiko-Ermittlung berücksichtigt werden.

Am EFGS können Mitgliedstaaten der EU 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 nationalen Corona-Apps jeweils Verantwortlichen gemeinsam betrieben und verantwortet (Art. 26 DSGVO). Sie haben in ihrer Eigenschaft als gemeinsam Verantwortliche ein

²⁸ *Europäische Kommission: Coronavirus: new steps towards setting-up of an interoperability solution for mobile tracing and warning apps*, vom 15.07.2020, 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 11.10.2022).

formalisiertes Antragsverfahren ausgearbeitet, in dessen Rahmen die rechtlichen und technischen Anforderungen für die Teilnahme überprüft werden.

In technischer Hinsicht sind die jeweils zuständigen Server der verschiedenen nationalen Corona-Apps (im Fall der CWA ist dies der CWA Server) mit dem EFGS verbunden. Die Server der nationalen Corona-Apps laden in regelmäßigen Abständen die Positivschlüssel der Nutzer der eigenen nationalen Corona-App hoch und die zur Verfügung gestellten Positivschlüssel der Nutzer von anderen nationalen Corona-Apps herunter. Das Design des EFGS folgt den Interoperabilitätsleitlinien²⁹, den zwischen den Mitgliedstaaten und der Europäischen Kommission vereinbarten technischen Spezifikationen³⁰, den in der EU Toolbox aufgeführten Leitlinien und den EU-Leitlinien zur Gewährleistung der uneingeschränkten Einhaltung der Datenschutzstandards durch Mobil-Apps³¹ sowie den Empfehlungen der Europäischen Kommission für den Einsatz von KontaktNachverfolgungs-Apps zur Bekämpfung der Pandemie³². 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 Kontakt Personen in einem länderübergreifenden Kontext dienen darf. Die Zwecke, für die die über den EFGS ausgetauschten Daten verwendet werden dürfen, sind damit abschließend festgelegt.

Zudem sind die Datenkategorien festgelegt, die über den EFGS verteilt 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.

²⁹ 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 11.10.2022).

³⁰ [Set of Technical Specifications](#).

³¹ 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 11.10.2022).

³² 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 11.10.2022).

Die Angabe zu relevanten Ländern ermöglicht es den teilnehmenden Verantwortlichen, bei Bedarf 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 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 von der CWA kein Gebrauch gemacht.

Im o. g. Durchführungsbeschluss ist grundlegend festgelegt, welche Aufgaben die gemeinsam Verantwortlichen bei der Geltendmachung von Betroffenenrechten jeweils haben und wie bei Verletzungen des Schutzes personenbezogener Daten vorzugehen ist.

5.5.11 Schweizer Gateway Service (CHGS)

Der CHGS zur länderübergreifenden Warnung zwischen Deutschland und der Schweiz ist ein auf Schweizer Seite entwickelter und betriebener Fork des von TSI und SAP entwickelten EFGS-Systems, das unabhängig vom EFGS weiterentwickelt und betrieben wird. Technischer Betreiber des CHGS ist das BAG, welches auch die Schweizer Corona-App herausgibt und für diese Datenverarbeitungsvorgänge verantwortlich ist.

Funktion und Funktionsweise des CHGS entsprechen derjenigen des EFGS mit der Maßgabe, dass der Zweck des CHGS in der Ermöglichung von länderübergreifenden Warnungen zwischen Nutzern der Schweizer Corona-App und Nutzern anderer nationaler Corona-Apps liegt. Die Notwendigkeit des CHGS ergibt sich daraus, dass die Teilnahme am im Übrigen funktional und technisch äquivalenten EFGS durch einen Durchführungsbeschluss der EU-Kommission, also eine „Rechtsvorschrift der Union, denen die Verantwortlichen unterliegen“ (Art. 26 Abs. 1 S. 2 DSGVO), geregelt wird. Da die Schweiz kein Mitglied der EU ist, unterliegt sie diesem Durchführungsbeschluss nicht.

Anmerkung:

Zum Stand dieses DSFA-Berichts ist das Schweizer Corona-Warn-System aufgrund eines Beschlusses des Bundesrats der Schweiz deaktiviert, so dass gegenwärtig kein Datenaustausch zwischen dem CHGS und dem CWA Server stattfindet. Das Serversystem der Schweizer Corona-App wird jedoch aufrechterhalten, um es bei Bedarf wieder aktivieren zu können.³³ Bei der Risikoanalyse im Zusammenhang mit dem CHGS wird seitens des DSFA-Teams vorsorglich ein weiterhin aktiv genutztes CHGS zugrunde gelegt, auch wenn infolge der Deaktivierung zurzeit tatsächlich keine personenbezogenen Daten verarbeitet werden.

³³ Vgl. <https://www.bag.admin.ch/bag/de/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html> (letzter Abruf: 14.04.2022).

5.5.12 Validierungsdienste

Validierungsdienste dienen der in Online-Buchungsprozesse integrierten Validierung von COVID-Zertifikaten (Online-Validierung). Validierungsdienste werden eigenverantwortlich von Drittanbietern (sog. Prüfpartner) entwickelt und betrieben. Sie verfügen über Schnittstellen sowohl für Wallet-Apps als auch zu den Backendsystemen der Leistungsanbieter (z. B. den von Veranstaltern eingesetzten Buchungssysteme), mit denen sie zusammenarbeiten. Die Validierungsdienste prüfen für die Leistungsanbieter im Rahmen von Online-Buchungen die von einem Wallet-App-Nutzer aus einer Wallet-App übermittelten COVID-Zertifikate auf Echtheit- und Gültigkeit sowie darauf, ob sie die vom jeweiligen Leistungsanbieter festgelegten Validierungsanforderungen erfüllen. Die Echtheits- und Gültigkeitsprüfung durch die Validierungsdienste erfolgt grundsätzlich wie bei stationären oder mobilen Prüfsystemen anhand der Public Keys und Business Rules, die vom EU-Gateway³⁴ bereitgestellt werden. Zusätzlich können mit einem Validierungsdienst aber auch individuelle Business Rules des jeweiligen Leistungsanbieters geprüft werden, die im Kontext von Validierungsdiensten als „Validierungsanforderungen“ bezeichnet werden.

Alle Stellen und Personen, die einen Validierungsdienst entwickeln und/oder anbieten möchten, können auf die von TSI im Auftrag der EU-Kommission entwickelte Referenzimplementierung für einen Validierungsdienst zurückgreifen. Leistungsanbieter können zudem auf Referenzimplementierungen und Testanwendungen zurückgreifen, um den Aufwand für die Integration des Online-Validierungsverfahrens in den bestehenden Buchungsprozess zu reduzieren. Deren Quellcodes werden auf GitHub unter der Apache-2.0-Lizenz veröffentlicht.³⁵

Die konkrete Datenverarbeitung durch Validierungsdienste ist nicht vom Prüfgegenstand umfasst. Die Validierungsdienste sind für die eigene Datenverarbeitung im Rahmen der Gültigkeitsprüfung und Übermittlung der Ergebnisse verantwortlich. Entsprechendes gilt für die Datenverarbeitung durch Leistungsanbieter.

5.6 Datenflüsse und Prozesse

Nachfolgend werden die Datenflüsse und Prozesse bei der Nutzung der verschiedenen Funktionen der CWA App dargestellt.

³⁴ Der regulatorische und technische Rahmen des EU-Gateways wird in der DCC-VO und in den Interoperabilitätsrichtlinien des eHealth-Netzwerk festgelegt. Das EU-Gateway verarbeitet keine personenbezogenen Daten von CWA-Nutzern oder Zertifikatsinhabern.

³⁵ <https://github.com/eu-digital-green-certificates/dgca-validation-service> (Validierungsdienst); für Leistungsanbieter: <https://github.com/eu-digital-green-certificates/dgca-validation-decorator> (Validation Decorator, fungiert als Bindeglied zwischen Buchungssystem und Validierungsdienst).

5.6.1 Risiko-Ermittlung

Bei aktiver Risiko-Ermittlung werden bei Begegnungen von Personen mit aktiviertem ENF zufällige, fortlaufend wechselnde Kennungen (sog. Entfernungsschlüssel, 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 regelmäßig die aktuellen Positivschlüssel- und Check-in-Pakete vom CDN-Magenta über das Internet (Schritt 2) herunter. Die empfangenen RPIs werden mit den heruntergeladenen Positivschlüsseln und die heruntergeladenen Check-ins mit den vom CWA-Nutzer durchgeföhrten Check-ins abgeglichen (Matching) (Schritt 3). Die von Nutzern anderer nationaler Corona-Apps für die länderübergreifende Warnung zur Verfügung gestellten Positivschlüssel sind Bestandteil der Positivschlüssel-Pakete und werden beim Matching daher berücksichtigt.

5.6.1.1 Schritt 1: Begegnungsaufzeichnung

Der Austausch von RPIs des CWA-Nutzers mit Smartphones von anderen Nutzern im Rahmen der Begegnungsaufzeichnung erfordert die Aktivierung der Risiko-Ermittlung in der CWA App und die Aktivierung des ENF auf Ebene des Betriebssystems. Zudem muss die Bluetooth-Schnittstelle aktiviert sein.

Die nachfolgend dargestellten Datenflüsse und Prozesse der Begegnungsaufzeichnung finden nicht in der CWA App, sondern auf Ebene des Betriebssystems im ENF statt.

Für die Begegnungsaufzeichnung verwendet das ENF zwei Datenstrukturen:

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

Der Tagesschlüssel ist ein Zufalls Wert, der in der Regel einmal täglich vom ENF generiert und gespeichert wird. Aus dem Tagesschlüssel wird vom ENF alle 10 bis 20 Minuten ein neuer RPI abgeleitet.

Der jeweils zuletzt abgeleitete RPI wird vom ENF mittels BLE je nach Gerät ca. alle fünf Minuten für zwei bis vier Sekunden versendet. Gleichzeitig empfängt das ENF die auf diese Weise von anderen Smartphones ausgesendeten RPIs. Dieser Austausch der RPIs erfolgt zwischen allen Smartphones mit aktiviertem ENF und unabhängig davon, welche Corona-App installiert ist.

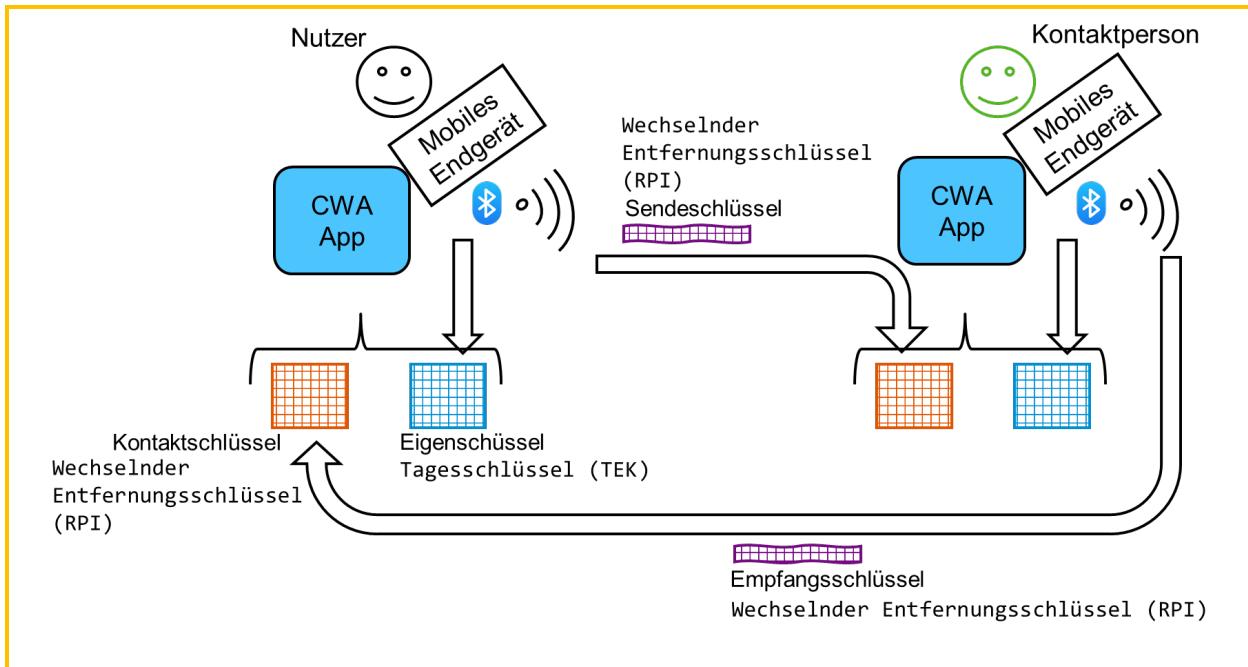


Abbildung 11: Austausch von RPIs

Um die lokale Risikobewertung nach dem Austausch von RPIs im Rahmen der Risiko-Ermittlung (Anwendungsphase 2) zu ermöglichen, werden zu den aufgezeichneten RPI jeweils der Tag der Begegnung sowie technische Metainformationen zur Bluetooth-Sendeleistung und Empfangsstärke gespeichert, die Rückschlüsse auf den Tag, die Dauer und zum Abstand der jeweiligen Begegnung ermöglichen und auf deren Basis später, sollte in Schritt 3 festgestellt werden, dass eine Begegnung mit einer Corona-positiv getesteten Person stattgefunden hat, die RPI-Metadaten (ENF V1) (siehe Abschnitt 5.7.4) bzw. Exposure-Window-Daten (ENF V2) (siehe Abschnitt 5.7.4) erzeugt werden.

5.6.1.2 Schritt 2: Download der Warnungen

5.6.1.2.1 Bluetooth-basierte Warnungen

Warnungen an CWA-Nutzer, die per Bluetooth die RPI des warnenden Nutzers empfangen haben, werden in Gestalt der Positivschlüssel des warnenden Nutzers bereitgestellt. Der Download der aktuellen Positivschlüssel-Pakete eines warnenden Nutzers findet unter den gleichen Voraussetzungen wie Schritt 1 statt, zusätzlich muss eine Internetverbindung bestehen.

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

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

Die Positivschlüssel werden in stündlich zusammengestellte Stundenpakete zusammengefasst, um CWA-Nutzer möglichst schnell zu warnen. Die Stundenpakete enthalten stets eine Mindestanzahl von derzeit 140 Positivschlüsseln, um eine Re-Identifizierung zu erschweren.

Die CWA App ruft bei aktiver Hintergrundaktualisierung und WLAN-Verbindung mehrmals täglich von dem CDN-Magenta das aktuelle Positivschlüssel-Paket ab, das die Positivschlüssel aller Nutzer enthält, die in den letzten 14 Tagen über eine nationale Corona-App eine Warnung ausgelöst haben (**Positivschlüssel-Paket**). Steht keine WLAN-Verbindung zur Verfügung werden dennoch einmal täglich die aktuellen Positivschlüssel an die CWA-Nutzer übermittelt. Bei deaktivierter Hintergrundaktualisierung werden die Positivschlüssel-Pakete bei jeder manuellen Aktualisierung des Risikowerts geladen.

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), die aktuellen Coronastatistik-Daten sowie die Value Sets und Business Rules von dem CDN-Magenta geladen.

Sämtliche Daten des CDN-Magenta werden über eine verschlüsselte Verbindung bereitgestellt und durch das CDN-Magenta signiert. Die Signatur wird nach jedem Laden in der CWA App auf Echtheit geprüft.

5.6.1.2.2 Warnungen von eingecheckten CWA-Nutzern

Warnungen von einem anderen CWA-Nutzer, der zur gleichen Zeit wie der CWA-Nutzer bei einem Event eingecheckt war, werden als sogenannte Check-ins übermittelt und die aktive Risiko-Ermittlung und eine Internetverbindung voraus.

Die Funktionsweise ist mit derjenigen von Bluetooth-basierten Warnungen vergleichbar. Die CWA App ruft bei aktiver Hintergrundaktualisierung ständig von dem CDN-Magenta eine Liste mit den Check-ins aller CWA-Nutzer ab, die diese innerhalb der letzten Stunde über die CWA App geteilt haben (**Check-in-Paket**). Falls kein CWA-Nutzer in dieser Zeit seine Check-ins geteilt hat, kann das Check-in-Paket auch keine Check-ins enthalten. Check-in-Pakete werden jeweils 15 Tage zum Download bereitgestellt und anschließend gelöscht. Jedes Check-in-Paket hat eine eindeutige 6-stellige Zahl als Dateinamen, der aus der aktuellen Unixzeit abgeleitet wird (z. B. 448188). Dieser Name des Pakets wird auch dafür verwendet, um festzustellen ob und wann ein Paket gelöscht werden muss.

Jedes nichtleere Check-in-Paket enthält neben den echten auch eine zufällige Zahl von durch den CWA Server hinzugefügten falschen Check-ins des warnenden CWA-Nutzers (Fake Check-ins), um das Re-Identifizierungsrisiko für diesen durch Verkettung von mehreren Check-in-Paketen zu reduzieren.

5.6.1.2.3 In Vertretung warnen

Wenn ein Gesundheitsamt im Rahmen seiner Kontaktnachverfolgungsmaßnahmen erfährt, dass eine positiv getestete Person ein bestimmtes, in der CWA App angelegtes Event besucht hat und diese positiv getestete Person aber keine Warnung über die CWA App auslösen kann (z. B. weil sie kein CWA-Nutzer ist oder sich nicht bei dem Event eingecheckt hat), kann das Gesundheitsamt den Veranstalter ansprechen und ihm eine PIW-TAN und ggf. die Aufenthaltsdauer des positiv getesteten Gastes mitteilen. Die PIW-TAN erhält das Gesundheitsamt von der Verifikations-Hotline, welches diese vom Portalserver anfordert.

Der CWA Server bietet für die Funktion „In Vertretung warnen“ einen eigenen Endpunkt an, an den die CWA Apps die Vertreterwarnungen in Form von Check-in-Paketen übermitteln. Die Check-in-Pakete entsprechen inhaltlich den „normalen“ Check-in-Paketen, die bei Warnungen von eingekochten CWA-Nutzern übermittelt werden.

5.6.1.3 Schritt 3: Matching

5.6.1.3.1 Bluetooth-basierte Warnungen

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.

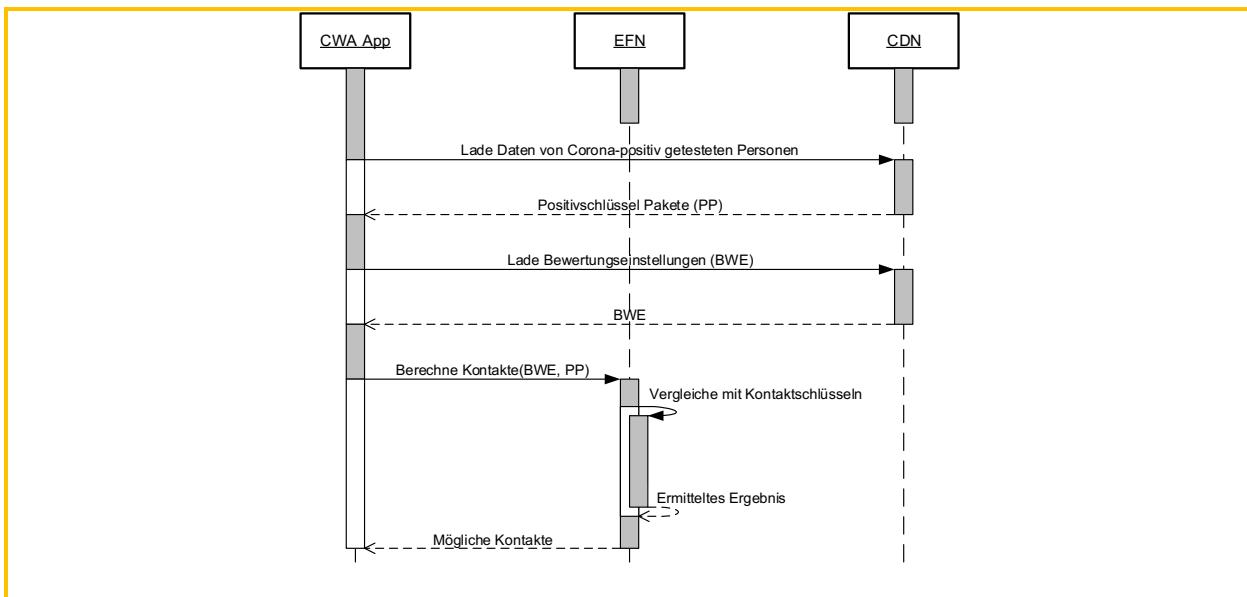


Abbildung 12: Laden der Positivschlüssel-Pakete und Ermittlung möglicher Kontakte

5.6.1.3.2 Warnungen von eingetragenen CWA-Nutzern

Das Matching von Warnungen eingetragener CWA-Nutzer findet unter der Voraussetzung statt, dass der CWA-Nutzer die Risiko-Ermittlung aktiviert hat. Da die Event-Registrierung unabhängig vom ENF funktioniert, kann das ENF jedoch deaktiviert sein. Das Matching wird lokal in der CWA App durch Abgleich der heruntergeladenen Check-ins mit den gespeicherten Check-in-Daten des CWA-Nutzers durchgeführt. Sofern Übereinstimmungen vorliegen, werden diese in einer Datenbank (TraceTimeIntervalMatches) gespeichert.

5.6.1.3.3 In Vertretung warnen

Das Vorgehen beim Matching von Warnungen, die mit „In Vertretung warnen“ ausgelöst werden, ist mit dem Vorgehen beim Matching von Warnungen von eingetragenen CWA-Nutzern identisch. Daher kann auf Abschnitt 5.6.1.3.2 entsprechend verwiesen werden.

5.6.2 Berechnung des Infektionsrisikos

Wenn in Schritt 3 der Anwendungsphase 1 ein Match festgestellt wird, übergibt das ENF die mit den betreffenden RPIs im ENF aufgezeichneten RPI-Metadaten (ENF V1) (siehe Ziffer 5.7.4) bzw. Exposure-Window-Daten (ENF V2) (siehe Ziffer 5.7.4) an die CWA App. Die RPI-Metadaten bzw. Exposure-Window-Daten werden von der CWA App nach Maßgabe der BWE (siehe Ziffer 5.7.4) ausgewertet, um das Infektionsrisiko (Total Risk Score) für den CWA-Nutzer zu berechnen.

Im Fall eines Matches von Event-Daten werden die in der TraceTimeIntervalMatches-Datenbank gespeicherten Daten von der CWA App selbst in die Struktur von entsprechenden Exposure-Window-Daten umgewandelt.

Die Berechnung des Infektionsrisikos findet lokal statt. Das ermittelte Infektionsrisikos 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 das ermittelte Infektionsrisiko schließlich auf dem Home-Bildschirm in Form eines dreistufigen Risikostatus (z. B. „erhöhtes Risiko“) an. Zudem werden dem CWA-Nutzer Handlungsempfehlungen des RKI, basierend auf dem zuletzt ermittelten Risikostatus, angezeigt.

5.6.3 Testregistrierung

Im Fall eines durchgeföhrten eigenen oder des Corona-Tests eines Familienmitglieds kann der CWA-Nutzer über die CWA App den Testinformationsprozess starten und damit über das Testergebnis durch die CWA App benachrichtigt werden. Zudem kann der CWA-Nutzer für den Fall eines negativen Testergebnisses die Ausstellung eines Testzertifikats anfordern.

PCR-Tests werden durch Ärzte oder Testzentren durchgeführt und an das jeweils angeschlossene Labor weitergegeben. Antigen-Schnelltest werden von Teststellen durchgeführt. Von den Laboren und Teststellen werden die Testergebnisse auf den zentralen Test Result Server übertragen und können vom CWA-Nutzer über die CWA App vom Server abgerufen werden, sofern die Testpersonen 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 anlässlich der Einwilligung übergebenen Kennung in Form eines QR-Codes und einem technischen Verifikationsverfahren eingerichtet.

Bei Durchführung eines PCR-Tests erhält die getestete Person im ersten Schritt dazu bei der Stelle, die den Test durchführt, z. B. in der ärztlichen Praxis, ein Informationsblatt, auf dem dieses Verfahren beschrieben ist. Zu dem Informationsblatt erhält die getestete Person einen QR-Code, der mit Hilfe der CWA App eingescannt werden kann. Die getestete Person entscheidet sodann gegenüber der Stelle, die den Test durchführt, ob sie 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.

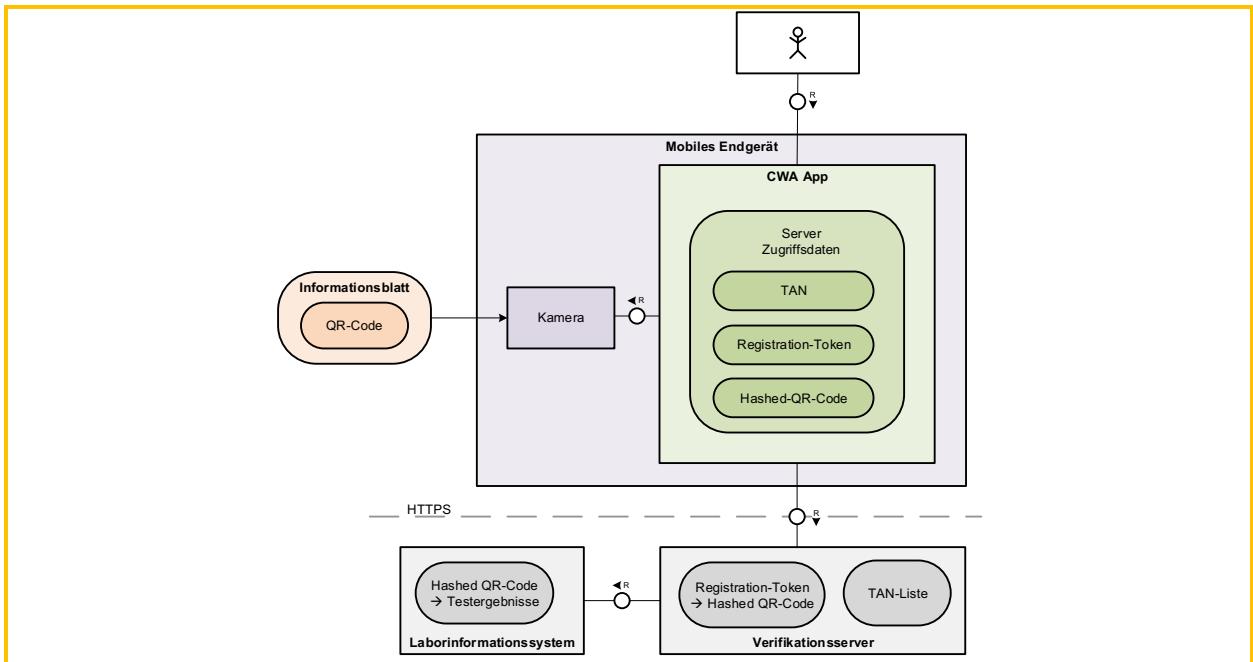


Abbildung 13: Zusammenspiel von QR-Code und Testergebnis über die CWA App

Bei Durchführung eines Antigen-Schnelltests entscheidet die getestete Person, ob sie der Übermittlung des Schnelltest-Ergebnisses an den Test Result Server zum Zweck des späteren Abrufs über die CWA App zustimmt. Die Einwilligung wird im Teststellen-System eingetragen. Zusätzlich entscheidet sie, ob sie eine namentliche Anzeige des Schnelltest-Ergebnisses in der CWA App wünscht (namentlicher Testnachweis). Die Teststelle generiert sodann einen individuellen QR-Code oder Link und stellt der getesteten Person diesen zur Verfügung. Wenn die getestete Person eine nicht-namentliche Anzeige wünscht, sind in dem QR-Code nur die GUID sowie der Testzeitpunkt kodiert. Wenn die getestete Person die namentliche Anzeige wünscht, sind zusätzlich der Vor-, Nachname und das Geburtsdatum im QR-Code enthalten, wie von der getesteten Person gegenüber der Teststelle angegeben. Der CWA-Nutzer kann den QR-Code mit der CWA App einscannen. Zuvor wird er gefragt, ob es sich um einen eigenen oder den Test eines Dritten handelt. Im letzteren Fall muss er einen (beliebigen) Namen eingeben, unter dem der Test in der CWA App verwaltet wird. Die aus dem QR-Code ausgelesenen Daten werden in der CWA App gespeichert.

Vor dem Einscannen des QR-Codes zu einem eigenen Test willigt der CWA-Nutzer in die Datenverarbeitung in Zusammenhang mit dem Verfahren ein. Der CWA-Nutzer authentifiziert sich – ohne dass Angaben zu seiner Person übermittelt werden – unter Verwendung des QR-Codes und der darin enthaltenen GUID bei dem Verifikationsserver.

Die CWA App berechnet hierfür den Hash der GUID. Im Fall eines PCR-Tests wird zudem ein zweiter Hash berechnet, der auf der GUID und zusätzlich auf dem in der CWA App im Rahmen der Anforderung des Testzertifikats vom CWA-Nutzer eingegebenen Geburtsdatum basiert. Der bzw. die Hash-Werte werden dann an den Verifikationsserver gesendet und von diesem dem Test Result Server bekannt gegeben. Der Test Result Server verwendet die Hash-Werte dann zur internen Ablage der (noch nicht vorliegenden) Testergebnisse.

Die Verwendung eines zweiten Hash für PCR-Tests ist erforderlich, da der QR-Code, in dem die GUID enthalten ist, auf dem Probenbegleitschein aufgedruckt ist, so dass nicht kontrolliert

werden kann, dass der QR-Code tatsächlich nur einmal ausgegeben wird (z. B. könnte der Probenbegleitschein mit dem QR-Code kopiert und somit an mehrere CWA-Nutzer ausgegeben werden). Die Verwendung eines zweiten Hash-Wertes verhindert somit die Ausgabe von falschen Testzertifikaten, die sich auf ein nicht dem CWA-Nutzer gehörendes Testergebnis beziehen. Da bei Schnelltests die QR-Codes von den Teststellen individuell für den CWA-Nutzer in einer kontrollierten Systemumgebung erzeugt werden, besteht bei Schnelltests keine Notwendigkeit für diese Maßnahme.

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 die dem Registration Token zugeordneten Hash-Werte ermittelt und den zugehörigen Teststatus vom Test Result Server abfragt und dessen Antwort dann an die CWA App zurückgibt. Der CWA-Nutzer kann diesen Vorgang so oft wiederholen, bis ein endgültiges Ergebnis feststeht.

Wenn das Testergebnis feststeht, wird der CWA-Nutzer per Mitteilung (sofern die CWA App hierzu berechtigt und entsprechend konfiguriert worden ist) auf das Vorliegen des Testergebnisses hingewiesen. Dieses wird dann in der geöffneten CWA App angezeigt. Wenn der CWA-Nutzer ein negatives Testergebnis zu einem Schnelltest erhalten hat und gegenüber der Teststelle seine Einwilligung in die namentliche Anzeige des Testergebnisses erteilt hat, kann er zudem die Detailansicht als namentlichen Schnelltest-Nachweis aufrufen (namentlicher Testnachweis siehe Abschnitt 5.4.9).

Falls der CWA-Nutzer ein Testzertifikat angefordert hat, wird dieses von der CWA App angefordert (siehe Abschnitt 5.6.12.3).

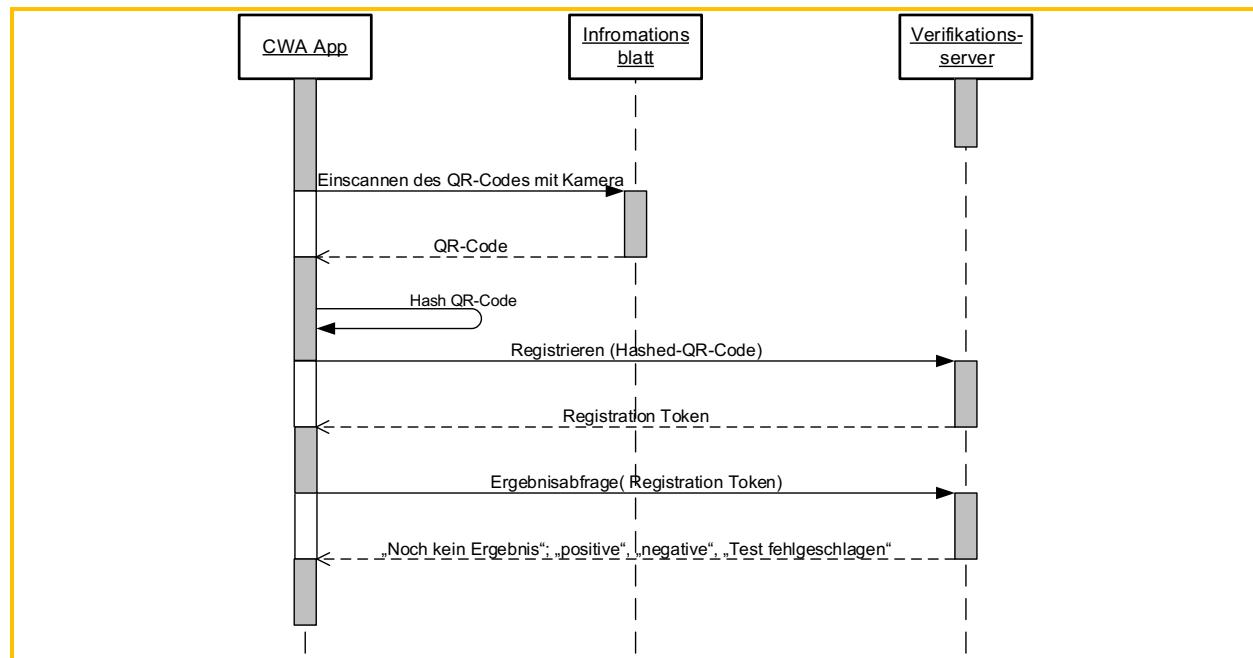


Abbildung 14: Einscannen des QR-Codes, Testregistrierung und Testergebnisabfrage

Falls das abgerufene eigene Testergebnis positiv ist, wird eine TAN vom Verifikationsserver angefragt. 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).

5.6.4 Verifikations-Hotline

Die Hotline steht CWA-Nutzern zur Verfügung, die die Risiko-Ermittlung genutzt und ein positives Ergebnis eines PCR-Tests erhalten haben, denen die Testregistrierung jedoch nicht zur Verfügung steht. Daneben steht die Hotline auch den Mitarbeitern von Gesundheitsämtern zur Verfügung, die eine PIW-TAN für die Funktion „In Vertretung warnen“ anfordern möchten.

Für CWA-Nutzer, die ein positives Ergebnis eines Schnelltests erhalten haben, steht die Verifikations-Hotline nicht zur Verfügung. 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 bzw. Gesundheitsamts-Mitarbeiter durch einen speziell geschulten Mitarbeiter der Hotline gemäß einem Skript Plausibilitätsfragen gestellt. Die Antworten werden nicht gespeichert. Wenn der Mitarbeiter der Hotline die Antworten für schlüssig hält und den Anrufer somit als einen positiv getesteten CWA-Nutzer bzw. Gesundheitsamts-Mitarbeiter verifiziert, erfragt er beim Anrufer eine Telefonnummer und den Namen für einen Rückruf. Danach beendet der Mitarbeiter der Verifikations-Hotline das Telefonat, um über die Weboberfläche des Portalservers eine teleTAN bzw. PIW-TAN abzufragen.

Der Portal Server verbindet sich mit dem Verifikationsserver, der die teleTAN bzw. PIW-TAN generiert. Der Hashwert der teleTAN bzw. PIW-TAN wird auf dem Verifikationsserver gespeichert, die teleTAN bzw. PIW-TAN wird im Klartext an den Portal Server zurückgegeben und von dort über die Weboberfläche dem Mitarbeiter der Hotline zur Verfügung gestellt. Die teleTAN bzw. PIW-TAN wird dem positiv getesteten CWA-Nutzer bzw. Gesundheitsamts-Mitarbeiter 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 und PIW-TAN haben jeweils eine Gültigkeit von einer Stunde.

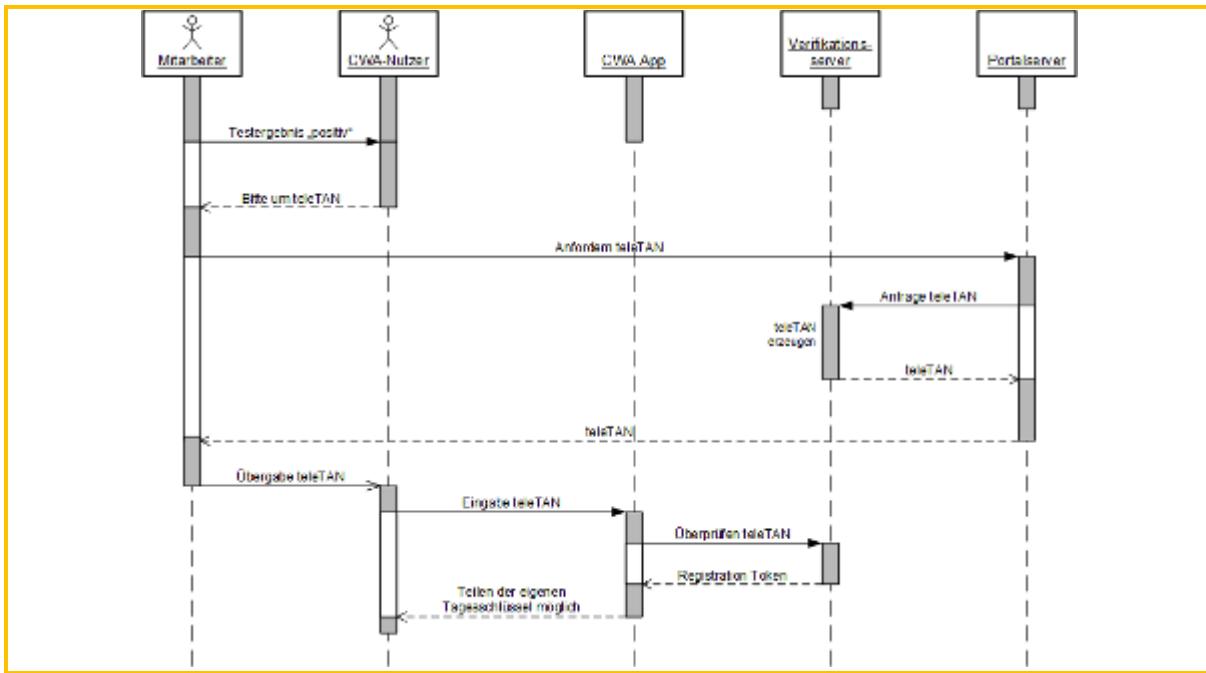


Abbildung 15: Abfrage teleTAN

5.6.5 Auslösen einer Warnung

Nach dem Abruf eines eigenen positiven Testergebnisses in der CWA App oder Eingabe einer gültigen teleTAN (nur bei PCR-Testergebnissen) kann ein positiv getesteter CWA-Nutzer seine Tagesschlüssel und ggf. Check-ins übermitteln, damit andere Nutzer gewarnt werden können.

Solange ein CWA-Nutzer innerhalb von vier Stunden nach dem Abruf eines positiven Testergebnisses in der CWA App keine Warnung auslöst, wird er von der CWA App erstmals nach zwei Stunden und letztmalig nach vier Stunden mit einer Mitteilung an das Teilen seines Testergebnisses erinnert (Erinnerungsfunktion). Voraussetzung ist, dass die CWA App zum Versand von Mitteilungen berechtigt ist (siehe Ziffer 5.4.15.3). Die Mitteilung wird direkt auf dem Bildschirm des Smartphones angezeigt, auch bei Gebrauch anderer Programme bzw. auf dem Sperrbildschirm.³⁶

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 Warnung ausdrücklich einwilligen.

³⁶ Screenshot zur Erinnerungsfunktion siehe Ziffer 5.4.8, dort Abb. 6.

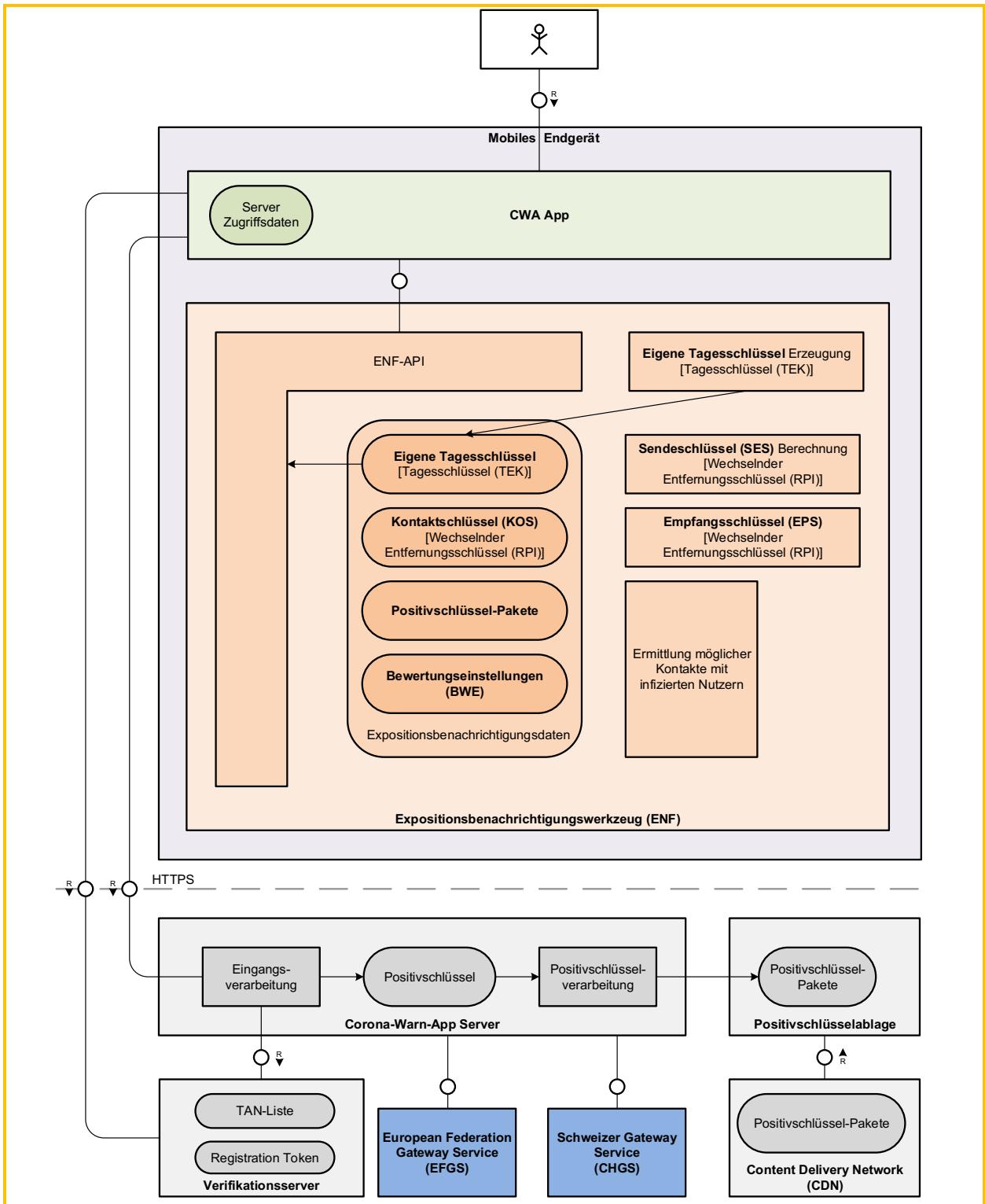


Abbildung 16: Die CWA App übergibt die TAN und die Eigenschlüssel an den CWA Server

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. 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.

Sofern der CWA-Nutzer seine Einwilligung in die Übermittlung der Tagesschlüssel bzw. Check-ins (einschließlich der etwaigen zusätzlichen Angaben zum Symptombeginn) erklärt hat und die erforderliche Systemfreigabe erteilt hat (entweder im Rahmen der initialen Einwilligung bei der Abfrage des Testergebnisses, sofern diese nicht länger als fünf Tage zurückliegt oder unmittelbar im Zusammenhang mit dem Erhalt des Testergebnisses), fordert die CWA App vom ENF die Tagesschlüssel der letzten 14 Tage an (sofern das ENF aktiviert ist).

Die CWA App setzt sodann jeweils einen Zahlenwert von 0 bis 8 in das Datenfeld „TransmissionRiskLevel“ (TRL) der vom ENF erhaltenen Tagesschlüssel und der ggf. lokal gespeicherten Check-ins. Dieser Zahlenwert wird nach Maßgabe der aktuell in der CWA App hinterlegten BWE ermittelt 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 TRL-Wert der 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. Zudem wird jeder Tagesschlüssel um das Datum DaysSinceOnsetOfSymptoms (DSOS) ergänzt, das auf Basis der Angaben zum Symptombeginn bestimmt wird. Bei Check-ins, die über die Funktion „In Vertretung warnen“ übermittelt werden, wird standardmäßig der Wert 5 in das Datenfeld TRL gesetzt.

Die so bearbeiteten Tagesschlüssel und Check-ins 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 und Check-ins frei. Im weiteren Verfahren generiert der CWA Server aus von allen positiv getesteten CWA-Nutzern übermittelten Positivschlüsseln und Check-ins die entsprechenden Paketdaten (Positivschlüssel-Pakete und Check-in-Pakete) und übergibt diese – im Fall der Positivschlüssel-Pakete gemeinsam mit den über das EFGS und CHGS zur Verfügung gestellten Positivschlüsseln der Nutzer anderer nationaler Corona-Apps – dem CDN-Magenta.

Prozesse bei Tagesschlüsseln:

Da der am Übermittlungstag verwendete Tagesschlüssel vom ENF V1 nicht an die CWA App weitergegeben wird, wird dieser in einem zweiten Schritt am nächsten Tag von der CWA App beim ENF V1 angefordert und mit dem entsprechend gesetzten TRL-Wert und der TAN an den CWA Server nachträglich übermittelt. Dieser Prozess findet im Hintergrund statt. Ab Release 1.8 der CWA App, die das ENF V2 verwendet, wird jedoch auch der am Übermittlungstag verwendete Tagesschlüssel vom ENF V2 an die CWA App weitergegeben, so dass der bisher notwendige zweite Schritt am nächsten Tag entfällt.

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.

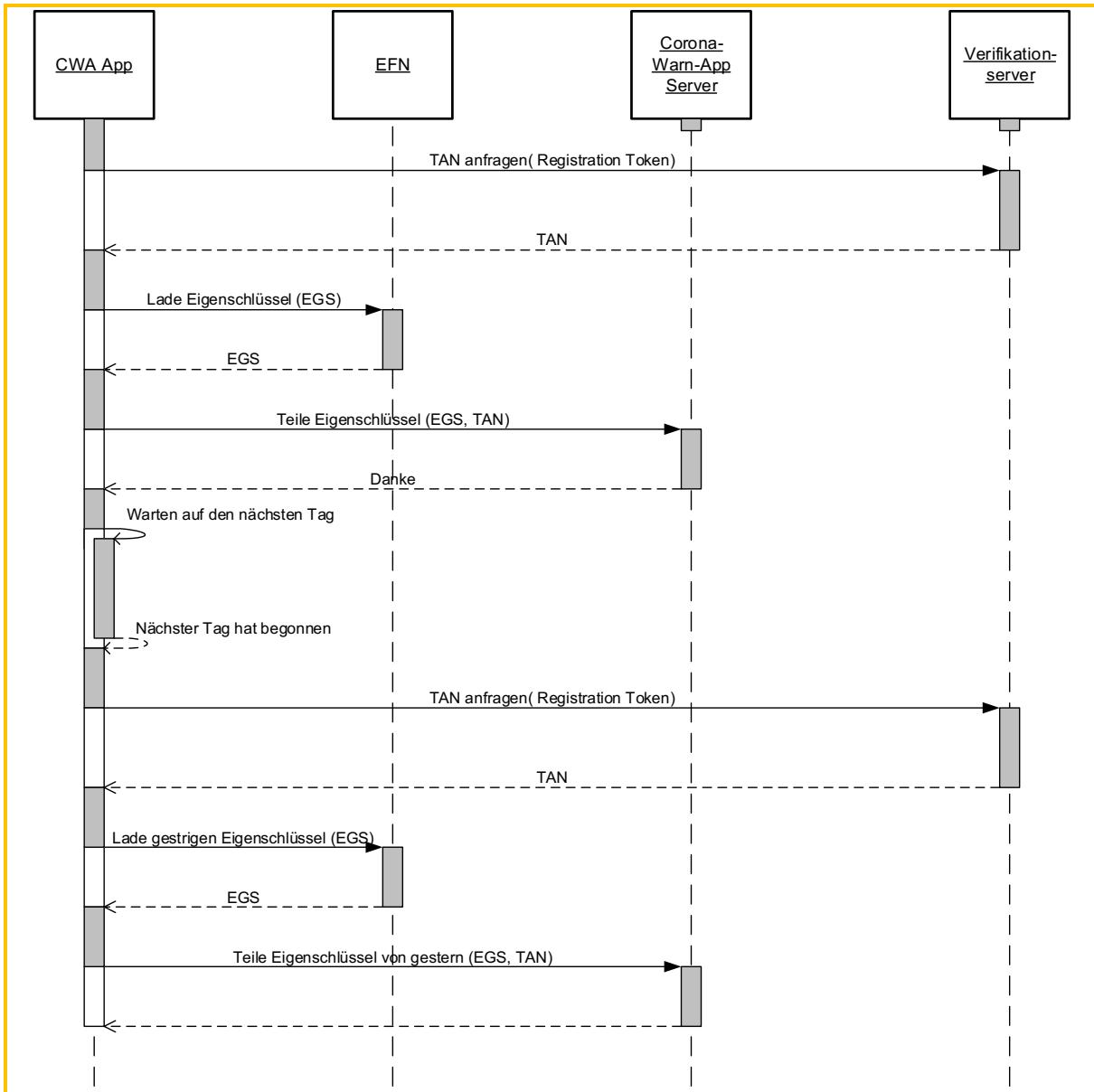


Abbildung 17: Ablauf beim Bereitstellen der Eigenschlüssel durch hochladen auf den CWA Server

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 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. Die Metadaten zu Positivschlüsseln dienen auch der

Gewährleistung der Abwärtskompatibilität der CWA App. 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 und CHGS stehen die standardisierten Daten dann für diese Server der einzelnen nationalen Corona-Apps zur Verfügung.

Die Server der einzelnen nationalen Corona-Apps berechnen aus dem DSOS-Wert und der Angabe zum ReportType unter Verwendung ihrer eigenen nationalen BWE den TRL-Wert jedes Positivschlüssels. Die Positivschlüssel der anderen nationalen Corona-Apps können dadurch mit den Positivschlüsseln der eigenen Nutzer der jeweiligen nationalen Corona-Apps vergleichbar gemacht und somit im Rahmen der Risiko-Ermittlung auf gleiche Weise berücksichtigt werden.

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

Im EFGS zur Verfügung stehende Positivschlüssel der CWA-Nutzer stehen den Verantwortlichen der am EFGS teilnehmenden 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 anhand des Länder-Werts jeweils entscheiden, ob und in welcher Weise sie die Positivschlüssel der Nutzer einer bestimmten 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).

Entsprechendes gilt in Bezug auf den CHGS. Die im CHGS zur Verfügung stehenden Positivschlüssel der CWA-Nutzer werden allerdings nur mit dem BAG als Verantwortlichen für die Schweizer Corona-App geteilt, und die dort bereitgestellten Positivschlüssel von Nutzern der Schweizer Corona-App werden nur mit dem RKI geteilt, d. h. der CWA Server stellt die Positivschlüssel von Schweizer Nutzern nicht dem EFGS zur Verfügung. So wie im Fall des EFGS kann der CWA-Nutzer keine gesonderte Freigabe nur für die Schweizer Corona-App erteilen oder diese als Zielland der auszulösenden Warnung ausnehmen.

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 gemeinsamen Verantwortlichen geprüft. Entsprechend wird hinsichtlich der am CHGS abgerufenen Positivschlüssel verfahren, wobei sich die gemeinsame Koordination und Prüfung auf RKI und BAG als gemeinsame Verantwortliche für die Datenverarbeitung durch das CHGS beschränkt.

Prozesse bei Check-ins:

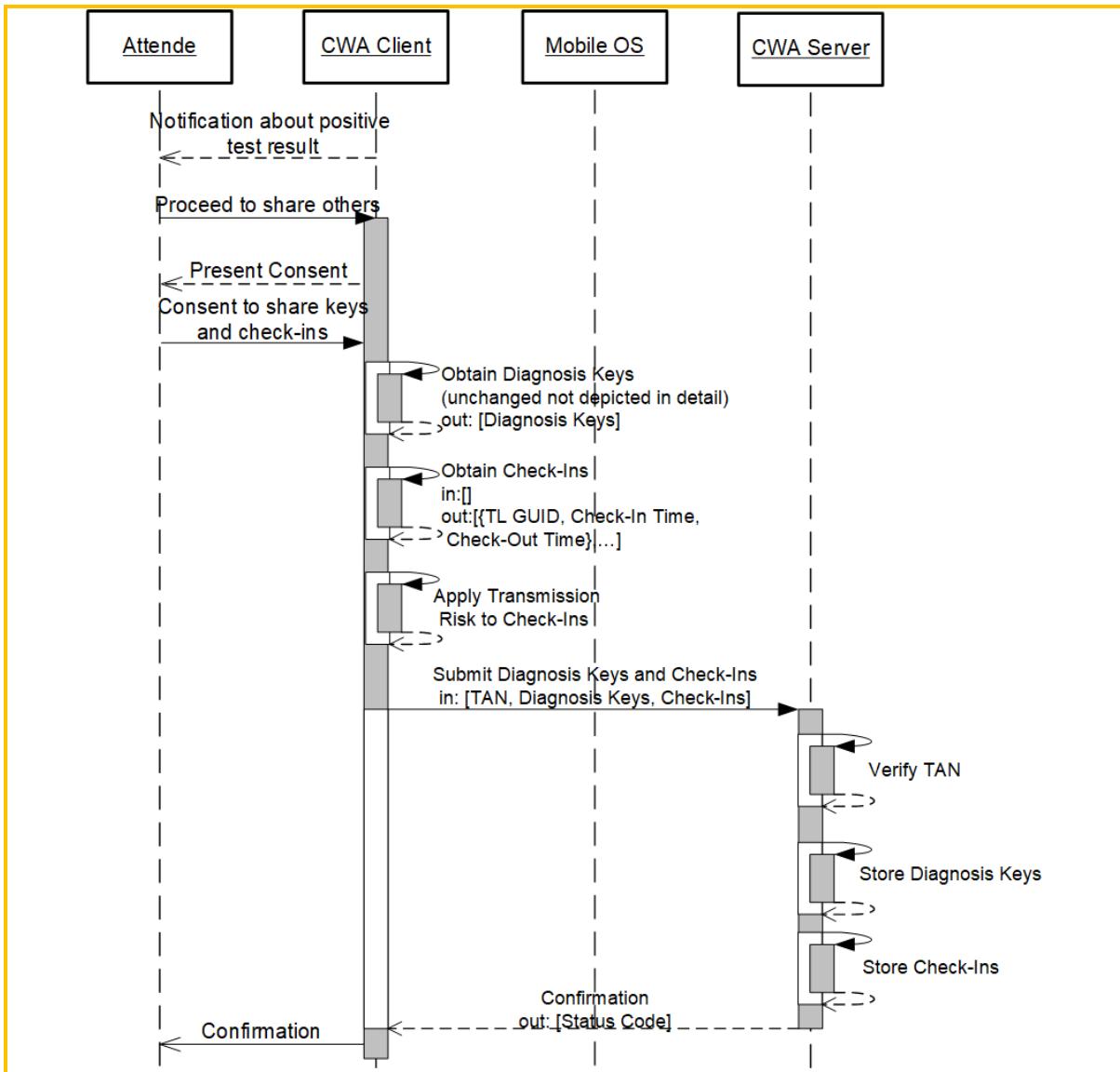


Abbildung 18: Ablauf beim Bereitstellen der Check-ins

Die Check-ins wurden vom CWA Server bei Übermittlungen durch CWA Apps bis Release 2.7 wie folgt verarbeitet:

1. Validierung des Payloads
2. Validierung der Check-ins
3. Filterung nach Transmission Risk Level

4. Herausfiltern von veralteten Check-ins
5. Herausfiltern von zukünftigen Check-ins
6. Anpassung von aktuell gültigen Check-ins
7. Überprüfung der Check-in Plausibilität
8. Erzeugung von Fake Check-ins
9. Speicherung als TraceTimeIntervalWarning

Seit Release 2.8 der CWA App werden die Check-ins verschlüsselt in Gestalt der CheckInProtectedReports übermittelt. Der CWA Server kann die Check-ins dann nicht mehr lesen, so dass die Schritte 3 bis 7 entfallen. Hintergrund für diese Maßnahme sind gegenüber dem RKI geäußerte rechtliche Bedenken auf Seiten von Apple, wonach die Übermittlung von unverschlüsselten Check-ins an das RKI als ein Verstoß gegen die Nutzungsbedingungen für das ENF angesehen werden könnte. Im Sinne einer pragmatischen, schnellen Erledigung der aufgeworfenen Bedenken hat das RKI die Verwendung der verschlüsselten CheckInProtectedReports vorgeschlagen, womit Apple einverstanden war.

5.6.6 Verwenden des Kontakt-Tagebuchs

Wenn der CWA-Nutzer das Kontakt-Tagebuch nutzt, werden seine **Kontakt-Tagebuch-Einträge** lokal im Speicher der CWA App in einer SQL-Datenbank gespeichert. Das RKI hat keinen Zugriff auf die Kontakt-Tagebuch-Einträge. Im Fall von Android-Smartphones erfolgt die Speicherung in der durch das Betriebssystem verschlüsselten „Application Sandbox“ und im Fall von iPhones in der „App Sandbox“ von iOS unter Verschlüsselung durch SQLite.

Die Export-Funktion des Kontakt-Tagebuchs greift auf die reguläre Teilen-Systemfunktion des Betriebssystems zu, um die Kontakt-Tagebuch-Einträge der letzten 14 Tage über das Teilen-Systemmenü im einfachen Textformat an andere Apps auf dem Smartphone übergeben zu können. Da die Festlegung der für den Export verfügbaren Apps vom Betriebssystem in Abhängigkeit vom Exportformat vorgenommen wird, kann der CWA-Nutzer seine Kontakt-Tagebuch-Einträge mit den installierten Apps teilen, die ein Textformat verarbeiten können. Die Liste der Kontakt-Tagebuch-Einträge in Textform kann vom CWA-Nutzer bearbeitet werden. Die exportierte Liste der Kontakt-Tagebuch-Einträge wird automatisch um die eine Überschrift und einen Hinweis ergänzt:

„Kontakte der letzten 14 Tage (Zeitraum) - Die nachfolgende Liste dient dem zuständigen Gesundheitsamt zur Kontaktnachverfolgung gem. § 25 IfSG“

Im Hinblick auf die Begegnungshistorie erfolgt keine zusätzliche Datenverarbeitung. Es handelt sich nur um eine zusätzliche Darstellung der ermittelten Risikobegegnungen und Begegnungen mit niedrigem Risiko in der Kalenderansicht des Kontakt-Tagebuchs.

5.6.7 Event-Registrierung

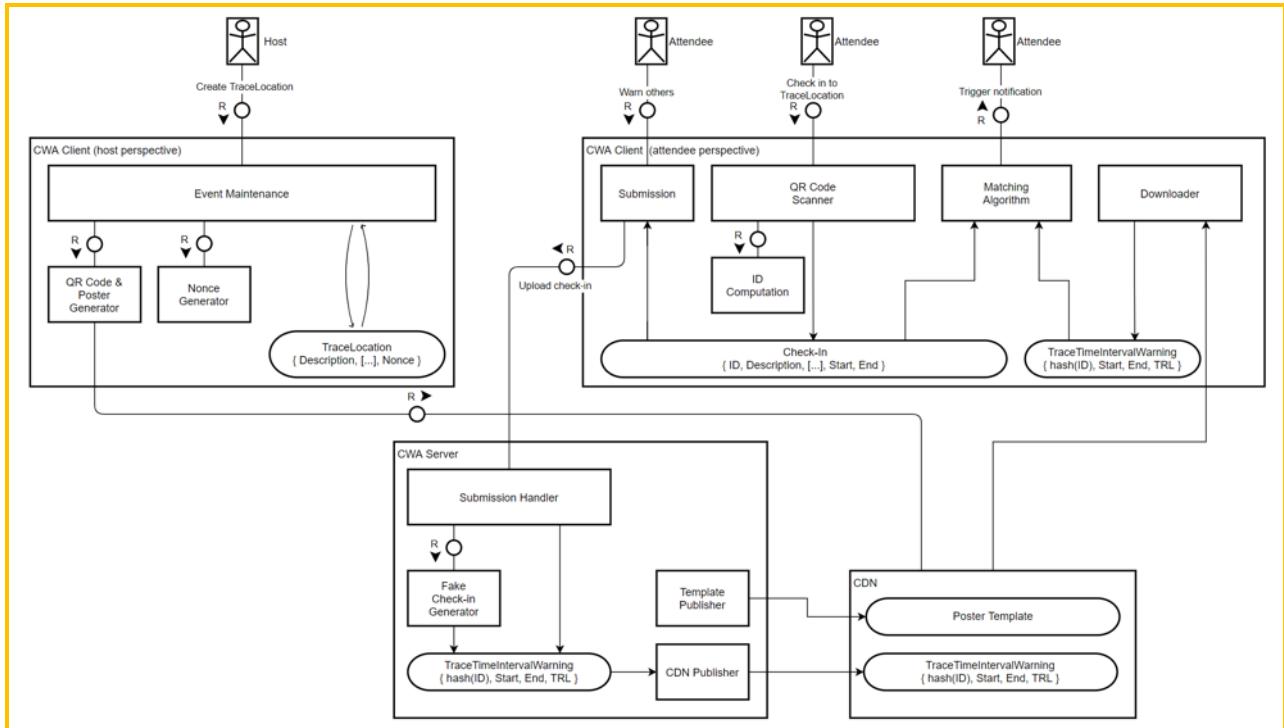


Abbildung 19: Ablaufübersicht Event-Registrierung

5.6.7.1 Anlegen eines Events (als Veranstalter)

Das Anlegen eines Events dient der Erstellung eines QR-Codes mit kodierten Event-Details, der von den Gästen des CWA-Nutzers eingescannt werden kann (Einchecken). Die Erstellung des QR-Codes erfolgt lokal in der CWA App.

Beim Anlegen eines Events werden die vom CWA-Nutzer (Veranstalter) eingegebenen und von der CWA App erzeugten Event-Details in einer eigenen Datenbanktabelle („TraceLocations“) gespeichert.

5.6.7.2 Ein- und Auschecken bei Events (als Gast)

Der CWA-Nutzer checkt sich – ohne Angaben zu seiner Person zu machen – durch Einscannen des vom Veranstalter bereitgestellten QR-Codes ein. Dabei werden die kodierten Event-Details aus dem QR-Code ausgelesen, dekodiert und zusammen mit den von der CWA App erzeugten weiteren Event-Details in einer Datenbanktabelle gespeichert. Beim (manuellen oder automatischen) Auschecken wird schließlich die Auscheckzeit in Unixzeit hinzugespeichert.

5.6.8 Anlegen eines Schnelltest-Profil

Wenn der CWA-Nutzer ein Schnelltest-Profil anlegt, werden seine Profilangaben lokal in einer SQLite-Datenbank im Speicher der CWA App verschlüsselt gespeichert. Das RKI hat keinen Zugriff auf das Schnelltest-Profil.

Die Speicherverschlüsselung erfolgt bei Android-Smartphones durch den Sandbox-Mechanismus von Android. Bei iPhones wird hierfür ebenfalls der Sandbox-Mechanismus von iOS sowie eine eigene Anwendungsverschlüsselung der SQLite-Datenbank genutzt.

5.6.9 Fehlerberichte

Wenn der CWA-Nutzer die Aufzeichnung von Fehlerberichten aktiviert, werden die **Anwendungsdaten** in Form von Anwendungslogs lokal im App-Speicher abgelegt. Solange der CWA-Nutzer die Fehlerberichte nicht ausdrücklich aktiv teilt oder sendet, gibt die CWA App die Fehlerberichte weder an das Betriebssystem noch an das RKI oder sonstige Empfänger weiter.

Verwendet der CWA-Nutzer die Funktion „Fehlerbericht senden“, wird von der CWA App bei dem Data Donation Server zunächst ein OTP angefordert (ELS OTP).³⁷ Das ELS OTP wird von der CWA App mit dem Fehlerbericht zu einer Zip-Datei zusammengefasst und diese dann an den Log Storage Server (siehe Abschnitt 5.6.11) übermittelt.

Der CWA Log Storage Server entpackt die Zip-Datei und überprüft zunächst, ob der darin enthaltene Fehlerbericht von einer gültigen CWA App gesendet wurde. Hierzu wird das in der Zip-Datei enthaltene ELS OTP an den Data Donation Server übermittelt. Der Data Donation Server verifiziert, ob es sich bei der Anfrage um eine echte CWA App handelt oder nicht. Dabei werden das ELS OTP und EDUS OTP (siehe Abschnitt 5.6.11) zu jeder Zeit getrennt voneinander gespeichert und verarbeitet. Da keine Verbindung zwischen den OTPs des gleichen CWA-Nutzers besteht, selbst wenn diese zeitgleich verarbeitet werden sollten, kann somit auch nicht festgestellt werden, dass sich die OTPs auf den gleichen CWA-Nutzer beziehen.

Bei erfolgreicher Verifizierung wird der Fehlerbericht auf dem Log Storage Server abgelegt und ihm dort eine Fehlerberichts-ID zugewiesen. Die Fehlerberichts-ID wird an die CWA App übermittelt und im App-Speicher in einer SQL-Datenbank zusammen mit dem Sendedatum des Fehlerberichts gespeichert. Alle gespeicherten Einträge für gesendete Fehlerberichte werden dazu verwendet, um dem CWA-Nutzer eine historische Übersicht aller geteilten Fehlerberichte anzuzeigen. Die Historie der Fehlerberichte in der CWA App kann gelöscht

³⁷ OTPs werden auch für die Echtheitsprüfung im Zusammenhang mit den Einladungen zu Befragungen (EDUS) verwendet (siehe Abschnitt 5.6.11). Zur besseren Unterscheidung werden die OTPs daher je nach Verwendungszusammenhang auch als EDUS OTP oder ELS OTP bezeichnet.

werden, indem die CWA App deinstalliert oder zurückgesetzt wird (Funktion „Anwendung zurücksetzen“).

Über das Webportal des Log Storage Servers können autorisierte Entwickler aus dem Kernentwicklerteam auf Weisung des RKI auf die Fehlerberichte und die Fehlerberichts-ID zugreifen. Zum Zugriff müssen die Mitglieder des Kernentwicklerteams ihre persönlichen Zugangsdaten für das Webportal eingeben. Das Webportal ist so konfiguriert, dass die Analyse der Fehlerberichte nur über das Webportal möglich ist, d. h. eine Speicherung auf dem Client eines Entwicklers oder ein Download der Datei ist nicht möglich.

5.6.10 Datenspende

Sofern der CWA-Nutzer an der Datenspende teilnimmt, werden die Nutzungsdaten sowie die eventuellen optionalen Angaben des CWA-Nutzers

- Altersgruppe (Altersgruppe 1 (bis 30), 2 (31-59), 3 (60 oder älter) oder „keine Angabe“ und
- Region (Bundesland und wahlweise konkrete Angaben zum Kreis bzw. Bezirk oder „keine Angabe“)

an den CWA Data Donation Server übermittelt.

Um zu verhindern, dass die Ergebnisse der Auswertung der im Rahmen der Datenspende erhobenen Nutzungsdaten durch massenhaft übermittelte Daten (z.B. im Rahmen konzertierter Angriffe) beeinträchtigt werden, wird der Verifikations-Dienst (Privacy-preserving Access Control, PPAC) des jeweiligen Betriebssystemherstellers Apple oder Google verwendet. Aufgrund des frei zugänglichen Quellcodes der CWA App wäre es grundsätzlich möglich an der Datenspende auch ohne jede Nutzung der CWA App teilzunehmen. Dritte könnten manipulierte Nutzungsdaten an den CWA Data Donation Server senden und die Zielsetzung der Datenspende vereiteln. Der Einsatz des Verifikations-Dienstes dient somit als risikoreduzierende Maßnahme, indem der jeweilige Hersteller bestätigt, dass die CWA App in einer nicht-manipulierten Umgebung ausgeführt wird. Die Existenz eines im Rahmen des Verifikations-Dienstes erzeugten Tokens erlaubt somit eine Unterscheidung zwischen Datenspenden, die von einer CWA App stammen und solchen, bei denen dies nicht der Fall ist. Anhand des Verifikations-Dienstes wird auch sichergestellt, dass im Rahmen der Datenspende nicht mehrfach dieselben Datenpunkte im gleichen Zeitabschnitt zur Verfügung gestellt werden. Hierfür werden das Datum der Übermittlung und das für einen Monat gültige Token gesondert gespeichert.

Als Verifikations-Dienst kommt unter iOS das DeviceCheck-Framework von Apple und unter Android der Google-Dienst SafetyNet zum Einsatz.

Die Nutzungsdaten werden jeweils ohne identifizierende Merkmale, getrennt von dem Token auf dem CWA Data Donation Server gespeichert. Für das RKI ist eine Re-Identifizierung der CWA-Nutzer anhand der Nutzungsdaten nicht möglich.

Widerruft der CWA-Nutzer die Einwilligung für die Datenspende in der CWA App, wird die Übermittlung der Nutzungsdaten sofort eingestellt. Da die bereits übermittelten Daten keine

Identifizierung des CWA-Nutzers zulassen, ist keine Löschung erforderlich und auch nicht möglich.

5.6.10.1 Apple DeviceCheck

Der Apple-Verifikations-Dienst zur Echtheitsprüfung der Endgeräte DeviceCheck besteht aus zwei Komponenten, nämlich einer betriebssystemseitigen API (iOS-API) und einer serverseitigen API (Server-API). Die iOS-API wird von iOS lokal und die Server-API von einem Apple-Server unter <https://api.devicecheck.apple.com> bereitgestellt.

Die iOS-API kann von einer iOS-App genutzt werden, um einen sogenannten DeviceCheck-Token vom iOS-Betriebssystem anzufordern. Das DeviceCheck-Token wird bei jeder API-Abfrage neu generiert und enthält verschlüsselte Informationen zum Endgerät (iPhone), zum Entwickler-Account (hier: Entwickler-Account des RKI) sowie zum Zeitpunkt der Erzeugung des DeviceCheck-Tokens. Nur Apple kann diese Informationen auslesen. Das DeviceCheck-Token ist 30 Tage gültig. Da das DeviceCheck-Token bei jeder Abfrage neu generiert wird, kann es nicht verwendet werden, um App- oder Entwickler-übergreifende Profile anzufertigen.

Die CWA App eines an der Datenspende teilnehmenden CWA-Nutzers übermittelt das von der iOS-API erhaltene DeviceCheck-Token gemeinsam mit den Nutzungsdaten einmal täglich an den CWA Data Donation Server. Der CWA Data Donation Server übermittelt daraufhin nur das DeviceCheck-Token an die Server-API des Apple-Servers.

Der Apple-Server prüft das DeviceCheck-Token nach einem nicht-öffentlichen Verfahren auf Echtheit und gibt dem CWA Data Donation Server die Aussage zurück, ob es sich um ein echtes, nicht-manipuliertes Apple-Gerät handelt und das DeviceCheck-Token von einer App des RKI angefordert wurde (als Angabe „wahr“ oder „falsch“). Da der Apple-Server von Apple betrieben wird, kann nicht ausgeschlossen werden, dass dieser sich in einem Drittland befindet.

Ist die Echtheitsprüfung erfolgreich, werden die von der CWA App im Rahmen der Datenspende übermittelten Nutzungsdaten in Tabellenform auf dem CWA Data Donation Server gespeichert. Das DeviceCheck-Token wird gesondert, also nicht zusammen mit den Nutzungsdaten gespeichert. Die gesonderte Speicherung des DeviceCheck-Tokens dient dazu, sicherzustellen, dass die übermittelten Nutzungsdaten im jeweiligen Zeitraum nur einmal gespeichert werden.

Da die Tabellen mit den Nutzungsdaten keine eindeutige identifizierende Kennung (identifier) enthalten, können anhand der Nutzungsdaten durch das RKI keine fortlaufenden Profile der teilnehmenden CWA-Nutzer angefertigt werden. Die von einem spezifischen CWA-Nutzer an einem anderen Tag übermittelten Nutzungsdaten können nicht mit den an anderen Tagen übermittelten Nutzungsdaten zusammengeführt werden.

Sofern die Echtheitsprüfung nicht erfolgreich war oder das DeviceCheck-Token bereits auf dem CWA Data Donation Server gespeichert ist, werden die Nutzungsdaten verworfen.

5.6.10.2 Google SafetyNet

Auf Android-Geräten kommt der Google-Verifikations-Dienst zur Echtheitsprüfung der Endgeräte SafetyNet zum Einsatz. Der Dienst besteht ebenfalls aus zwei Komponenten, nämlich der lokalen Komponente SafetyNet Attestation API sowie einem SafetyNet-Server von Google. Die SafetyNet Attestation API ist Bestandteil der Google-Play-Dienste, die auf jedem Android-Gerät mit der Play-Store-App installiert sind.

Eine Android-App (hier: CWA App) kann die SafetyNet Attestation API lokal aufrufen und eine sogenannte Nonce (eine zufällige Zahlenfolge, die von der Android-App festgelegt wird) übergeben. Der lokale SafetyNet-Attestation-Dienst wertet daraufhin die Integrität des Endgeräts und der CWA App lokal auf Basis von nicht-öffentlichen, von Google festgelegten Kriterien aus und übermittelt im Fall eines positiven Ergebnisses das Ergebnis des Prüfungsvorgangs und den Nonce an den SafetyNet-Server von Google.

Dieser validiert den Prüfungsvorgang auf Basis eines ebenfalls nicht-öffentlichen Verfahrens, signiert bei erfolgreicher Validierung das Ergebnis und sendet ein entsprechendes Zertifikats-Token sowie die Nonce an die CWA App zurück. Der Validierungsvorgang auf dem SafetyNet-Server dient dazu sicherzustellen, dass der Validierungsprozess auf dem Endgerät manipulationsfrei ablief. Es kann nicht ausgeschlossen werden, dass der SafetyNet-Server sich in einem Drittland befindet.

Die CWA App des teilnehmenden CWA-Nutzers übermittelt das signierte Bewertungsergebnis (Zertifikats-Token) gemeinsam mit den Nutzungsdaten und einem Salt (zufällige Zeichenfolge zur Vermeidung von "Replay-Attacken") an den CWA Data Donation Server. Der CWA Data Donation Server überprüft das von der CWA App empfangene Zertifikats-Token lokal, d. h. ohne einen weiteren Zugriff auf einen Google-Server. Stellt der CWA Data Donation Server fest, dass das gültige Zertifikats-Token vorliegt, werden die Nutzungsdaten in einer Tabelle gespeichert.

Das Zertifikats-Token wird gesondert, also nicht zusammen mit den Nutzungsdaten gespeichert. Die gesonderte Speicherung des Zertifikats-Tokens dient dazu, sicherzustellen, dass die übermittelten Nutzungsdaten im jeweiligen Zeitraum nur einmal gespeichert werden.

Da die Tabellen mit den Nutzungsdaten keine eindeutige identifizierende Kennung (identifier) enthalten, können anhand der Nutzungsdaten durch das RKI keine fortlaufenden Profile der teilnehmenden CWA-Nutzer angefertigt werden. Die von einem spezifischen CWA-Nutzer an einem anderen Tag übermittelten Nutzungsdaten können nicht mit den an anderen Tagen übermittelten Nutzungsdaten zusammengeführt werden.

Sofern die Echtheitsprüfung nicht erfolgreich war oder das Zertifikats-Token bereits auf dem CWA Data Donation Server gespeichert ist, werden die Nutzungsdaten verworfen.

5.6.11 Einladung zu Befragungen

Sollte ein CWA-Nutzer eine Einladung zu einer Befragung im Kontext der Anzeige eines hohen Risikostatus auf dem Home-Bildschirm angezeigt bekommen und er im folgenden Screen auf den Einwilligungs-Button tippen, wird ein OTP in der CWA App generiert (auch sog. EDUS OTP).

Zugleich wird das im Zusammenhang mit der Datenspende bereits beschriebene Verfahren von Apple (DeviceCheck) bzw. Google (SafetyNet Attestation) zur Prüfung der Echtheit des Endgeräts, auf dem die CWA App ausgeführt wird, genutzt. Die CWA App übermittelt den DeviceCheck-Token bzw. Zertifikats-Token dann gemeinsam mit dem OTP an den CWA Server. Ist die Verifikation des jeweiligen Tokens erfolgreich, wird vom CWA Server ein Link generiert, der das OTP enthält. Das OTP dient an dieser Stelle zugleich der einmaligen Zuordnung der Anfrage der CWA an den CWA Server und verhindert so die Mehrfachteilnahme an einer Befragung.

5.6.12 Zertifikats-Wallet

5.6.12.1 Speichern von Impfzertifikaten

Um ein Impfzertifikat (oder ein anderes COVID-Zertifikat) zu speichern, muss der CWA-Nutzer mit der Kamera seines Smartphones den zu dem Impfzertifikat gehörigen QR-Code einscannen. Der QR-Code enthält eine zlib-komprimierte und base45-kodierte Darstellung des Inhalts des Impfzertifikat, der dann von der CWA App ausgelesen und lokal gespeichert wird. Zum Schutz vor Zip-Bombenangriffen ist die maximale Ausgabegröße der Zlib-Dekompression auf 10 MB begrenzt.

Die aus dem QR-Code ausgelesenen Daten (siehe Abschnitt 5.5.3) werden lokal im App-Speicher gespeichert. Seit App-Release 2.7 setzt dies eine vorgeschaltete erfolgreiche Prüfung der elektronischen Signatur im QR-Code auf technische Gültigkeit voraus (Signaturprüfung). Die Signaturprüfung erfolgt lokal auf dem Smartphone des CWA-Nutzers. Ziel der Signaturprüfung ist es zu verhindern, dass unechte oder technisch ungültige Impfzertifikat in der CWA App gespeichert werden. Daher bewertet die Signaturprüfung ein Impfzertifikat als ungültig, wenn das technische Ablaufdatum des betreffenden Impfzertifikat erreicht oder seine elektronische Signatur mit einem unbekannten oder zum Zeitpunkt des Auslesens noch nicht oder nicht mehr gültigem Signaturschlüssel elektronisch signiert worden ist.

Zu diesem Zweck lädt die CWA App vom CDN-Magenta zunächst die DCC Digital Signing Certificate List (DCC DSC List) herunter. Die DCC DSC List enthält sämtliche Signaturschlüssel, die von den nationalen Zertifikatservices der am COVID-Zertifikat teilnehmenden Länder bisher zur elektronischen Signierung von COVID-Zertifikaten

verwendet worden sind.³⁸ Die CWA App prüft in einem ersten Schritt, ob die aus dem QR-Code ausgelesene elektronische Signatur mit einem auf der DCC DSC List aufgeführten Signaturschlüssel elektronische signiert worden ist, indem die in der DCC DSC List enthaltenen Signaturschlüssel jeweils in ein X.509-Format (Zertifikat) umgewandelt und dann nacheinander mit der aus dem QR-Code ausgelesenen elektronischen Signatur abgeglichen werden. Sollte dabei keine Übereinstimmung festgestellt werden, wird die Signaturprüfung abgebrochen und dem CWA-Nutzer das eingelesene Impfzertifikat in der CWA App als ungültig angezeigt.

Sollte eine Übereinstimmung festgestellt werden, wird in einem zweiten Schritt geprüft, ob der für die elektronische Signierung verwendete Signaturschlüssel aktuell technisch gültig ist, d. h. ob der technische Gültigkeitszeitraum des Signaturschlüssel bereits begonnen hat und falls ja noch nicht abgelaufen ist. Ergibt die Prüfung, dass der verwendete Signaturschlüssel noch nicht oder nicht mehr gültig ist, wird dem CWA-Nutzer das eingelesene Impfzertifikat ebenfalls als ungültig angezeigt und die Signaturprüfung abgebrochen.

Der dritte und letzte Schritt der Signaturprüfung erfolgt anhand des Wertes des im Signaturschlüssel enthaltenen Datenfelds „extended key usage“. Dieses vom eHealth-Netzwerk vorgeschlagene optionale Datenfeld soll zur Beschreibung der Zertifikatskategorie (Impf-, Genesenens- oder Testzertifikat) dienen und die Art der ausgebenden Stelle bezeichnen, für die der Signaturschlüssel gültig ist.³⁹ Stimmt die festgelegte Zertifikatskategorie mit denjenigen des ausgelesenen COVID-Zertifikats überein (hier jeweils: Impfzertifikat), ist die Signaturprüfung erfolgreich abgeschlossen und das Impfzertifikat wird von der CWA App als technisch gültig behandelt. Andernfalls wird die Signaturprüfung abgebrochen und das Impfzertifikat als ungültig behandelt. Sofern das Datenfeld in dem Signaturschlüssel von einem nationalen Zertifikatsservice nicht verwendet wird, ist der Signaturschlüssel für alle Zertifikatskategorien gültig, so dass der dritte Schritt der Signaturprüfung immer erfolgreich abgeschlossen werden kann.

Die eHealth-Guidelines schließen die Verwendung von zusätzlichen oder anderen als den vorgeschlagenen extended-key-usage-Werten nicht aus. Von dieser Möglichkeit machen die nationalen Zertifikatsservices der anderen COVID-Zertifikate ausgebenden Ländern teilweise Gebrauch. Entsprechend der eHealth-Guidelines werden die länderspezifischen Gültigkeitswerte über das von der EU-Kommission betriebene DCC-Gateway den nationalen Zertifikatsservices bekanntgegeben und von diesen zusammen mit den DCC DCS Lists an die CWA App bzw. die anderen nationalen Corona-Apps verteilt, die diese dann jeweils im Rahmen der Signaturprüfung anwenden.

Wenn die Signaturprüfung erfolgreich abgeschlossen und das Impfzertifikat entsprechend von der CWA App gespeichert worden ist, wird das hinzugefügte Impfzertifikat dem CWA-Nutzer nach Maßgabe der aktuellen Value Sets (siehe Abschnitt 5.5.3) in der CWA App angezeigt. Die Value Sets werden stets aktualisiert, wenn der CWA-Nutzer die Zertifikatsübersicht aufruft

³⁸ Vor Release 2.7 konnten lediglich vom RKI elektronisch signierte COVID-Zertifikate gespeichert werden, so dass die DCC DSC List nur die vom RKI verwendeten Signaturschlüssel enthielt.

³⁹ eHealth Network, Guidelines on Technical Specifications for Digital Green Certificates – Volume 1 V1.0.5 vom 21.04.2021, S. 12.

und eine Internetverbindung zur Verfügung steht. Sobald der Prozess gestartet wurde, wird eine Anfrage an das CDN-Magenta zum Herunterladen des aktuellen Value-Sets-Pakets gesendet. Sollte sich das Value-Set-Paket seit dem letzten Download geändert haben, wird das neue Paket heruntergeladen. Wenn sich das Value-Sets-Paket nicht geändert haben sollten, wird die CWA App darüber informiert und der Prozess zur Aktualisierung der Value Sets wird beendet.

Der in der CWA App angezeigte QR-Code ist keine Kopie des gescannten QR-Codes, sondern wird neu von der CWA App auf Basis der aus dem QR-Code ausgelesenen Daten (siehe Abschnitt 5.5.3) generiert. Dieser neu generierte QR-Code enthält die base45-kodierten Inhalte des gescannten QR-Codes – im Fall von Impfzertifikaten also den Impfstatus (siehe Abschnitt 5.5.3) – sowie ein Präfix zur Kennzeichnung der Versionsnummer der von der CWA App verwendeten Datenstruktur (z. B. „HC1“ = Health Certificate Version 1). Beispiel:

HC1:6BFOXN*TS0B [...]

Anhand des Präfixes wird der sog. Kontext definiert, d. h. wie der aus dem QR-Code ausgelesene Text interpretiert werden muss (z. B. in welcher Reihenfolge welche Informationen zum Impfstatus genannt werden und welches Value Set zur Anzeige zu verwenden ist). Die Definitionen zum Kontext werden von den nationalen technischen Ausstellern der Impfzertifikate (in Deutschland das RKI) an die EU-Kommission gemeldet, die diese über einen zentralen Server für Anbieter von Prüf-Anwendungen zum Download bereitstellt.⁴⁰

5.6.12.2 Speichern von Genesenenzertifikaten

Die Verarbeitungsschritte beim Scannen bzw. Speichern eines Genesenenzertifikats erfolgen nach dem gleichen Prinzip wie das Speichern eines Impfzertifikats. Es wird daher auf die Darstellung in Abschnitt 5.6.12.1 entsprechend Bezug genommen.

5.6.12.3 Speichern von Testzertifikaten

Wenn ein Testzertifikat im Papierformat gescannt wird, entsprechen die Verarbeitungsschritte denen beim Scannen eines Impfzertifikats im Papierformat. Es wird daher auf die Darstellung in Abschnitt 5.6.12.1 entsprechend Bezug genommen.

Wenn der CWA-Nutzer über die CWA App ein negatives Testergebnis erhalten und im Rahmen der Testregistrierung ein Testzertifikat für den betreffenden Test angefordert hat, fordert die CWA App beim DCC Server das Testzertifikat an. Hierfür erzeugt die CWA App für das Testergebnis zunächst lokal einen öffentlichen und einen privaten Schlüssel. Der öffentliche Schlüssel wird zusammen mit dem bereits vorliegenden Registration Token des betreffenden Tests von der CWA App an den DCC Server übermittelt. Der DCC Server leitet

⁴⁰ eHealth Network, Guidelines on Technical Specifications for Digital Green Certificates Volume: Interoperable 2D Code, Version 1.3 vom 21.04.2021.

den Registration Token zusammen mit der Anforderung des Testzertifikats an den Verifikationsserver weiter. Der Verifikationsserver „übersetzt“ das Registration Token in den bzw. die dem Test zugeordneten Hash-Werte (abgeleitet aus der GUID bzw. der GUID und dem Geburtsdatum des CWA-Nutzers) und gibt diese dem DCC Server bekannt. Der DCC Server generiert sodann die eindeutige Zertifikatskennung des Testzertifikats und leitet diese zusammen mit dem öffentlichen Schlüssel des CWA-Nutzers und dem bzw. den Hash-Werten an die Systeme der Labore bzw. Teststellen weiter. Diese ergänzen die für das zugeordnete Testzertifikat erforderlichen Informationen zum Teststatus, verschlüsseln diese Informationen mit dem öffentlichen Schlüssel des CWA-Nutzers und geben den daraus berechneten Hashwert an den DCC Server zurück. Der DCC Server gibt den Hashwert nun an den Zertifikatsservice⁴¹ weiter, wo er durch das RKI elektronisch signiert wird. Der signierte Hashwert wird schließlich an den DCC Server zurückgegeben, der diesen dann an die CWA App des CWA-Nutzers weiterleitet. Die CWA App entschlüsselt mit dem privaten Schlüssel den signierten Hashwert und erzeugt daraus lokal das endgültige Testzertifikat.

5.6.12.4 Zuordnung zu Zertifikatsinhabern

Zur Verbesserung der Nutzungsfreundlichkeit zeigt die CWA App mehrere COVID-Zertifikate der gleichen Person zusammengefasst unter dem jeweiligen Namen an. Die Zuordnung erfolgt lokal durch einen Vergleich der in der Zertifikatsaussage enthaltenen Daten des Zertifikatsinhabers.

Die Funktion ist mit einer Fehlertoleranz ausgestattet, damit die bei Personen mit mehreren Vornamen oder mit aus mehreren Wörtern zusammengesetzten Nachnamen häufig uneinheitliche Namensanwendung berücksichtigt werden kann. Hierzu werden Namenszusätze und akademische Titel in den Namensangaben der Zertifikatsaussage herausgefiltert und nur noch die insoweit bereinigten Vor- und Nachnamen sowie das Geburtsdatum für die Zuordnung verwendet. Mehrere COVID-Zertifikate werden von der CWA App einer Person zugeordnet, wenn mindestens ein Vorname, mindestens ein Nachname und das Geburtsdatum exakt übereinstimmen.

5.6.12.5 Speichern von Familienzertifikaten

Bei der Nutzung der Funktion für Familienzertifikate werden die mit der CWA App gescannten COVID-Zertifikate von Angehörigen des CWA-Nutzers in der CWA App gespeichert und können dem CWA-Nutzer dann nach den jeweiligen Zertifikatsinhabern gruppiert angezeigt werden. Die Verarbeitungsschritte in Bezug auf die Daten der jeweiligen weiteren Zertifikatsinhaber entsprechen im Übrigen den Verarbeitungsschritten bei eigenen COVID-Zertifikaten des CWA-Nutzers, so dass auf die entsprechenden Darstellungen der Verarbeitung von Impfzertifikaten (Abschnitt 5.6.12.1), Genesenenzertifikaten (Abschnitt

⁴¹ Der Zertifikatsservice gehört zu CovPass und wird daher in der DSFA zu den digitalen COVID-Zertifikaten behandelt.

5.6.12.1), Testzertifikaten (Abschnitt 5.6.12.1) und der Zuordnungsfunktion (Abschnitt 5.6.12.1) verwiesen werden kann.

Die Namen, unter denen Familienzertifikate jeweils verwaltet werden, werden ebenso wie der Name des CWA-Nutzers ausschließlich lokal verarbeitet.

5.6.12.6 Zertifikats-Gültigkeitsprüfung

Bei aktiver Nutzung der Gültigkeitsprüfung von COVID-Zertifikaten lädt die CWA App die gegenwärtig gültigen Regelsätze der Mitgliedstaaten vom CDN-Magenta herunter. Es werden immer die Regelwerke sämtlicher Mitgliedsländer heruntergeladen. Die Prüfung der COVID-Zertifikate gegen den Regelsatz des ausgewählten Mitgliedslandes findet lokal auf dem Endgerät des CWA-Nutzers statt. Anschließend wird dem CWA-Nutzer das Prüfergebnis angezeigt.

Zudem lädt die CWA App regelmäßig die aktuelle Widerrufsliste vom CDN-Magenta und gleicht die darin enthaltenen Informationen über widerrufene Zertifikate mit den gespeicherten COVID-Zertifikaten ab. Die Widerrufsliste enthält keine vollständigen Zertifikatskennungen, sondern den sog. R-Wert gesperrter Zertifikate. Es handelt sich dabei um einen ganzzahligen Zufallswert, der auf eine spezifische Zertifikatskennung verweist, aber aus dem Wert nicht reproduziert werden kann. Dieselben Ausgangsdaten erzeugen einen neuen, einzigartigen, aber auf das spezifische Zertifikat bezogenen R-Wert. Die Widerrufslisten enthalten dabei nur die ersten Teil-Segmente des R-Wertes. Die CWA App gleicht diese Segmente mit den daraus abgeleiteten eindeutigen Kennungen der auf dem Smartphone gespeicherten COVID-Zertifikate ab. Sofern es eine Übereinstimmung gibt, wird das betreffende COVID-Zertifikat in der CWA App als ungültig angezeigt. Das widerrufene digitale COVID-Zertifikat selbst wird dabei jedoch nicht technisch verändert. Der Abgleich findet ausschließlich lokal statt.

Das Verfahren zur Umsetzung von Zertifikatssperrungen basiert auf den Richtlinien des eHealth-Netzwerks.⁴²

5.6.12.7 Mitteilungen über Auffrischimpfungen

Die CWA App zählt die Tage seit der letzten gültigen Impfung einer Impfserie und zeigt diese auch bei dem entsprechenden Impfzertifikat an. Mittels der über das CDN-Magenta bereitgestellten Regelwerke, die auch Angaben zu den von den jeweiligen nationalen Stellen empfohlenen Zeitpunkten für Auffrischimpfungen umfassen, wird dann abgeglichen, ob nach dem für ein Impfzertifikat maßgeblichem Regelwerk eine Auffrischimpfung erforderlich sein

⁴² eHealth Network, Guidelines on EU DCC Revocation - B2A Communication between the Backend and the Applications, V1.1 vom 30.03.2022, S. 7 ff.

könnte. Wenn das der Fall ist, wird von der CWA App über die lokale Mitteilungsfunktion des Betriebssystems eine entsprechende Mitteilung ausgelöst, sofern die CWA App zum Versand von Push-Mitteilungen berechtigt ist (siehe unter Ziffer 5.4.15.3).

5.6.12.8 Druckversion von Zertifikaten

Die Erstellung von Druckversionen von auf dem Smartphone gespeicherten digitalen COVID-Zertifikaten erfolgt ausschließlich lokal auf dem Smartphone.

Das Template für die PDF-Version des jeweiligen Zertifikats ist Bestandteil der CWA App und im Speicher der CWA App abgelegt.

Wenn der CWA-Nutzer die Druckversion eines Zertifikats über die Funktion erstellt, wird das Template aus dem App-Speicher ausgelesen und die Platzhalter mit den jeweiligen Zertifikatsangaben befüllt. Die Zertifikatsangaben werden aus der im App-Speicher bereits hinterlegten elektronischen Version des jeweiligen Zertifikats ausgelesen.

Anschließend wird das erstellte PDF-Dokument an die Teilen-Schnittstelle des Betriebssystems übergeben. Sobald der CWA-Nutzer den Teilen-Dialog des Betriebssystems schließt, wird das PDF-Dokument aus dem App-Speicher gelöscht. Diese Löschung erfolgt unabhängig davon, ob das PDF-Dokument geteilt worden ist.

Die Funktion zur Erstellung der Druckversion eines Zertifikats wird entsprechend für die Exportfunktion für alle in der CWA App gespeicherten digitalen COVID-Zertifikate verwendet. Es wird hierbei nach demselben Verfahren ein Gesamt-PDF erstellt, aus dem die Zertifikate anschließend wieder in andere Wallet-Apps (insbesondere in die CovPass-App) eingelesen werden können.

5.6.12.9 Nutzung der Online-Validierungsfunktion

Abgrenzung des Prüfgegenstands: Die konkreten Datenverarbeitungen auf Seiten der Leistungsanbieter und Prüfpartner bzw. Validierungsdienste liegen nicht im Einflussbereich des RKI und sind nicht Gegenstand dieser DSFA. Die nachfolgende Skizzierung der Datenflüsse und Prozesse auf Seiten der Leistungsanbieter und Prüfpartner soll in erster Linie die Einordnung und Bewertung der lokalen Verarbeitungstätigkeiten der CWA App erleichtern.

Bei der Entwicklung der lokalen Verarbeitungstätigkeiten der CWA App für die Online-Validierung ist das RKI ein Online-Validierungsverfahren gemäß den Richtlinien des eHealth-Netzwerks zugrunde gelegt.⁴³

⁴³ eHealth Network, Guidelines on the use of Digital Covid Certificates in traveller and online booking scenarios, V1.2.0 vom 21.10.2021, S. 15 ff.

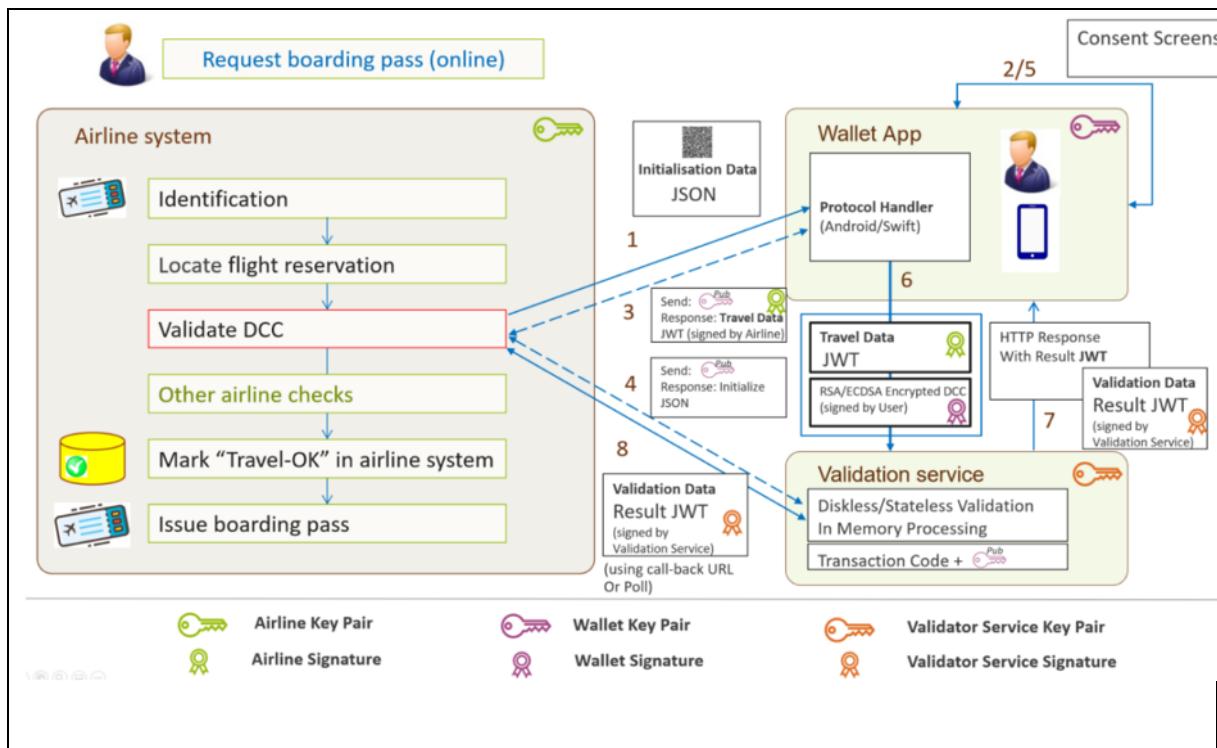


Abbildung 20: Übersicht des allgemeinen Prozesses (Quelle: eHealth-Netzwerk)

Zur Einleitung des Online-Validierungsverfahrens muss der Leistungsanbieter dem Zertifikatsinhaber im Rahmen des Buchungsvorgangs einen individuell erzeugten Initialisierungs-QR-Code aushändigen. Der Initialisierungs-QR-Code enthält einen Initialisierungs-Token mit einer Transaktions-ID, einer kurzen Beschreibung des Buchungsvorgangs (z. B. „Buchungsnummer 1234“), eine Bezeichnung des Leistungsanbieters (z. B. „Lufthansa“) und einer URL, unter der die Wallet-App ein vom Leistungsanbieter bereitgestelltes sog. Identity Document abrufen kann, welches die zum Abruf des Validation Access Token mit den für die Online-Validierung benötigten Validierungsanforderungen enthält.

Um die URL des Identity Documents zu verifizieren, wird von der CWA App eine Service Provider Allow List (SPAL) verwendet. Diese enthält die gehaschten URLs der Leistungsanbieter und wird regelmäßig von der CWA App vom CDN-Magenta heruntergeladen. Sofern ein Initialisierungs-QR-Code gescannt wurde, wird die darin hinterlegte URL mit der SPAL abgeglichen. Wenn die URL in der SPAL nicht enthalten ist, wird CWA-Nutzer darauf hingewiesen, dass der Leistungsanbieter nicht bekannt ist und er vor Fortsetzung des Vorgangs die Vertrauenswürdigkeit des Leistungsanbieters genau überprüfen sollte.

Nachdem der CWA-Nutzer den Initialisierungs-QR-Code mit dem QR-Code-Scanner der CWA App ausgelesen und der CWA-Nutzer seine Einwilligung in den Abruf der weiteren Buchungsdaten vom Leistungsanbieter erteilt hat, lädt die CWA App das Identity Document mit den Public Keys des Leistungsanbieters und des Validierungsdienstes sowie Angaben zu dem Server des Leistungsanbieters, von dem das Validation Access Token abgerufen werden kann. Das Identity Document ist mit dem privaten Schlüssel des Leistungsanbieters elektronisch signiert und kann von der CWA App nur geladen werden, wenn das Initialisierungs-Token aus dem Initialisierungs-QR-Code vorliegt.

Die CWA App prüft lokal, ob der Validierungsdienst auf der vom BMG verwalteten Liste anerkannter Validierungsdienste genannt ist. Diese Liste enthält die vom BMG aufgenommenen Validierungsdienste und wird regelmäßig von der CWA App vom CDN-Magenta heruntergeladen. Wird der Validierungsdienst nicht in der Liste der anerkannten Validierungsdienste aufgeführt, wird der Online-Validierungsvorgang abgebrochen. Dadurch soll die unwissentliche Übermittlung von COVID-Zertifikaten an unbefugte oder unzuverlässige Empfänger (z. B. Spoofers), die sich als Prüfpartner eines (kompromittierten) Leistungsanbieters ausgeben, verhindert werden.

Anhand der in dem im Identity Document enthaltenen Zugangsdaten lädt die CWA App vom Serversystem des Leistungsanbieters das Validation Access Token mit den konkreten Validierungsanforderungen. Anhand dieser prüft die CWA App sodann, welche der gespeicherten COVID-Zertifikate für die Prüfung grundsätzlich in Frage kommen und schlägt ein geeignetes Zertifikat vor. Diese Eignungsprüfung findet ausschließlich lokal statt. Die wesentlichen Validierungsanforderungen (Name und Geburtsdatum des Zertifikatsinhabers, welche Zertifikatskategorien werden akzeptiert, ggf. Zeitpunkt, zu dem die Gültigkeit vorliegen muss) werden dem CWA-Nutzer bei der Anzeige und Bestätigung bzw. Auswahl der in Frage kommenden Zertifikate angezeigt.

Sofern der CWA-Nutzer einwilligt, werden die Validierungsdaten und das ausgewählte COVID-Zertifikat mit einem von der CWA App für den jeweiligen Validierungsvorgang generierten privaten Schlüssel elektronisch signiert und das Zertifikat mit dem Public Key des Validierungsdienstes verschlüsselt und dann an die im Identity Document bezeichnete Schnittstelle des Validierungsdienstes übermittelt. Der Public Key des von der CWA App generierten privaten Schlüssels wird von der CWA App zusammen mit dem Validation Access Token zugleich auch an den Leistungsanbieter übermittelt, der seinerseits den Public Key an den Validierungsdienst weitergibt.

Der Validierungsdienst entschlüsselt die empfangene Datei und überprüft, ob die elektronischen Signaturen sowohl des COVID-Zertifikats als auch des Validation Access Token echt sind und ob das COVID-Zertifikat die Validierungsanforderungen des Leistungsanbieters erfüllt.

Das Validierungsergebnis (also ob die Validierung erfolgreich oder nicht erfolgreich war) und im Fall einer nicht erfolgreichen Validierung auch der Grund (beispielsweise welche Validierungsanforderungen des Leistungsanbieters vom Validierungsdienst als nicht erfüllt bewertet worden sind) wird an die CWA App in Form des Result Token übermittelt und dem Nutzer angezeigt. Die Datenstruktur des Validierungsergebnisses wird von dem Validierungsdienst elektronisch signiert und von der CWA App nach dem Empfang mittels des Public Keys des Validierungsdienstes auf Echtheit geprüft.

Damit der Leistungsanbieter das Validierungsergebnis abrufen kann, muss er dieses beim Validierungsdienst unter Angabe der Transaktions-ID aus dem Initialisierungs-Token und dem Public Key des Nutzers anfordern. Der Leistungsanbieter erhält vom Validierungsdienst daraufhin ausschließlich das zur Transaktions-ID gehörige und vom Validierungsdienst elektronisch signierte Validierungsergebnis zurück. Im Falle einer nicht erfolgreichen

Validierung werden die Gründe für die fehlgeschlagene Prüfung gemäß den Richtlinien des eHealth-Netzwerks nicht an den Leistungsanbieter mitgeteilt.

Der CWA-Nutzer kann einen begonnenen Online-Validierungsvorgang auf jedem Einwilligungsscreen der CWA App abbrechen. Sofern der Online-Validierungsvorgang nicht abgeschlossen wird oder werden kann, wird er von der CWA App automatisch abgebrochen. In der CWA App werden zum Validierungsvorgang grundsätzlich keine personenbezogenen Daten über den Validierungsvorgang hinaus gespeichert. Der CWA-Nutzer hat die Möglichkeit ein Validierungs-Log zu aktivieren, in dem die Angaben zu einem erfolgten Validierungsvorgang gespeichert werden (Bezeichnung und URL des Leistungsanbieters, Buchungsanforderungen, übermitteltes Zertifikat, Bezeichnung und URL des Validierungsdienstes). Diese optionale Dokumentation stellt sicher, dass der CWA-Nutzer über die Wallet-App erfolgte Validierungsvorgänge nachvollziehen und gegebenenfalls eigene datenschutzrechtliche Betroffenenrechte geltend machen kann. Das Log-File wird im geschützten App-Speicher abgelegt und kann vom CWA-Nutzer jederzeit gelöscht werden.

Der Validierungsdienst hat vor Abgabe der zweiten Einwilligung in der CWA App keine Daten erhalten.

Wird der Online-Validierungsvorgang abgebrochen, ruft die CWA App gemäß den Richtlinien des eHealth-Netzwerks den im Identity Document genannten Serverendpunkt des Leistungsanbieter für die Meldung von Validierungsabbrüchen auf, so dass der Leistungsanbieter die Löschung der bisher zu dem Validierungsprozess bei ihm angefallenen Daten veranlassen kann.

5.6.13 Deinstallation der CWA App

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

Durch diesen Schritt nicht automatisch gelöscht werden die Daten, die durch das jeweilige Betriebssystem gespeichert und verwaltet werden. Dies betrifft zum einen Verschlüsselungsschlüssel in der KeyChain. Unter iOS bleiben zudem die Daten in der Begegnungsaufzeichnung des ENF zunächst erhalten. Unter Android werden mit der Deinstallation der CWA App die Schlüssel dann automatisch gelöscht, wenn keine weitere Corona-App installiert ist, die Zugriff auf die Begegnungsaufzeichnung des ENF hat.

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 oder im Rahmen der Datenspende an den Data Donation Server übermittelter 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.

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 und CHGS beinhaltet keine Zugriffe 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 im ENF zufällig generierten Wert. Die Bezeichnung als Tagesschlüssel röhrt daher, dass der Tagesschlüssel einmal täglich neu generiert wird.

Mehr als ein Tagesschlüssel wird nur generiert, wenn der CWA-Nutzer eine CWA App ab Version 1.8 nutzt und ein Testergebnis teilt. In diesem Fall wird der Tagesschlüssel des Tages, an dem das Teilen des Testergebnis erfolgt, zusammen mit den übrigen Tagesschlüsseln an den CWA Server übermittelt, weshalb vom ENF V2 ein neuer Tagesschlüssel generiert wird, der bis zum Ablauf des jeweiligen Tages als Ersatz für den zuvor geteilten Tagesschlüssel verwendet wird. Dieses in der ENF-Dokumentation sogenannte „Same Day Keys“-Feature ermöglicht, dass Begegnungen, die am Tag des Auslösens der Warnung aufgezeichnet werden, bis zu einem Tag früher als bisher gewarnt werden können.

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 getester Nutzer andere Nutzer infizieren könnte (Übertragungsrisiko). 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.⁴⁴ Das TransmissionRiskLevel wird von der CWA App, über die der Tagesschlüssel (als Positivschlüssel) bereitgestellt wird, nach Maßgabe der zum Zeitpunkt des Teilens des Testergebnisses aktuellen BWE festgelegt.

Wenn die Tagesschlüssel über eine andere nationale Corona-App (mit möglicherweise abweichenden BWE) bereitgestellt werden, wird der Wert des TRL auf dem CWA Server nach Maßgabe der vom RKI definierten Bewertungsregeln ausgehend vom Wert des **DaySinceOnsetOfSymptoms (DSOS)**, der Bestandteil von geteilten Tagesschlüsseln (Positivschlüssel, siehe Abschnitt 5.7.8.1) ist.

Das TransmissionRiskLevel-Feld wird für die Risikoberechnung in Form von Score-Werten (ENF V1) benötigt (siehe dazu Abschnitt 5.7.8.1 (Angabe als Score-Wert) und 5.7.8.2 (Angabe als Minutenwert) beschrieben).

KeyData:

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

⁴⁴ Google: Exposure Notifications API, abrufbar unter: <https://developers.google.com/android/exposure-notifications/exposure-notifications-api#data-structures> (abgerufen am 11.10.2022).

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.

5.7.4 RPI-Metadaten (ENF V1)

Die vom ENF 1 während einer Scan-Instanz aufgezeichneten RPIs anderer Nutzer werden zusammen mit den folgenden Metadaten im Kontaktprotokoll des ENF gespeichert:

- (1) Datum der Begegnung
- (2) Dämpfungswert in dB (gemeldete Signalstärke – gemessene RSSI)
- (3) 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)
- (4) Dauer der Begegnung (exposure) in 5er Schritten (<5/10/15/20/25/30/>30 Minuten)

Der Dämpfungswert wird vom ENF 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 ergebende Wert ist der Dämpfungswert und kann als Indikator für die räumliche Entfernung der Begegnung verwendet werden.

Im Kontaktfall übergibt das ENF V1 die RPI-Metadaten im Rahmen der Risiko-Ermittlung an die CWA App, die unter Verwendung dieser Daten nach Maßgabe der BWE das **Übertragungsrisiko** in Bezug auf die betreffende Begegnung berechnet.

5.7.5 Exposure-Window-Daten (ENF V2)

Die CWA App ab Version 1.8 nutzt die Funktionen des ENF V2 zur Risikoberechnung. Die Risikoberechnung des ENF V2 basiert auf sogenannten Exposure Windows. Wenn in Schritt 3 der Anwendungsphase 1 ein Match festgestellt wird, übergibt das ENF V2 zu der jeweiligen Begegnung im ENF V2 aufgezeichnete Daten in Form einer von Apple und Google definierten Datenstruktur zurück, welche das zugehörige Exposure Window abbildet.

Erfolgt die Risikoberechnung anhand von gematchten Check-ins, werden die vom CWA Server heruntergeladenen Check-ins und die lokalen Check-in-Details von der CWA App unter Berücksichtigung der sowohl in den Check-ins als auch in den Check-in-Details enthaltenen Zeitintervalle auf zeitliche Überschneidungen hin untersucht und auf Basis der daraus abgeleiteten Begegnungsdauer und des TRL-Wertes selbst in die Struktur eines Exposure Windows gebracht.

Sowohl das vom ENF V2 als auch das von der CWA App selbst erzeugte Exposure Window wird im Folgenden als Exposure-Window-Daten bezeichnet.

Ein Exposure Window beschreibt eine vom ENF aufgezeichnete bzw. eine aus dem Checkin-Matching abgeleitete Begegnung für eine maximale Zeitspanne von 30 Minuten. Sollte eine Begegnung länger als 30 Minuten andauern, dann existieren dementsprechend mehrere Exposure Windows, um die Zeitspanne der Begegnung zu dokumentieren. Mehrere Exposure Windows lassen sich nicht einander zuordnen, auch wenn sie sich auf die gleiche Begegnung beziehen. Ein Exposure Window bezieht sich immer nur auf ein anderes Gerät und enthält Informationen über die empfangenen BLE Signale jeweils eines anderen Geräts, die während der Begegnung aufgezeichnet wurden.

Exposure-Window-Daten enthalten folgende Angaben:

- (1) *Date*: Datum der Begegnung
- (2) *Report Type*: Angabe der Diagnosemethode, die dem von dem positiv getesteten Nutzer geteilten Testergebnis zugrunde liegt. Die Angabe der Diagnosemethode erfolgt in drei Kategorien, die jeweils einer Risikostufe entsprechen (confirmed test diagnosis, clinical diagnosis, self-reported diagnosis). Die Kategorien werden vom ENF V2 vorgegeben. Die Diagnoseart ergibt sich aus dem entsprechenden Datenfeld des Positivschlüssels.
- (3) *Infectiousness*: Angabe der Infektiosität⁴⁵ des positiv getesteten Nutzers am Tag der Begegnung (siehe Datenfeld „Date“). Die Risikostufe der Infektiosität wird auf einer dreistufigen Skala angegeben (High, Standard, None). Die Einstufung erfolgt nach Maßgabe der BWE auf Basis des Werts DSOS, der mit den Positivschlüsseln jeweils verknüpft ist.

⁴⁵ Der Wert der Infektiosität bei Verwendung des ENF V2 entspricht funktional dem Wert des TRL bei Verwendung des ENF V1, ist jedoch von diesem zu unterscheiden, da er anders berechnet wird.

Days since symptom onset	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+10	+11	+12	+13	+14	
Infectiousness	None															Standard											High			
Weight	No weight															100%											200%			

Abbildung 21: Beispielhafte Zuordnungstabelle zur Ermittlung der Infectiousness

- (4) Aufzeichnungen zu den Scan-Instanzen, die dem Exposure Window zugrunde liegen:
- typicalAttenuation: Durchschnittlicher Dämpfungswert der von dem anderen ENF ausgesendeten RPI während des Scans in dB.
 - minAttenuation: Niedrigster gemessener Dämpfungswert der von dem anderen ENF ausgesendeten RPI während des Scans in dB.
 - secondsSinceLastScan: Angabe der Sekunden in 60er-Schritten, die seit dem letzten Scan des ENF V2 nach von anderen ENF-Instanzen ausgesendeten RPIs vergangen sind. Dieser Wert ist unabhängig davon, ob bei dem letzten Scan eine Begegnung aufgezeichnet worden ist. Der Wert kann maximal 320 Sekunden (5 Minuten) betragen. Durch Addition aller secondsSinceLastScan-Werte in einem Exposure Window kann auf die ungefähre Dauer der Begegnung geschlossen werden, wobei die maximale Dauer aus den oben genannten Gründen 30 Minuten betragen kann.

Die BLE-Signale von zwei Geräten führen zu zwei Exposure Windows von denen man nicht weiß, dass sie parallel liegen. Diese werden dann für die Risikoberechnung der Begegnungen herangezogen.

5.7.6 Positivschlüssel (Diagnoseschlüssel)

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, von dieser um die Felder DaysSinceOnsetOfSymptoms (DSOS) und TRL ergänzt und dann als sogenannter Positivschlüssel dann gebündelt an den CWA Server übermittelt. Von dort werden sie am EFGS den Verantwortlichen der anderen nationalen Corona-Apps in Form von Positivschlüssel-Paketen zur Verfügung gestellt, um die länderübergreifende Risiko-Ermittlung zu ermöglichen. Ein Positivschlüssel ist somit ein „umgewidmeter“ Tagesschlüssel eines Nutzers, der in der CWA App oder einer anderen nationalen Corona-App eine Warnung ausgelöst hat.

Der DSOS-Wert stellt die Differenz in Tagen zwischen der RollingStartNumber und dem **DOS (Date of Onset of Symptoms)** dar. Er wird Bestandteil der Tagesschlüssel, sobald sie als Positivschlüsseln verwendet werden.

Vor der Übermittlung durch die CWA App an den CWA Server setzt die CWA App zudem den TRL-Wert (siehe zu diesem Datenfeld die Beschreibung des Tagesschlüssels in Abschnitt 5.7.2). Zur Bestimmung des TRL-Werts verwendet die CWA App eine feststehende Zuordnungstabelle. Diese Zuordnungstabelle ist so aufgebaut, dass einer bestimmten

Kombination von Risikoparameter-Werten ein TRL-Wert zugeteilt wird. Welche Risikoparameter in der Zuordnungstabelle berücksichtigt werden, hängt davon ab, welche Version der CWA App beim Auslösen der Warnung verwendet wird:

CWA App < V1.5 (ENF V1):

Der TRL-Wert wird in Abhängigkeit vom Gültigkeitstag des jeweiligen Positivschlüssels relativ zu dem Tag, an dem die Warnung ausgelöst wird, festgelegt.

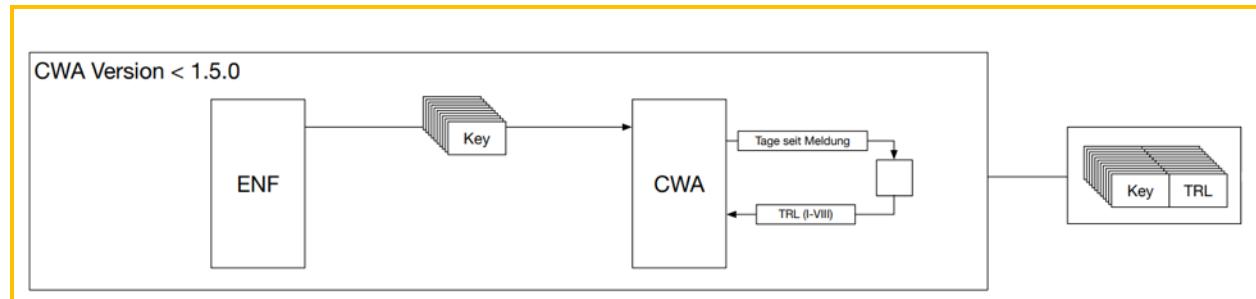


Abbildung 22: Bestimmung des TRL in der CWA App Version <1.5⁴⁶

Day since submissionDay	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Alter eines Positivschlüssels in Tagen															
TransmissionRiskLevel	I	I	I	I	I	I	I	I	III	V	VIII	VIII	VIII	VI	V

Abbildung 23: Zuordnungstabelle für die Bestimmung des TRL in der CWA App Version <1.5 [5]

CWA App >= V1.5 (ENF V1):

Der TRL-Wert wird weiterhin in Abhängigkeit vom Tag der Warnung festgelegt (siehe CWA App bis V1.5), zusätzlich werden nunmehr aber auch die Angaben zum Symptomstatus bzw. Symptombeginn (DOS) berücksichtigt. Wenn der CWA-Nutzer keine Angaben zum Symptombeginn macht, werden Standardwerte relativ zum Zeitpunkt des Testergebnisabrufs gesetzt.

⁴⁶ eigene Grafik.

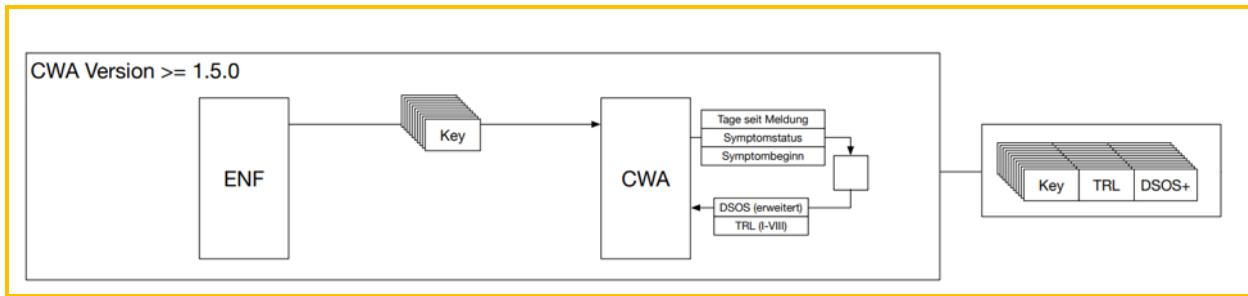


Abbildung 24: Bestimmung des TRL in der CWA App in Version <= 1.5⁴⁷

CWA App Version >= 1.8 (ENF V2):

Die CWA App ab Version 1.8 bestimmt den TRL-Wert anhand der Werte „Report Type“ (siehe Abschnitt 5.7.2) und „Infectiousness“ (Infektiosität).

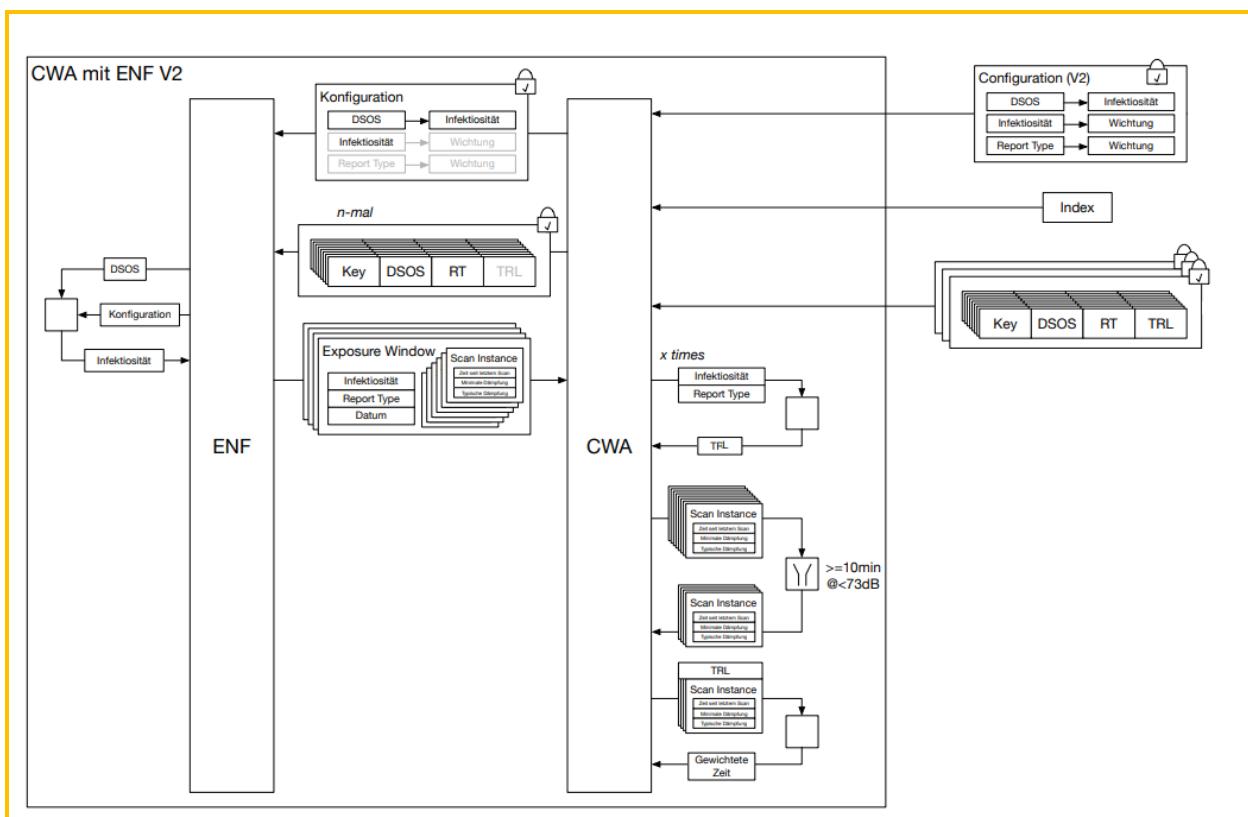


Abbildung 25: Übersicht auf der CWA App in Version 1.8 mit ENF V2⁴⁸

Die Infectiousness wird mit dem Wert High, Standard oder None angegeben, der nach Maßgabe der BWE aus den Angaben zum Symptombeginn abgeleitet wird.

⁴⁷ eigene Grafik.

⁴⁸ eigene Grafik.

Days since symptom onset	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+10	+11	+12	+13	+14
Infectiousness	None														Standard	High				Standard									
Weight	No weight														100%	200%				100%								None	No weight

Abbildung 26: Zuordnungstabelle zur Ermittlung der Infectiousness mit ENF V2⁴⁹

5.7.7 Metadaten zu Positivschlüsseln (CWA Server)

Nach Eingang der Positivschlüssel auf dem CWA Server werden dort zu allen durch die CWA App übermittelten Positivschlüsseln jeweils die Angaben zu DSOS und Report Type als Metadaten-Werte hinzugespeichert, so dass diese für Nutzer einer anderen Version der CWA App oder einer anderen nationalen Corona App für eine eigene (abweichende) Berechnungsmethode zur Bewertung des Risikos zur Verfügung stehen. Die Positivschlüssel werden dann mit diesen Metadaten an das CDN-Magenta weitergegeben und von dort schließlich an die CWA Apps der CWA-Nutzer verteilt.

Die DSOS- und Report-Type-Werte werden auf dem CWA Server anhand des im Positivschlüssel enthaltenen TRL-Werts gemäß folgender Zuordnungstabelle bestimmt:

TRL	Report Type	DSOS
1	1	1
2	2	1
3	3	1
4	4	1
5	1	2
6	2	2
7	3	2
8	4	2

Zudem wird auf dem CWA Server das Datenfeld „CountryOfOrigin“ ergänzt, welches das Ursprungsland des Positivschlüssels bezeichnet. Entsprechend den Spezifikationen des EFGS und des CHGS lautet der Wert bei Positivschlüsseln von CWA-Nutzern stets „DE“.

Die Metadaten zu Positivschlüsseln werden benötigt, um den Austausch bzw. die Kompatibilität von Warnungen einerseits zwischen CWA Apps unabhängig von der

⁴⁹ eigene Grafik.

verwendeten ENF-Version sowie andererseits zwischen CWA Apps und anderen nationalen Corona-Apps über das EFGS bzw. CHGS zu ermöglichen.

5.7.8 Bewertungseinstellungen (BWE)

Bei den BWE handelt es sich um eine komplexe Datenstruktur, die die Konfigurationseinstellung für die Risikobewertung der Kontakte des CWA-Nutzers beinhaltet.

Das Ergebnis der Berechnung auf Basis der BWE ist ein Wert, der das Infektionsrisiko des CWA-Nutzers in Bezug auf eine Begegnung angibt (Risikowert, siehe Ziffer 5.7.12). Der Risikowert wird dann in den dem CWA-Nutzer auf dem Home-Screen angezeigten Risikostatus übersetzt.

Die BWE werden vom RKI herausgegeben und aktualisiert. Es können auf diese Weise neueste epidemiologische Erkenntnisse in die Risiko-Ermittlung einfließen.

Der Aufbau und die Funktionsweise der BWE wird von den Festlegungen der Anbieter des ENF Apple und Google vorgegeben, so dass sich der Gestaltungsspielraum des RKI auf die Festlegung der Werte und Gewichtungen der vom ENF definierten Risikoparameter begrenzt.

Welche Werte für welche Risikoparameter festgelegt werden können hängt davon ab, welche Methode für die Berechnung und Angabe des Risikowerts gewählt wird. Das ENF sieht zwei Methoden vor:

- (1) Berechnung eines Score-Werts zwischen 0 und 4096⁵⁰
- (2) Berechnung von Meaningful Exposure Minutes (MEM)⁵¹

Die CWA App verwendete bisher die Methode 1, die mit dem ENF V1 eingeführt worden ist. Ab Release 1.8 wird die CWA App das ENF V2 verwenden und somit die MEM-Methode (Exposure Window mode) nutzen. Diese Methode ist auf iPhones mit iOS 14 oder höher und auf Android-Smartphones mit der im Rahmen des Google Play Service bereitgestellten Google API for Exposure Notifications v1.6 oder höher verfügbar, so dass der CWA-Nutzer ggf. ein Systemupdate durchführen muss, um die CWA App V1.8 installieren zu können.

Um die Kompatibilität der Risiko-Ermittlung zu früheren Versionen der CWA App zu gewährleisten, wird die CWA App für eine noch festzulegende Übergangszeit beide Methoden unterstützen. Auf technischer Ebene ist dies möglich, da höhere ENF-Versionen abwärtskompatibel sind.

⁵⁰ Apple und Google verwenden in der ENF-Dokumentation zur Bezeichnung dieser Methode das Schlagwort „V1“, vgl. <https://developers.google.com/android/exposure-notifications/exposure-notifications-api#rationale> („legacy v1 mode“, „v1 mode“), (abgerufen am 11.10.2022) und <https://developer.apple.com/documentation/exposurenotification/enexposureconfiguration> („V1 calculation“), (abgerufen am 11.10.2022).

⁵¹ In der ENF-Dokumentation wird diese Methode von Google als „Exposure Window mode“ und von Apple als „Meaningful Exposure Minutes (MEMs)“-Methode bezeichnet.

Nachfolgend werden die in den BWE definierten Risikoparameter und Rechenformeln für die Berechnungsmethoden beider ENF-Versionen beschrieben.

5.7.8.1 Berechnung eines Score-Werts (ENF V1)

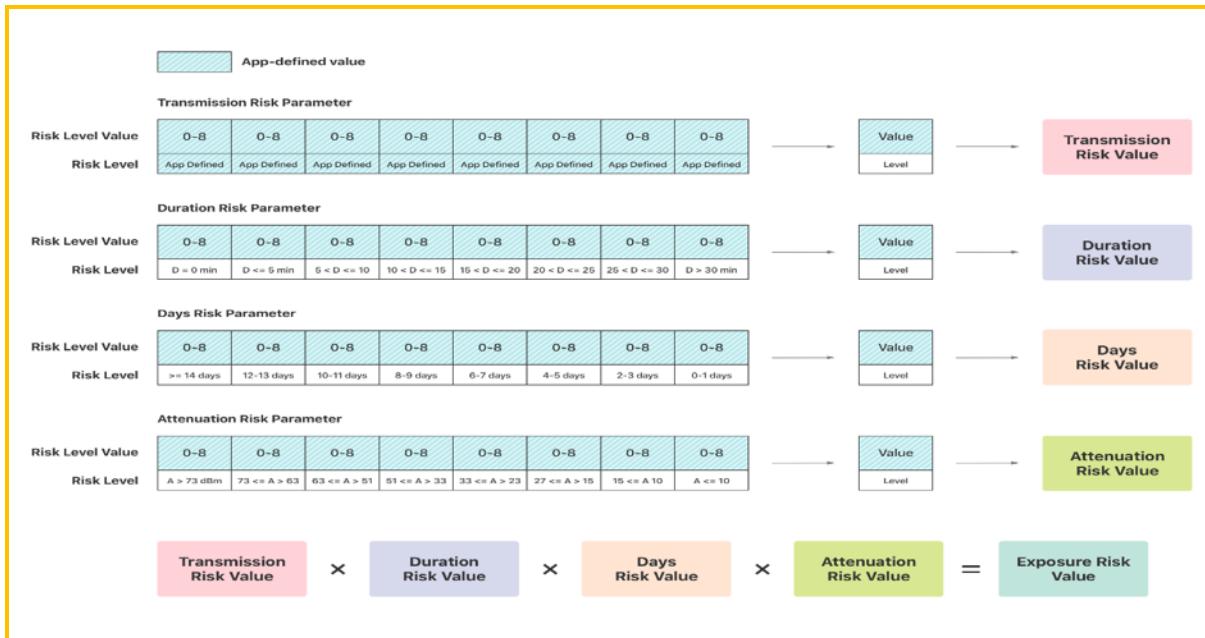


Abbildung 27: Übersicht Datenstruktur und Rechenformel bei der Berechnung als Score-Wert (Quelle: Apple/Google)

Wenn der Risikowert als Score-Wert berechnet wird, haben die BWE nach den Spezifikationen des ENF vier Risikoparameter, deren Risikostufen (Risk Level) und die entsprechenden Gewichtungswerte (Risk Level Value) jeweils teilweise vom RKI festgelegt werden müssen:

- (1) Transmission Risk Parameter: Dieser Risikoparameter bildet die Höhe des **Übertragungsrisikos** ab, das von der Kontaktperson ausgeht. Die Grenzwerte (Risk Level) werden vom RKI definiert. Der Gewichtungswert entspricht dem TRL-Wert des betreffenden Positivschlüssels.
- (2) Duration Risk Parameter: Dieser Risikoparameter bildet die summierte Dauer der Begegnungen mit einem positiv getesteten Nutzer an einem bestimmten Tag ab. Die Zuordnung erfolgt zu Zeitfenstern, die vom ENF V1 vorgegeben werden. Die Dauer der Begegnung wird den RPI-Metadaten entnommen (siehe Ziffer 5.7.4), sodass die Zuordnung in 5er Schritten erfolgt (<5/5/10/15/20/25/30/>30 Minuten).
- (3) Days Risk Parameter: Dieser Risikoparameter bildet den zeitlichen Abstand in Tagen seit der letzten Begegnung mit einem positiv getesteten Nutzer ab. Die Grenzwerte sind Tageszeiträume und werden vom ENF V1 vorgegeben.
- (4) Attenuation Risk Parameter: Dieser Risikoparameter bildet den durchschnittlichen räumlichen Abstand der Begegnungen mit einem positiv getesteten Nutzer ab. Die

Grenzwerte sind Dämpfungswert-Bereiche und werden vom ENF vorgegeben. Die Dämpfungswerte der Begegnung werden den RPI-Metadaten entnommen (siehe Ziffer 5.7.4).

Für die Berechnung des Risikowerts als Score-Wert multipliziert die CWA App die vier Gewichtungswerte, die den ermittelten Risikostufe jeweils zugeordnet sind:

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

5.7.8.2 Berechnung von MEM (ENF V2)

In der CWA App kommt ab Release 1.8 zur Risikoberechnung das Verfahren auf Basis der Methode 2 zum Einsatz, die seit der Veröffentlichung des ENF V2 zur Verfügung steht (ExposureWindow mode). Die Risikoberechnung des ENF V2 basiert auf sogenannten Exposure Windows, die vom ENF V2 in Form von Exposure-Window-Daten dargestellt werden.

Es gibt zwei Berechnungsoptionen, um den Exposure Window mode zur Auswertung der in den Exposure-Window-Daten enthaltenen Informationen zu nutzen: Zum einen kann eine von vom ENF V2 vorgegebene Formel genutzt werden, um aus den im ENF V2 gespeicherten Exposure-Window-Daten einen vorberechneten Risikowert (ERV) in Form eines MEM-Werts zu errechnen; die Berechnung erfolgt in diesem Fall durch das ENF V2, welches den errechneten ERV dann an die App übergibt. Zum anderen kann die App aber auch die Exposure-Window-Daten vom ENF V2 anfordern und diese unter Verwendung einer eigenen Formel verwenden, um einen selbst definierten Risikowert zu berechnen (manuelle Risikoberechnung⁵²). Das RKI hat sich aus noch darzustellenden Gründen für die manuelle Risikoberechnung entschieden.

Um die Risikoberechnungsoptionen und die Vorgehensweise des RKI vergleichen und bewerten zu können wird zunächst der Ablauf bei Verwendung von vorberechneten ERV dargestellt. Anschließend wird die vom RKI vorgesehene Umsetzung der manuellen Risikoberechnung dargestellt, welche seit Release 1.8 der CWA App zum Einsatz kommt.

⁵² In der ENF-Dokumentation von Google wird diese Vorgehensweise als „manual risk scoring“ bezeichnet, die für Gesundheitsbehörden den Vorteil eines größeren Gestaltungsspielraums bei der Risikoberechnung haben soll. Vgl. mit einer Beispielberechnung <https://developers.google.com/android/exposure-notifications/meaningful-exposures#example-manual> (Abruf: 02.12.2020).

5.7.8.2.1 Option 1: Vorberechnete MEM

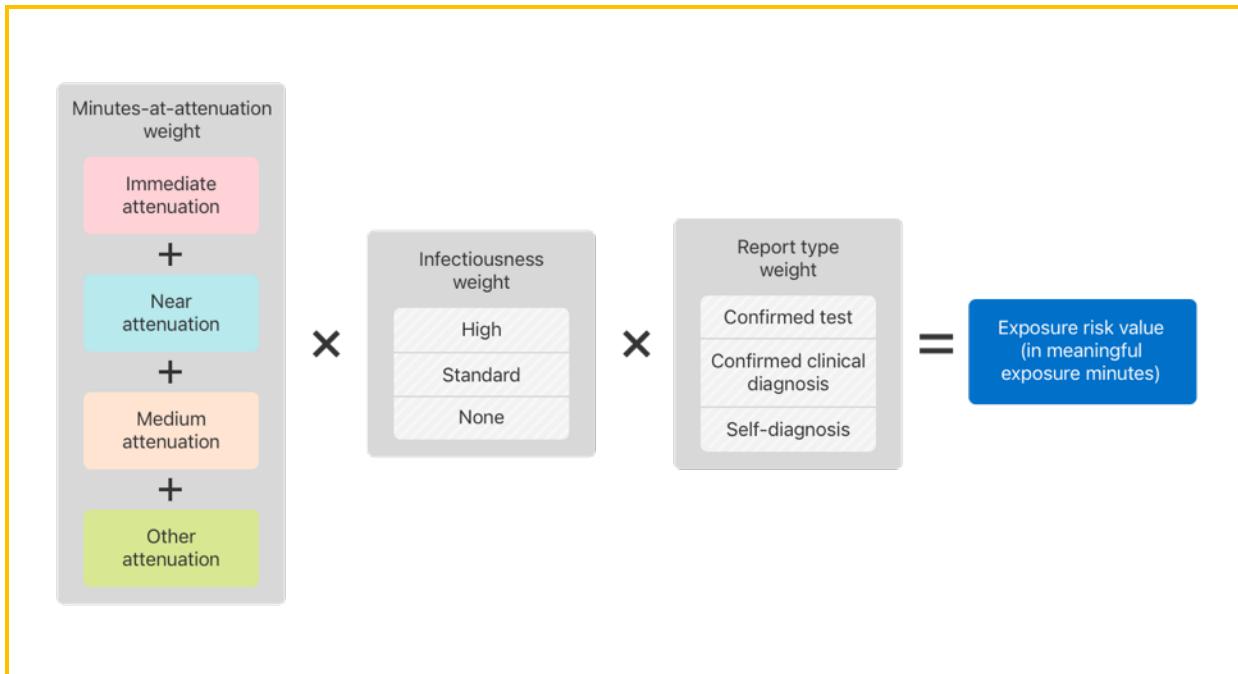


Abbildung 28: Übersicht Risikoparameter und Formel bei der Berechnung als MEM-Wert (Quelle: Apple/Google)

Wenn der Risikowert als vorberechneter Exposure Risk Value (ERV) berechnet wird, haben die BWE nach den Spezifikationen des ENF V2 drei Risikoparameter, deren Risikostufen und Gewichtungswerte (weight) jeweils vom App-Betreiber festgelegt werden:

- (1) Weighted minutes-at-attenuation: Dieser Risikoparameter bildet die Zeitspannen ab, in der sich der CWA-Nutzer an einem Tag in einem bestimmten räumlichen Abstand zu einem positiv getesteten Nutzer jeweils aufgehalten hat (Exposure Windows). Der räumliche Abstand wird in vier Risikostufen eingeteilt (immediate, near, medium, other). Die Zuordnung einer vom ENF aufgezeichneten Begegnung zu einer Risikostufe erfolgt anhand von Dämpfungswert-Bereichen und wird vom RKI festgelegt. Die niedrigste Risikostufe ist „other“ und kann verwendet werden, um Begegnungen mit epidemiologisch nicht relevanten räumlichen Abständen zuzuordnen. Die Dämpfungswerte sind Bestandteil der RPI-Metadaten (siehe Ziffer 5.7.4). Eine Begegnung, in deren Verlauf variierende Abstände aufgezeichnet worden sind, kann mehreren Risikostufen zugeordnet werden.
- (2) Infectiousness: Dieser Risikoparameter bildet die Infektiosität eines positiv getesteten Nutzers am Tag einer Begegnung ab. Die Risikostufe der Infektiosität wird auf einer dreistufigen Skala angegeben (High, Standard, None). Die Zuordnung einer Begegnung zu einer Infectiousness-Risikostufe erfolgt dabei relativ zum Wert DSOS (DaysSinceOnsetOfSymptoms), der mit den Positivschlüsseln verknüpft ist.
- (3) Report type: Dieser Risikoparameter gibt an, welche Diagnosemethode dem von einem positiv getesteten Nutzer geteilten Testergebnis zugrunde liegt. Die Angabe der

Diagnosemethode erfolgt in drei Kategorien, die jeweils einer Risikostufe entsprechen (confirmed test diagnosis, clinical diagnosis, self-reported diagnosis).

Die Gewichtungen der verschiedenen Risikostufen der einzelnen Risikoparameter werden vom App-Betreiber jeweils durch einen Wert zwischen 0 und 250 Prozent festgelegt, der als Multiplikator fungiert.

Für die Angabe des Risikowerts als ERV bzw. MEM-Angabe berechnet die App zunächst den Wert der Weighted minutes-at-attenuation durch Multiplikation der Dauer der Begegnung (auf Basis des Minutenwerts aus den vom ENF freigegebenen RPI-Metadaten) mit dem Prozentwert, der der Risikostufe dieser Begegnung zugeordnet ist. Der Minutes-at-attenuation-Wert muss somit nicht der tatsächlichen Dauer der Begegnung entsprechen.

$$\text{Weighted minutes-at-attenuation} = (\# \text{ of Minutes}) * (0-250\%)$$

Bei mehreren über einen Tag verteilten Begegnungen oder bei variierenden Risikostufen im Rahmen einer einzelnen Begegnung mit dem gleichen positiv getesteten Nutzer werden die Weighted-minutes-at-attenuation-Werte der einzelnen Begegnungen bzw. Risikostufen addiert.

Der Weighted-minutes-at-attenuation-Wert wird mit den Gewichtungswerten für die ermittelten Risikostufen der übrigen Risikoparameter (Infectiousness, Report type) multipliziert.

Beispielrechnung:

Das ENF von Nutzer A hat an Tag 1 mit dem Nutzer B eine 5-minütige Begegnung der Risikostufe „immediate“ (Gewichtung 150%), eine 15-minütige Begegnung der Risikostufe „medium“ (50%) und eine 30-minütige Begegnung der Risikostufe „other“ (0%). B ruft an Tag 4 über seine App ein von einem Labor hinterlegtes positives PCR-Testergebnis (Report type = Confirmed test) ab (200%). Noch am gleichen Tag löst B über seine App eine Warnung aus, wobei er angibt, dass er an Tag 2 erste Corona-Symptome bemerkt hat. Der DOS-Wert von B am Tag der Begegnung mit A beträgt somit +1, der der Risikostufe „High“ zugeordnet ist (200%).

Das Ergebnis der Berechnung ist ein Wert von 60 MEM:

Zunächst werden die Weighted-minutes-at-attenuation-Werte der einzelnen Begegnungen festgestellt und dann zu einem Gesamtwert addiert:

$$(5 \text{ Minuten} * 150\% = 7,5 \text{ Minuten}) + (15 \text{ Minuten} * 50\% = 7,5 \text{ Minuten}) + (30 \text{ Minuten} * 0\% = 0 \text{ Minuten}) = 15 \text{ Minuten}$$

Der Weighted-minutes-at-attenuation-Wert wird nun mit den Gewichtungswerten für die Faktoren Infectiousness und Report type multipliziert, um den ERV als MEM-Wert zu erhalten:

$$15 \text{ Minuten} * 200\% * 200\% = 60 \text{ MEM}$$

Der der MEM-Wert kann nun einem Risikostatus zugeordnet werden, so dass A beispielsweise über ein hohes Risiko informiert wird.

5.7.8.2.2 Option 2: Manuelle Risikoberechnung (CWA App ab V1.8)

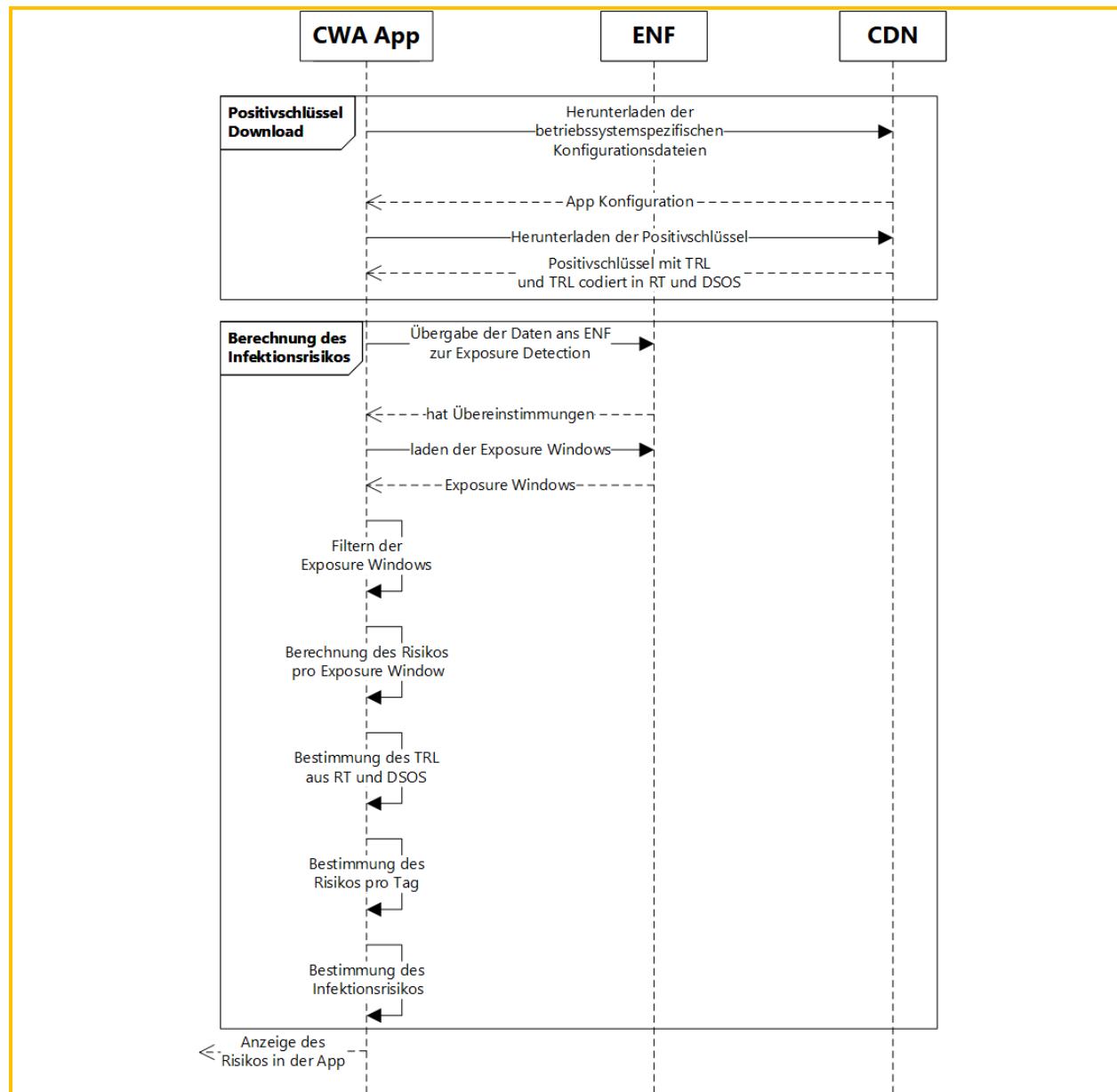


Abbildung 29: Verallgemeinerte Darstellung der Risikoberechnung der CWA App ab V1.8 mit ENF V2⁵³

Nachfolgend wird die von der CWA App verwendete Berechnungsmethode beschrieben:

⁵³ eigene Grafik.

Phase 1: Positivschlüssel-/Check-in-Download

In Phase 1 werden die vom CWA Server bereitgestellten Positivschlüssel bzw. Check-ins von der CWA App heruntergeladen.

Phase 2: Laden von Exposure Windows

Die heruntergeladenen Positivschlüssel werden an das ENF V2 übergeben. Dieses überprüft, ob es Übereinstimmungen gibt (siehe Abschnitt 5.6.1.3.1). Sofern das der Fall ist, erhält die CWA App die Exposure-Window-Daten zu den identifizierten Begegnungen.

Im Fall von heruntergeladenen Check-ins erfolgt das Matching und – im Fall eines Matches – auch das Erzeugen der Exposure-Window-Daten durch die CWA App selbst (siehe Abschnitt 5.6.1.3.2).

Phase 3: Berechnung des Infektionsrisikos nach Maßgabe der BWE

1. Filtern von Exposure Windows in Abhängigkeit von der gemessenen Bluetooth-Signalstärke (typicalAttenuation, minAttenuation) und der Begegnungsdauer (secondsSinceLastScan). Bei diesem Schritt werden die Exposure Windows aus der weiteren Auswertung herausgenommen, die aus Sicht des RKI epidemiologisch nicht relevant sind.

Bei gematchten Check-ins entfällt dieser Schritt, da keine Bluetooth-Signale anfallen. Stattdessen wird eine Vorfilterung bereits auf dem CWA Server durchgeführt, so dass Check-ins mit unbrauchbaren oder unplausiblen Angaben bereits auf Server-Ebene verworfen werden können.

2. Bestimmung des TRL. Bei diesem Schritt wird jeweils die TRL der verbleibenden Exposure Windows bestimmt. Die TRL ergibt sich bei Bluetooth-basierten Warnungen aus der Summe der Werte für Infectiousness und Report Type. Im Fall von Check-in-basierten Warnungen wird der im Check-in enthaltene TRL-Wert übernommen.

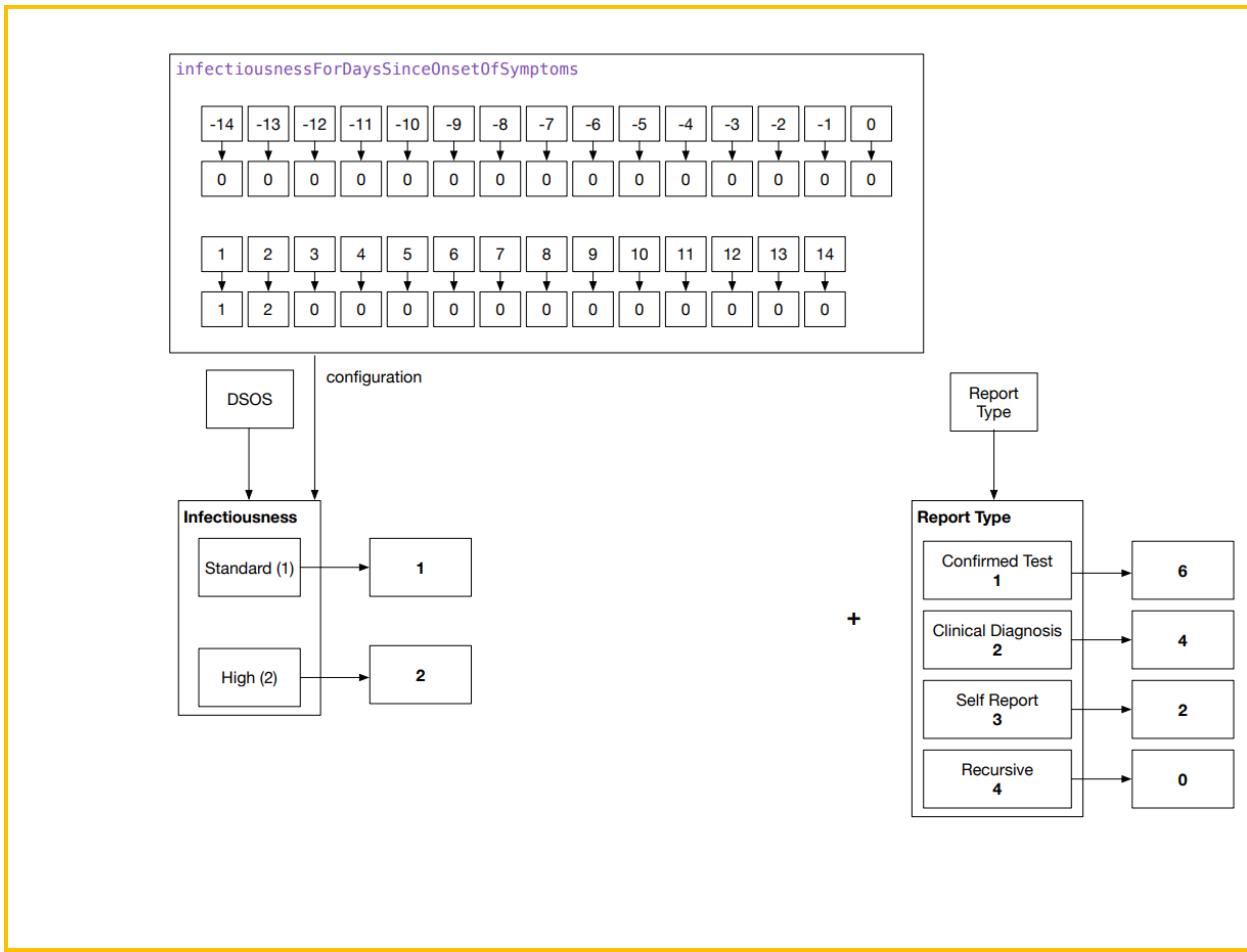


Abbildung 30: Berechnung des Transmission Risk Levels unter Verwendung des ENF V2⁵⁴

3. Nur bei Positivschlüssen: Nachdem die TRL der Exposure Windows bestimmt wurden, findet eine erneute Filterung statt. Dabei werden Exposure Windows, deren TRL unter einem bestimmten Wert liegt und daher aus epidemiologischer Sicht nicht relevant ist, bei der weiteren Risikoberechnung nicht mehr berücksichtigt.
4. Für die verbleibenden Exposure Windows wird der jeweilige TransmissionRiskValue-Wert ermittelt. Dieser ergibt sich aus der Multiplikation des soeben ermittelten TRL mit dem in den BWE festgelegten transmissionRiskLevelMultiplier-Wert.
5. Ermittlung des Weighted-minutes-at-attenuation-Werts (vgl. Option 1).
6. Berechnung der Normalized Time als MEM-Wert. Diese entspricht dem ERV (vgl. Option 1) und ergibt sich im Fall der CWA App aus der Multiplikation der Werte des TransmissionRiskValue und der Weighted-minutes-at-attenuation.
7. Ermittlung der Risiko-Begegnungen. Die Normalized-Time-Werte der Exposure Windows werden jeweils dem Risikowert „High“ oder „Low“ zugeordnet. Der Risikowert „High“ wird als Risiko-Begegnung eingestuft. Die Anzahl der Risiko-Begegnungen wird

⁵⁴ eigene Grafik.

dem CWA-Nutzer auf dem Home-Screen der CWA App angezeigt (z. B. „Keine Risiko-Begegnungen“).

- Ermittlung und Anzeige des Risikostatus. Die Normalized-Time-Werte der Exposure Windows werden addiert. Die Summe wird dann dem Risikostatus „Erhöhtes Risiko“ (wenn Summe ≥ 15 Minuten) oder „Geringes Risiko“ (wenn Summe < 15 Minuten) zugeordnet. Der Risikostatus wird dem CWA-Nutzer auf dem Home-Screen der CWA App angezeigt.

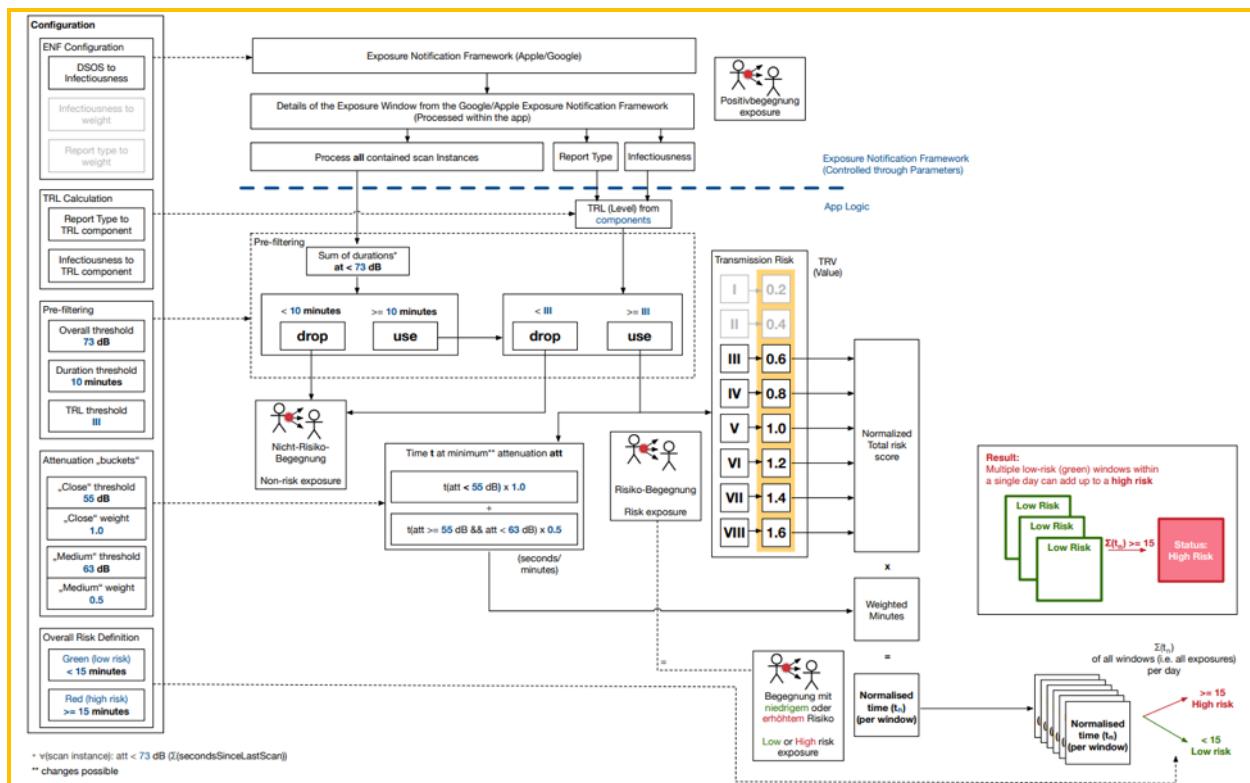


Abbildung 31: Übersicht zur Risikoberechnung in der CWA App ab V1.8 unter Verwendung des ENF V2⁵⁵

5.7.9 TAN

Die TAN ist eine einmal verwendbare Transaktionsnummer, die beim Abruf eines Testergebnisses automatisch generiert und dann in der CWA App abgelegt und zum Auslösen einer Warnung benötigt wird. Hat der CWA-Nutzer das Testergebnis nicht in der CWA App abgerufen, kann er eine teleTAN oder PIW-TAN eingeben, um eine TAN zu erhalten.

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.

⁵⁵ eigene Grafik.

5.7.10 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.

5.7.11 QR-Codes / GUID

Mehrere Funktionen der CWA verwenden jeweils einen funktionsspezifischen QR-Code. QR-Codes betreffen daher verschiedene Funktionen. Der Begriff bezeichnet deshalb stets einen bestimmten, Funktions-spezifischen QR-Code. Folgende Funktionen verwenden QR-Codes:

- Testregistrierung
- Event-Registrierung
- Schnelltest-Profil
- COVID-Impfzertifikat registrieren

Soweit sich die betreffende Funktion nicht aus dem jeweiligen Verwendungszusammenhang ergibt, ist der QR-Code für die Testregistrierung gemeint.⁵⁶

5.7.11.1 QR-Code für die Testregistrierung

Der QR-Code für die Testregistrierung wird einer Testperson bei Durchführung eines Corona-Tests mit Abnahme der Probe auf einem Probenbegleitschein ausgedruckt übergeben (bei PCR-Test) bzw. durch die Teststelle zur Verfügung gestellt (bei Schnelltest). 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. Bei Durchführung eines Schnelltests enthält der QR-Code zudem den Zeitpunkt der Testdurchführung. Sofern das Ergebnis des Schnelltests namentlich in der CWA App angezeigt werden soll, enthält der QR-Code außerdem Vor- und Nachname sowie Geburtsdatum des CWA-Nutzers, so wie gegenüber der Teststelle angegeben. Wenn der CWA-Nutzer den QR-Code scannt, übermittelt die CWA App 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 daher nicht zur Rückgabe

⁵⁶ Dies ist historisch bedingt. In den ersten Versionen der CWA App war der QR-Code für die Testregistrierung der einzige der CWA bekannte QR-Code. Daher war in der älteren CWA-Dokumentation keine Abgrenzung zu QR-Codes von anderen Funktionen erforderlich.

eines neuen Registration Token. Das Testergebnis kann nicht mehr von anderen mobilen Endgeräten mit installierter CWA App abgerufen werden.

Im Falle eines Schnelltests werden zudem die oben genannten weiteren Daten, soweit im QR-Code enthalten und zur (ggf. namentlichen) Anzeige des Testergebnisses benötigt werden, in der CWA App gespeichert (namentlicher Testnachweis, siehe Abschnitt 5.7.18).

5.7.11.2 QR-Code für Events

Siehe Abschnitt 5.7.21.2.

5.7.11.3 QR-Code für das Schnelltest-Profil

Siehe Abschnitt 5.7.21.

5.7.11.4 QR-Code für COVID-Zertifikate

Siehe Abschnitt 5.7.21.

5.7.12 Risikowert (Total Risk Score)

Der **Risikowert** gibt die Höhe des Infektionsrisikos eines Nutzers in Bezug auf eine oder mehrere im ENF aufgezeichnete Begegnungen mit einem bestimmten anderen Nutzer an einem Tag an. Der Risikowert berücksichtigt somit auch mehrere Begegnungen mit dem anderen Nutzer, die am gleichen Tag stattgefunden haben (sogenannte Begegnungsmenge).

Die Berechnung des Risikowerts erfolgt lokal in der CWA App und richtet sich nach den BWE der CWA App. Je nachdem, welche Berechnungsmethode in den BWE festgelegt ist, wird der Risikowert als Score-Wert zwischen 0 und 4096 oder als Minutenwert angegeben. Die Vorgehensweise zur Berechnung des Risikowerts wird ausführlich in den Abschnitten 5.7.8.1 (Angabe als Score-Wert) und 5.7.8.2 (Angabe als Minutenwert) beschrieben.

5.7.13 Risikostatus

Der Risikostatus wird im Rahmen der Risiko-Ermittlung ermittelt und gibt die Höhe des aktuellen Infektionsrisikos des CWA-Nutzers an. Er dient der Information der CWA-Nutzer und ermöglicht der CWA App die Anzeige von Risikostatus-spezifischen Hinweisen und Handlungsempfehlungen.

Der Risikostatus wird in zwei Stufen angegeben:

- Niedriges Risiko
- Erhöhtes Risiko

Der Risikostatus wird lokal in der CWA App ermittelt und gespeichert und nicht an das RKI, andere Nutzer oder sonstige Dritte weitergegeben.

Die Berechnung des Risikostatus erfolgt unter Berücksichtigung aller Risiko-Begegnungen und Check-ins der letzten 14 Tage, deren Risikowerte einen vom RKI festgelegten Grenzwert (also einen bestimmten Score- oder MEM-Wert) überschreitet.

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

5.7.14 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.

5.7.15 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.

5.7.16 Angaben zum Symptombeginn

Anlässlich einer Warnung kann ein positiv getesteter Nutzer optional Angaben zu dem Datum machen, an dem er zuerst Corona-Symptome festgestellt hat. Diese Angaben werden nur lokal in der App verarbeitet und nicht an das RKI, andere Nutzer oder sonstige Dritte weitergegeben. Die Angaben zum Symptombeginn dienen lediglich zur Konkretisierung des DOS- bzw. DSOS-Wertes und ermöglichen somit eine genauere Bestimmung des TRL bzw. Infectiousness.

5.7.17 Coronastatistik-Daten

Die Coronastatistik-Daten werden täglich auf dem CDN-Magenta hinterlegt und von dort an die CWA Apps der CWA-Nutzer verteilt. Die Coronastatistik-Daten enthalten vom RKI zusammengestellte, nicht personenbezogene Kennzahlen zum aktuellen nationalen und ggf.

lokalen Infektionsgeschehen und zur Nutzung der CWA App, die in der Statistik-Kachel auf dem Home-Screen der CWA App angezeigt werden.

Die Statistiken zum aktuellen Informationsgeschehen beruhen auf den Ergebnissen der Auswertung der von den Gesundheitsämtern gemäß IfSG an das RKI übermittelten Meldedaten, die vom RKI auch im Rahmen der laufenden Fallzahlenberichterstattung auf dem RKI-Dashboard unter <http://corona.rki.de> im Internet veröffentlicht werden müssen (§ 28a Abs. 3 IfSG). Die Statistiken zur Anzahl der über die CWA App ausgelösten Warnungen beruhen auf einem Vergleich der aggregierten Anzahl der vom Verifikationsserver in einem bestimmten Zeitraum ausgestellten TANs bzw. teleTANs mit der Anzahl der in einem Vergleichszeitraum von den installierten CWA Apps übermittelten Positivschlüssel.

Die lokalen Infektionsstatistiken werden an sieben verschiedenen Endpunkten des CDN - Magenta (/version/v1/local_stats_<id>, wobei <id> eine Ziffer zwischen 1 und 7 darstellt) zum Download für die CWA App bereitgestellt. Jeder Endpunkt liefert jeweils die aktuellen zusammengefassten Infektionsstatistiken eines oder mehrerer Bundesländer:

id	Bundesland (State id)
1	BW (7)
2	BY(9)
3	BE(11), BB(12), MV(13)
4	HB(4), HH(2), NI(3), SH(1)
5	NRW(5)
6	SN(14), ST(15), TH (16)
7	HE(6), RP (7), SL(10)

Die lokalen Datenpakete enthalten die zusammengefassten Statistiken für die jeweils enthaltenen Bundesländer sowie die entsprechenden Statistiken für jeden Landkreis bzw. Bezirk des jeweiligen Bundeslandes.

5.7.18 Schnelltest-Nachweis (Datenkategorie)

Der Schnelltest-Nachweis als Datenkategorie umfasst den QR-Code/Link, der auch für die Testregistrierung genutzt wird, die darin kodierten Angaben sowie den Vor- und Nachnamen und das Geburtsdatum der getesteten Person.

Wenn der CWA-Nutzer den QR-Code scannt bzw. den Link antippt, werden die darin enthaltenen Daten ausgelesen und in der CWA App gespeichert. Wenn das Schnelltest-Ergebnis vorliegt, wird es vom Test Result Server abgerufen und auf dem Home-Bildschirm der CWA App angezeigt. Wenn der Schnelltest negativ ist, kann der CWA-Nutzer die

Detailansicht des Schnelltest-Nachweises aufrufen. Dort wird das (negative) Testergebnis zusammen mit Vor- und Nachnamen, Geburtsdatum sowie dem Count-Up Timer angezeigt, so dass Dritte (z. B. Mitarbeiter von Geschäften) in Verbindung mit einem Identitätsnachweis (z. B. Ausweis) auf einen Blick prüfen können, ob die sich auf den Schnelltest-Nachweis berufende Person tatsächlich die Person ist, auf die sich der Schnelltest-Nachweis bezieht.

5.7.19 Schnelltest-Profil (Datenkategorie)

Ein Schnelltest-Profil umfasst zum einen alle vom CWA-Nutzer beim Anlegen des Schnelltest-Profils gespeicherten Angaben. Hier stehen folgenden Datenfelder zur Verfügung:

- Vorname
- Nachname
- Geburtsdatum
- Straße und Hausnummer
- Postleitzahl und Wohnort
- Telefonnummer
- E-Mail-Adresse

Es handelt sich nicht um Pflichtangaben, d. h. der konkrete Umfang und Inhalt des Schnelltest-Profils hängt davon ab, welche Datenfelder der CWA-Nutzer auf welche Weise tatsächlich ausfüllt.

Das Schnelltest-Profil ist in dem QR-Code enthalten, den der CWA-Nutzer bei der Teststelle vorzeigen und dadurch die manuelle Erfassung seiner Daten durch die Teststelle ersetzen kann (siehe Abschnitt 5.7.11.3).

5.7.20 Kontakt-Tagebuch-Einträge

Kontakt-Tagebuch-Einträge umfassen alle Daten zu den vom CWA-Nutzer in sein Kontakt-Tagebuch eingetragenen Kontaktpersonen, Orten und Treffen. Sie werden in vier verschiedenen Tabellen/Datenstrukturen mit jeweils zwei Spalten gespeichert.

Zwei dieser Tabellen enthalten jeweils die Stammdaten-Einträge. Stammdaten-Einträge bestehen aus den vom CWA-Nutzer eingetragenen Bezeichnungen für seine Kontaktpersonen („Tobias“) bzw. Orte („Bäcker“), ggf. deren Telefonnummer und E-Mail-Adresse sowie jeweils einer zufälligen Stammdaten-ID („1111“).

Zwei weitere Tabellen dienen der Speicherung der jeweiligen Informationen über die an einem bestimmten Tag vom CWA-Nutzer erfassten Kontaktpersonen und Orte, indem jeweils einem Datum die Stammdaten-IDs der an diesem Tag eingetragenen Kontaktpersonen bzw. Orte zugeordnet werden. Zusätzlich werden ggf. die weiteren Angaben der CWA-Nutzer zu den

Orten (Minutendauer des Besuchs des Ortes, Informationen zu äußereren Begleitumständen (Freitextfeld)) und Begegnungen (Dauer unter/über 15 Minuten; Aufenthalt drinnen/im Freien; Begegnung mit/ohne Maske; weitere Informationen zu Begleitumständen (Freitextfeld)) erfasst (Tageseinträge). Die CWA App greift auf diese Informationen zu und stellt sie in einer Kalenderansicht auf dem Hauptscreen des Kontakt-Tagebuchs dar.

5.7.21 Event-Daten

Die Kategorie der Event-Daten umfasst alle Daten, die spezifisch für die Zwecke der Event-Registrierung und die Risiko-Ermittlung auf Basis von geteilten Check-ins verarbeitet werden. Im Einzelnen sind dies:

- (1) Event-Details
- (2) QR-Code
- (3) Check-in-Details
- (4) Check-ins

5.7.21.1 Event-Details

Die Event-Details sind die Metadaten, die von der CWA App beim Anlegen eines Events lokal erzeugt und in einer Datenbanktabelle gespeichert werden. Neben den vom CWA-Nutzer (als Veranstalter) selbst eingegebenen Informationen zum Event (z. B. Typ und Bezeichnung des Events, Adresse/Ort, typische Aufenthaltsdauer, Startzeit des Events) erzeugt und speichert die CWA App auch eine zufallsgenerierte Event-GUID sowie einen zufälligen kryptografischen Seed Key.

5.7.21.2 QR-Code (für die Event-Registrierung)

QR-Codes für ein Event werden lokal von der CWA App erzeugt und enthalten eine kodierte URL mit folgender Struktur:

`https://e.coronawarn.app?v=1#<QR_CODE_PAYLOAD_BASE64URL>`

Der Platzhalter `<QR_CODE_PAYLOAD_BASE64URL>` repräsentiert die base64url-kodierten Event-Details.

Die Ziel-Domain im QR-Code (`https://e.coronawarn.app`) wird von der CWA App nicht aufgerufen und dient lediglich dazu, die Ziel-App für die kodierten Event-Details zu bezeichnen (hier: CWA App). Dies soll es ermöglichen, dass auch Event-Details für andere nationale Corona-Apps mit einer abweichenden Datenstruktur in dem gleichen QR-Code untergebracht werden können und somit perspektivisch eine länderübergreifende Event-Registrierung ermöglicht wird.

5.7.21.3 Check-in-Details

Die Check-in-Details umfassen die Angaben zu Events bei denen sich der CWA-Nutzer eingekickt hat und die beim Einchecken und Auschecken von der CWA App des CWA-Nutzers (als Gast) lokal in einer Datenbanktabelle gespeichert werden.

Beim Einchecken werden die aus dem QR-Code ausgelesenen dekodierten Event-Details, die Eincheckzeit sowie ein aus der Event-GUID unter Verwendung des im QR-Code enthaltenen Seed Keys abgeleiteter SHA-256-Hashwert gespeichert. Da dieser Hashwert bei jedem eingekickten CWA-Nutzer gleich ist, stellt er ein funktionales Äquivalent eines Positivschlüssels bei der ENF-basierten Risiko-Ermittlung dar, so dass die Risiko-Ermittlung und Warnung auf der Basis von Event-Daten leichter in die vorbestehenden Prozesse der CWA integriert werden kann. Beim (manuellen oder automatischen) Auschecken wird zudem die Auscheckzeit in Unixzeit hinzugespeichert.

5.7.21.4 Check-ins

Beim Auslösen einer Warnung werden von der CWA App von den Check-in-Details nur die gehashte Event-GUID, der diesbezügliche TRL-Wert und die jeweilige Eincheck- und Auscheckzeit (jeweils in 10-Minuten-Intervallen) zu einem Datensatz zusammengefasst und an den CWA Server übermittelt. Dieser Datensatz wird zur Abgrenzung von den lokal gespeicherten Check-in-Details als „Check-ins“ bezeichnet. Die Check-ins sind das funktionale Äquivalent zu den Positivschlüsseln bei Bluetooth-basierten Warnungen.

Seit Release 2.8⁵⁷ werden die Check-ins von der CWA App vor der Übermittlung in Form eines strukturierten CheckInProtectedReport-Datensatzes verschlüsselt:

MatchingKey	= SHA256(EventID)
EncryptionKey	= SHA256('CWA-KEY' EventID)
IV	= CRNG(16bytes)
EncryptedCheckIn	= AES-CBC(EncryptionKey, IV, VisitStart VisitEnd TRL)
MACKey	= SHA256('CWA-MAC-KEY' EventID)
MAC	= HMAC-SHA256(MACKey, IV EncryptedCheckIn)
CheckInProtectedReport	= MatchingKey IV EncryptedCheckIn MAC

5.7.22 Anwendungsdaten (Fehlerberichte)

Anwendungsdaten sind standardisierte technische Angaben zu bestimmten Ereignissen, die im Zusammenhang mit den Programmabläufen der CWA App eintreten. Ereignisse sind beispielsweise Fehlermeldungen, Datenbankzugriffe, Schnittstellenaufrufe oder bestimmte

⁵⁷ Der Hintergrund für die Änderung in diesem Release wird in Abschnitt 5.6.1.2.2 erläutert.

Nutzeraktionen (z. B. Starten der CWA App, Aufruf oder Deaktivierung einer bestimmten Funktion oder Änderung einer bestimmten App-Einstellung).

Die CWA App speichert Anwendungsdaten nur, wenn der CWA-Nutzer die Funktion „Fehlerberichte aufzeichnen“ aktiviert. In diesem Fall werden die Anwendungsdaten in einer lokalen Protokolldatei (Anwendungslog) chronologisch jeweils mit dem Zeitstempel des aufgezeichneten Ereignisses erfasst. Der CWA-Nutzer kann sich den Inhalt der Protokolldatei mittels der Teilen-Funktion in einfacher Textform ansehen.

Wenn die Fehlerberichtsaufzeichnung aktiviert ist, werden bestimmte Ereignisse, die personenbezogene Daten des CWA-Nutzers oder von Dritten enthalten können, von der Aufzeichnung im Anwendungslog ausgenommen bzw. nur in anonymisierter Form aufgezeichnet, da diese Informationen für die Fehleranalyse nicht erforderlich sind. Beispielsweise werden bei Ereignissen im Zusammenhang mit der Benutzung des Kontakt-Tagebuchs anstelle der im Einzelfall involvierten Kontakt-Tagebuch-Einträge nur technisch vergleichbare Zufallseinträge (z. B. gleiche Länge) aufgezeichnet. Ebenso werden in der CWA App im Rahmen der Online-Validierung verarbeitete personenbezogene Daten wie Buchungsanforderungen oder die Zertifikatsaussagen nicht in den Fehlerberichten erfasst. Daher enthalten die Anwendungslogs keine personenbezogenen Daten, die unmittelbar den Rückschluss auf den CWA-Nutzer ermöglichen.

5.7.23 Zertifikatsaussage

Die als Zertifikatsaussage zusammengefassten Daten umfassen die in einem COVID-Zertifikat in menschen- und maschinenlesbarer Form jeweils enthaltenen überprüfbaren personenbezogenen Daten des Zertifikatsinhabers zu seinem Impf-, Test- oder Genesenestatus.

Die Datenfelder der verschiedenen Zertifikatstypen entsprechen den jeweiligen Listen im Anhang der DCC-VO, mit der die für die länderübergreifende Prüfung und Anerkennung der digitalen COVID-Zertifikate erforderliche Einheitlichkeit gewährleistet wird. Für nationale Zwecke dürfen grundsätzlich zwar weitere Datenfelder aufgenommen werden. Von dieser Möglichkeit macht das RKI bei den in Deutschland ausgestellten COVID-Zertifikaten zurzeit jedoch keinen Gebrauch.

5.7.23.1 Impfstatus

Die Datenkategorie des Impfstatus umfasst folgende Angaben:

Feld	Beispiel
Name	Mustermann
Vorname	Erika

Feld	Beispiel
Standardisierter Name	MUSTERMAN, ERIKA
Geburtsdatum	02.06.1965
Impfdatum	03.06.2021
Land	Deutschland
Aussteller	RKI
Krankheit	U07.1
Impfstoff	1119349007 (mRNA-Impfstoff), 1119305005 (Vektor-Impfstoff)
Produkt / Hersteller	Moderna, BioNTech
Nummer der Impfung	„1 von 1“, „1 von 2“, „2 von 2“, „3 von 3“ ⁵⁸
Zertifikat gültig bis	03.06.2021, 16:55
Eindeutige Zertifikatskennung	siehe Abschnitt 5.7.25

5.7.23.2 Genesenenstatus

Die Zertifikatsaussage bei Genesenenzertifikaten umfasst folgende Angaben zum Genesenenstatus des Zertifikatsinhabers:

Feld	Beispiel
Name	Mustermann
Vorname	Erika
Standardisierter Name	MUSTERMAN, ERIKA
Geburtsdatum	02.06.1965

⁵⁸ Seit September 2021 werden in Deutschland auch sogenannte Auffrischimpfungen, also erneute Impfungen nach dem vollständigen Abschluss einer Impfserie, durchgeführt und entsprechende Impfzertifikate ausgestellt. Der Wert des Felds „Nummer der Impfung“ wird in diesem Fall gemäß Anhang II Nummer 5 des Durchführungsbeschluss (EU) 2021/1073 vom 28. Juni 2021 zur Festlegung technischer Spezifikationen und Vorschriften für die Umsetzung des mit der Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates geschaffenen Vertrauensrahmens für das digitale COVID-Zertifikat der EU dargestellt (z. B. „2 von 3“ oder „3 von 3“).

Feld	Beispiel
Datum der positiven Testung	12.07.2021
Land der Testung	Deutschland
Aussteller	RKI
Krankheit	U07.1
Zertifikat gültig ab	12.07.2021
Zertifikat gültig bis	08.01.2022
Eindeutige Zertifikatskennung	siehe unter 5.7.25

5.7.23.3 Teststatus

Die Zertifikatsaussage bei Testzertifikaten umfasst folgende Angaben zum Teststatus des Zertifikatsinhabers:

Feld	Beispiel
Name	Mustermann
Vorname	Erika
Standardisierter Name	MUSTERMANN, ERIKA
Geburtsdatum	02.06.1965
Datum der Probenahme	03.06.2021
Datum der Ergebnisfeststellung	03.06.2021
Land	Deutschland
Aussteller	RKI
Krankheit	U07.1
Testtyp	Schnell-Immunassey
Testname	Roche LightCycler qPCR
Produkt / Hersteller	BIOSYNEX S.A., BIOSYNEX COVID-19 Ag BSS

Feld	Beispiel
Testzentrum	Testzentrum Hamburg 1
Testresultat	Erkannt
Eindeutige Zertifikatskennung	siehe unter 5.7.25

5.7.24 Eindeutige Zertifikatskennung

Die eindeutige Zertifikatskennung ist der Identifikator für ein COVID-Zertifikat. Sie besteht aus einer alphanumerischen Zeichenfolge und enthält keine Angaben, die sie mit anderen Dokumenten oder Kennungen wie Pass- oder Personalausweisnummern verknüpft, damit eine direkte Zuordnung zur Person des Zertifikatsinhabers verhindert wird. Durch die eindeutige Zertifikatskennung wird auch der länderübergreifende Widerruf von ungültigen COVID-Zertifikaten über das EU-Gateway ermöglicht, indem Zertifikatswiderrufslisten zwischen den am EU-Gateway angeschlossenen Ländern ausgetauscht werden. Im aktuellen Release werden derartige länderübergreifende Widerrufslisten jedoch nicht umgesetzt.⁵⁹

Bei Impfzertifikaten wird der Unique Vaccination Certificate Identifier (UVCI) als eindeutige Zertifikatskennung in der Form von Option 3 der aktuellen Interoperabilitätsrichtlinien für Impfzertifikate des eHealth-Netzwerks⁶⁰ verwendet. Der UVCI besteht somit aus vier Segmenten: Die ersten zwei Segmente sind für alle Zertifikatsinhaber, die ihr COVID-Zertifikat von einer bestimmten bescheinigenden Stelle erhalten haben, gleich und werden mit dem Wert „01DE“ dargestellt. Der letzte Block enthält eine kryptografische Prüfsumme. Der dritte Block *Opaque Unique String* ist eine zufällige eindeutige Zeichenfolge, die kollisionssicher erzeugt wird. Beispiel für eine UVCI zu einer Impfung im Impfzentrum Landkreis Altötting (84503):

01DE/84503/DXSGWLWL40SU8ZFKIYIBK39A3#S

Die Struktur von eindeutigen Zertifikatskennungen für Test- und Genesenenzertifikate wird vom eHealth-Netzwerk nicht detailliert vorgegeben. Die vom RKI festgelegte Struktur für diese

⁵⁹ Ein Zertifikatswiderruf ist bisher in einer Konstellation erfolgt. Da in diesem Fall alle zu widerrufenden Zertifikate von derselben dem RKI bekannten bescheinigenden Stelle ausgegeben worden sind, hat sich das RKI zu einem Widerruf aller von dieser Stelle ausgegebenen Zertifikate entschlossen. In technischer Hinsicht konnte dieses Ziel mit einem Widerruf aller Zertifikate, die in ihrer eindeutigen Zertifikatskennung die gleichen zwei ersten Blöcke der ausgebenden Stelle enthielten, erreicht werden. Eine Verarbeitung von vollständigen, d.h. personenbezogenen eindeutigen Zertifikatskennungen war somit nicht erforderlich.

⁶⁰ eHealth Network, Guidelines on verifiable vaccination certificates – basic interoperability elements, Release 2 vom 12.03.2021.

Zertifikatstypen orientiert sich an der Struktur der UVCI. Dies entspricht der Empfehlung des eHealth-Netzwerks.⁶¹

5.7.25 COVID-Zertifikate

Ein COVID-Zertifikat bescheinigt gemäß den Vorgaben der EU-Verordnung über das digitale COVID-Zertifikat in den jeweiligen Amtssprachen und mindestens in englischer Sprache, dass der Zertifikatsinhaber in dem Mitgliedstaat, der die Bescheinigung ausstellt, eine Schutzimpfung erhalten oder einen negativen Corona-Test durchgeführt hat oder ihm eine Genesung von einer durchgemachten Corona-Infektion bescheinigt worden ist. COVID-Zertifikate können in Papierform und in elektronischer Form genutzt werden.

Ein COVID-Zertifikat enthält die jeweilige Zertifikatsaussage (siehe 5.7.23), also menschenlesbare Angaben zum bescheinigten Impf-, Test- oder Genesenestatus, sowie den maschinenlesbaren (digitalen) QR-Code, mit dem das COVID-Zertifikat elektronisch gespeichert und von Dritten mit einem Prüfsystem geprüft werden kann. Das COVID-Zertifikat in Papierform und die elektronisch gespeicherte Version in der CovPass-App oder CWA App sind gleichwertig (ErwG 18 DCC-VO).

5.7.26 Online-Validierungsdaten

Nachfolgend werden die bei der Nutzung des Online-Validierungsverfahrens bei einem Leistungsanbieter mit der CWA App relevanten Datenkategorien beschrieben. Die vom RKI umgesetzte Lösung entspricht der Referenzlösung der EU-Kommission, die wiederum auf den Vorschlägen des eHealth-Netzwerks basiert.

5.7.26.1 Initialisierungs-QR-Code

Für die Einleitung des Online-Validierungsverfahrens benötigt der Nutzer einen buchungsspezifischen Initialisierungs-QR-Code. Der Initialisierungs-QR-Code wird vom Leistungsanbieter erzeugt und enthält einen Initialisierungs-Token mit einer Transaktions-ID, einer kurzen menschenlesbaren Bezeichnung des Buchungsvorgangs (z. B. „Buchungsnummer 1234“), eine (Kurz-)Bezeichnung des Leistungsanbieters (z. B. „Lufthansa“) sowie eine URL, unter der die Wallet-App das vom Leistungsanbieter bereitgestellte Identity Document mit den für den jeweiligen Validierungsvorgang benötigten Buchungsdetails abrufen kann.

⁶¹ eHealth Network, Guidelines on COVID-19 citizen recovery interoperable certificates – minimum dataset, Release 1 vom 15.03.2021, S. 7 (dort in der Zeile zum “Certificate Identifier”).

Die Struktur der Initialisierungs-QR-Codes wird vom eHealth-Netzwerk nicht verbindlich oder abschließend vorgegeben.

5.7.26.2 Identity Document

Ein Identity Document bezieht sich stets auf einen spezifischen Buchungsvorgang, wird also für jeden diesbezüglich erfolgenden Validierungsvorgang individuell erzeugt. Verantwortlich für die Erzeugung und Bereitstellung des Identity Documents ist der Leistungsanbieter.

Das Identity Document enthält Angaben zu den für die Online-Validierung verwendeten Server-Endpunkten des Leistungsanbieters und des von ihm genutzten Validierungsdienstes, den vom Leistungsanbieter und der Wallet-App für das weitere Validierungsverfahren benötigten Public Keys und eine menschenlesbare Bezeichnung des Validierungsdienstes, die dem CWA-Nutzer in der CWA App zu Kontrollzwecken vor der Übermittlung des COVID-Zertifikats an den Validierungsdienst angezeigt wird.

Das Identity Document ist bei einer den Richtlinien des eHealth-Netzwerks entsprechenden Umsetzung des Backendsystems des Leistungsanbieters mit einem privaten Schlüssel des Leistungsanbieters elektronisch signiert und darf von der Wallet-App nur geladen werden können, wenn diese das korrekte Initialisierungs-Token aus dem Initialisierungs-QR-Code an das Backendsystem des Leistungsanbieters übermittelt.

5.7.26.3 Validation Access Token

Der Validation Access Token wird vom Leistungsanbieter generiert. Dies erfolgt nach der Referenzimplementierung durch den Dienst „*validation decorator*“. Der Validation Access Token kann von der CWA App von dem im Identity Document genannten Server-Endpunkt heruntergeladen werden. Der Validation Access Token ist mit einem für den jeweiligen Validierungsvorgang generierten Private Key des Leistungsanbieters signiert und enthält den vom Leistungsanbieter festgelegten Identifier des zugehörigen öffentlichen Schlüssels (z. B. „AccessTokenSignKey-663290“) sowie die vom Leistungsanbieter festgelegten Validierungsanforderungen.

Der zur Überprüfung der Echtheit der Signatur des Validation Access Token notwendige öffentliche Schlüssel des Leistungsanbieters wird im Identity Document wiedergegeben. Die CWA App setzt den Validierungsprozess nur fort, wenn ausschließlich der im Validation Access Token genannte Identifier des öffentlichen Schlüssels im Identity Document genannt wird und mit dem zugehörigen, ebenfalls im Identity Document enthaltenen Public Key die Echtheit der Signatur des Validation Access Token bestätigt werden kann.

5.7.26.4 Validierungsanforderungen

Die Validierungsanforderungen stellen eine Datenstruktur im Payload des Validation Access Token dar und umfassen die zur Durchführung der Online-Validierung vom Leistungsanbieter festgelegten vorgangsspezifischen Anforderungen an das zu validierende COVID-Zertifikat:

- Vorname und Name des Zertifikatsinhabers
- Geburtsdatum des Zertifikatsinhabers
- Bei Reisebuchungen:
 - Ausgangsland und -region der Transaktion
 - Zielland und -region der Transaktion
- Anforderungen an die Zertifikatskategorie (z. B. Impfzertifikat)
- Anzuwendende Business Rules, etwa spezielle Business Rules für Konzerte, Großveranstaltungen (wenn keine speziellen Business Rules angegeben werden, werden die Standard-Business-Rules angewendet)
- Datum der erforderlichen Gültigkeit des Zertifikats (Reisedatum oder Veranstaltungsdatum)
- Beginn und Ende des notwendigen Gültigkeitszeitraums des Zertifikats

Die Datenstruktur ist vom Leistungsanbieter signiert und die Signatur wird bei der vom eHealth-Netzwerk vorgeschlagenen Umsetzung vom Validierungsdienst geprüft, um Veränderungen der Datenstruktur auf dem Übermittlungsweg vom Leistungsanbieter zur Wallet-App und von der Wallet-App zum Validierungsdienst ausschließen zu können. Die konkrete Datenstruktur wird vom eHealth-Netzwerk nicht verbindlich oder abschließend vorgegeben. Die vom RKI festgelegte Struktur entspricht jedoch den Vorschlägen des eHealth-Netzwerks⁶² und muss daher von Leistungsanbietern eingehalten werden, sofern sie ihren Nutzern die Online-Validierung mit einer Wallet-App des RKI ermöglichen wollen.

5.7.26.5 Result Token / Validierungsergebnis

Der Result Token wird vom Validierungsdienst nach dem Abschluss der Validierung erzeugt. Er ist mit dem Private Key des Validierungsdienstes signiert und enthält das Validierungsergebnis sowie im Fall einer erfolglosen Validierung eine Begründung unter Bezeichnung der Validierungsanforderungen, die vom Validierungsdienst als nicht erfüllt bewertet worden sind. Die Begründung wird den Vorschlägen des eHealth-Netzwerks entsprechend nur an die Wallet-App des übermittelnden Wallet-Nutzers übermittelt. Der

⁶² eHealth Network, Guidelines on the use of Digital Covid Certificates in traveller and online booking scenarios, V1.2.0 vom 21.10.2021, S. 15 ff.

Leistungsanbieter erhält keine Rückmeldung, an welcher Validierungsanforderung die Validierung gescheitert ist.

Das Validierungsergebnis kann folgende Werte haben:

- OK (Validierung erfolgreich)
- NOK (Validierung nicht erfolgreich)
- CHK (Validierung ohne Ergebnis / offen)

5.7.27 Nutzungsdaten (Datenspende)

Die im Rahmen der Datenspende von teilnehmenden CWA-Nutzern zur Verfügung gestellten Nutzungsdaten enthalten folgende einzelnen Datenpunkte:

Nr.	Datenpunkt	Zweck
0.1	- <i>Created At</i> (YYYY-MM-DD)	(= <i>Submission Date</i>) Ermöglicht zeitliche Einordnung auf Tagesbasis
0.2	- <i>User Metadata</i> (Federal state, Kreis/Bezirk, Age Group (-29, 30 - 59, 60+))	Freiwillige Zusatzangaben: Geographische (administrative) Zuordnung (Bundesland / Kreis bzw. Bezirk) und grobe Altersangabe erlauben gezieltere Problemerkennung und Kommunikation sowie die Bewertung möglicher Auswirkungen regionaler Corona-Maßnahmen auf die Wirksamkeit der CWA
0.3	- <i>Client Metadata</i> (CWA Version, OS Version, ENF Version (Android only), App Config Hash)	Ermöglicht Identifizierung bzw. Eingrenzung von technischen Fehlerquellen (es werden keine nutzerspezifischen IDs, sondern nur die Versionsangaben erhoben)
1	Exposure Risk Metadata (once daily)	Abschätzung des Anteils von (neu) gewarnten CWA-Nutzern (tagesgenau); dient der Kalibrierung der Risikoberechnung
1.1	- <i>Created At, User Metadata</i>	s.o.
1.2	- <i>Risk Level (red/green)</i>	Ermöglicht Bildung des o.g. Anteils
1.3	- <i>Risk Level changed compared to previous submission (y/n)</i>	Ermöglicht Bildung des o.g. Anteils
1.4	- <i>Most recent date with exposure at risk level (if any)</i>	Dient der Abschätzung des Verzugs zwischen Risikobegegnung und Warnung
1.5	- <i>Date changed compared to previous submission (y/n)</i>	Dient der Abschätzung des Verzugs zwischen Risikobegegnung und Warnung
2	New Exposure Window (EW)	Abschätzung der Genauigkeit des GAEN; dient der Verbesserung der Risikoberechnung
2.1	- <i>Created At, Client Metadata</i>	s.o.
2.2	- <i>EW Header:</i>	

Nr.	Datenpunkt	Zweck
	<ul style="list-style-type: none"> • Date • RT, DSOS, TRL • CC 	<ul style="list-style-type: none"> • Zeitliche Einordnung (nur Datum) • Dient der Verbesserung des Algorithmus zur Abschätzung der Infektiosität der Indexperson • Kalibrierungsverlässlichkeit des BLE-Signals
2.3	- Scan Instances of EW	Bestandteil der Risikoermittlung
2.4	- Normalized Time of EW	Bestandteil der Risikoermittlung
3	Test Result Metadata	Abschätzung des Anteils von gewarnten CWA-Nutzern, die sich infiziert haben; Abschätzung des Anteils von infizierten Nutzenden, die andere warnen; dient der Verbesserung der Risikobewertung durch Hinweise zur Optimierung von Sensitivität und Spezifität
3.1	- Created At, User Metadata	s.o.
3.2	- Test Result	Ermöglicht Bildung des o.g. Anteils
3.3	- Hours Since Test Registration	Ermöglicht Auswertung des Verzugs zwischen Testregistrierung und Bereitstellung des Ergebnisses in der CWA (Evaluation der Zeitnähe)
3.4	- Risk Level at Test Registration	Ermöglicht Aussage, ob zum Zeitpunkt der Testregistrierung ein erhöhtes Risiko angezeigt wurde
3.5	- Days since most recent high risk at Test Registration	Verzug seit dem Tag des erhöhten Risikos
3.6	- Hours since high risk warning at Test Registration	Verzug seit Anzeige des erhöhten Risikos
4a	Key Submission Metadata (with user metadata)	Abschätzung des Anteils von infizierten Nutzenden, die andere warnen, und der Umstände, die zum Warnen führten
4a.1	- Created At, User Metadata	s.o.
4a.2	- Keys shared (y/n)	Ermöglicht Bildung des o.g. Anteils
4a.3	- Submitted after symptom flow (y/n)	Anteil der CWA-Nutzer, die Angaben zu ihren Symptomen gemacht haben
4a.4	- Submitted with TeleTAN (y/n)	Unterscheidung TAN/teleTAN als Verifikationsmittel der Key Submission, zur Plausibilisierung fehlender Bezüge zur Testregistrierung (z.B. fehlende Angabe in Hours since Test Registration)
4a.5	- Hours since reception of test result	Abschätzung des Verzugs von der Bereitstellung des Testergebnisses in der CWA App bis zum Warnen Anderer; Beitrag zum Nachweis der Wirksamkeit der CWA
4a.6	- Days since most recent high risk at Test Registration	Abschätzung des Verzugs vom jüngsten Tag mit erhöhtem Risiko bis zur Testregistrierung

Nr.	Datenpunkt	Zweck
4a.7	- Hours since high risk warning at Test Registration	Abschätzung des Verzugs von der Risikowarnung bis zur Testregistrierung
4a.8	- Hours since Test Registration	Abschätzung des Verzugs von der Testregistrierung in der CWA App bis zum Warnen Anderer
4b	Key Submission Metadata (with client metadata)	Abschätzung des Anteils von infizierten CWA-Nutzern, die andere warnen, und der Umstände, die zum Warnen führten
4b.1	- Created At, Client Metadata	s.o.
4b.2	- Keys shared (y/n)	Ermöglicht Bildung des o.g. Anteils
4b.3	- Submitted in background (y/n)	Ermöglicht Einschätzung der Wirksamkeit der Maßnahmen zur Optimierung der Nutzerführung im Rahmen der Warnung anderer
4b.4	- Submitted after cancel (y/n)	s.o.
4b.5	- Submitted after symptom flow (y/n)	Anteil der CWA-Nutzer, die Angaben zu ihren Symptomen gemacht haben
4b.6	- Submitted with advanced consent (y/n)	Ermöglicht Einschätzung der Wirksamkeit der Maßnahmen zur Optimierung der Nutzerführung im Rahmen der Warnung anderer
4b.7	- Last submission flow screen (Test Result, Warn Others, Symptoms 1/2)	s.o.

5.8 Löschung der Daten

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

5.8.1 Daten der Risiko-Ermittlung

Für alle für die Zwecke der Risiko-Ermittlung und der Berechnung des Infektionsrisikos 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 Löschfristen 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 Daten der Testregistrierung

Für alle im Rahmen der Testregistrierung 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.

Die Kopie 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 Daten der Warnfunktion

Für alle im Rahmen der Warnfunktion 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 der teleTAN bzw. PIW-TAN, die auf dem CWA Server gespeichert sind, werden nach 21 Tagen gelöscht.

Die TAN und die teleTAN bzw. PIW-TAN, 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 bzw. PIW-TAN, 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 Schnelltest-Profile

Die Schnelltest-Profile werden nur lokal im App-Speicher der CWA App gespeichert. Sie werden dort gelöscht, sobald der CWA-Nutzer eine manuelle Löschung vornimmt oder er die CWA App zurücksetzt.

5.8.5 Testergebnisse und Schnelltest-Nachweise

In der CWA App angezeigte PCR-Testergebnisse können jederzeit manuell durch den CWA-Nutzer gelöscht werden.

Ein namentlicher Testnachweis und ein negatives Schnelltest-Ergebnis werden für 48 Stunden in der CWA App als gültig angezeigt. Anschließend werden die Details zum Schnelltest nicht mehr angezeigt und der CWA-Nutzer erhält einen Hinweis, dass der Schnelltest nicht mehr aktuell ist.

Ein positives Schnelltest-Ergebnis wird angezeigt, bis der CWA-Nutzer andere gewarnt hat oder die App zurücksetzt hat. Eine automatische Löschung von Schnelltest-Ergebnissen erfolgt aktuell nicht.

Gelöschte Testergebnisse und Schnelltest-Nachweise werden zunächst in den Papierkorb verschoben. Der Papierkorb zeigt jeweils das Löschdatum an und erlaubt die Wiederherstellung der gelöschten Elemente. Nach 30 Tagen werden die gelöschten Elemente automatisch endgültig gelöscht.

5.8.6 Kontakt-Tagebuch-Einträge

Die Stammdaten-Einträge von Kontaktpersonen und Orten können vom CWA-Nutzer im Menü des Kontakt-Tagebuchs jederzeit manuell bearbeitet und gelöscht werden. Wenn keine manuelle Löschung von Stammdaten-Einträgen durchgeführt wird, erfolgt deren Löschung im Zuge der Deinstallation oder des Zurücksetzens der CWA App. Im Fall der Löschung eines Stammdaten-Eintrags wird auch dessen jeweilige Stammdaten-ID gelöscht. Die automatische

Lösung von Stammdaten-Einträgen, etwa nach 14 Tagen, ist nicht vorgesehen, um dem CWA-Nutzer die schnelle Eintragung von wiederkehrenden Kontakten auch bei längeren Kontaktabständen zu ermöglichen.

Die Tageseinträge werden nach 16 Tagen automatisch gelöscht. Zwar endet der epidemiologisch relevante Zeitraum von Tageseinträgen nach derzeitigem Kenntnisstand jeweils schon nach 14 Tagen. Da jedoch der Löschzeitpunkt ausgehend vom Eintragungsdatum anhand der jeweils aktuellen Systemzeit des Smartphones festgelegt wird, ist die um zwei Tage längere Aufbewahrungsdauer erforderlich, um im Fall von Reisen über mehrere Zeitzonen nach Osten, die für den CWA-Nutzer zu einer Verkürzung des Tages und somit zu einer (automatischen) Umstellung der Systemzeit führen können, eine zu frühe Lösung von Einträgen zu verhindern.

5.8.7 Event-Daten

Event-Daten zu angelegten und besuchten Events werden 15 Tage nach dem Auschecken automatisch gelöscht. Eine vorherige Löschung erfolgt, wenn und sobald das betreffende Event aus der Event-Verwaltung der CWA App gelöscht oder die CWA App zurückgesetzt wird.

5.8.8 Zugriffsdaten

Zur Lösung von Zugriffsdaten siehe unter Ziffer 7.1.1.

5.8.9 Anwendungsdaten / Fehlerberichte

Die während des Betriebs der CWA App anfallenden Anwendungsdaten werden bei deaktiverter Fehlerberichtsaufzeichnung nicht gespeichert und müssen demnach nicht gelöscht werden.

Bei aktiver Fehlerberichtsaufzeichnung werden die Anwendungsdaten in Form der Fehlerberichte so lange gespeichert, bis die Fehlerberichtsaufzeichnung wieder deaktiviert wird. Zur Deaktivierung (und somit Lösung) der Fehlerberichte muss der CWA-Nutzer in den „App-Einstellungen“ unter dem Menüpunkt „Fehlerberichte“ auf den Button „Stoppen und löschen“ tippen. Es gibt keine Möglichkeit, die Fehlerberichtsaufzeichnung zu deaktivieren, ohne dass die Lösung des bereits aufgezeichneten Fehlerberichts ausgelöst wird. Dies gewährleistet, dass zur Problembehebung nicht erforderliche Fehlerberichte auf dem Smartphone „vergessen“ werden.

Die auf dem Log Storage Server gespeicherten Fehlerberichte werden automatisiert nach 14 Tagen gelöscht.

5.8.10 COVID-Zertifikate

Die in der Wallet gespeicherten COVID-Zertifikate können vom CWA-Nutzer jederzeit manuell entfernt werden, wobei nicht zwischen eigenen und COVID-Zertifikaten von Familienangehörigen differenziert wird. Die entfernten COVID-Zertifikate werden zunächst in den Papierkorb verschoben und können von dort wiederhergestellt werden. Sofern der CWA-Nutzer die COVID-Zertifikate im Papierkorb nicht bereits manuell endgültig gelöscht hat, werden sie nach 30 Tagen automatisch endgültig gelöscht. Im Papierkorb kann der CWA-Nutzer das Löschdatum der gelöschten COVID-Zertifikate sehen.

5.8.11 Nutzungsdaten (Datenspende)

Nutzungsdaten und weitere freiwillige Angaben, die im Rahmen der Datenspende von teilnehmenden CWA-Nutzern an das RKI übermittelt werden, werden 180 Tage nach Bereitstellung der Daten durch den CWA-Nutzer an das RKI gelöscht.

5.8.12 Daten der Echtheitsprüfung (Token)

Token, die im Rahmen der Echtheitsprüfung von Apple oder Google an die CWA App übermittelt werden, werden von dieser nach 24 Stunden gelöscht.

5.9 Akteure und betroffene Personen

Nachfolgend werden die Akteure einschließlich der von der Verarbeitung betroffenen Personen beschrieben, die – neben den CWA-Nutzern – in verschiedenen Zusammenhängen Einfluss auf die Verarbeitung personenbezogener Daten im Rahmen des Prüfgegenstands nehmen können.

5.9.1 RKI

Das RKI gibt die CWA für die Bundesregierung heraus und ist für die Datenverarbeitung im Rahmen der CWA verantwortlich. Dem RKI obliegt die fachliche Gestaltung und Weiterentwicklung der CWA unter epidemiologischen Gesichtspunkten. Die epidemiologische Expertise der Beschäftigten des RKI wirkt sich insbesondere auf die Festlegung der Bewertungseinstellungen und die Gestaltung von neuen App-Funktionen aus.

Das RKI ist eine selbständige Bundesoberbehörde im Geschäftsbereich des BMG und die zentrale Einrichtung der Bundesregierung für die Erkennung, Verhütung und Bekämpfung von übertragbaren und nicht übertragbaren Krankheiten (§ 2 BGA-NachfG). Seine gesetzlichen Aufgaben umfassen die Erarbeitung von wissenschaftlichen Erkenntnissen als Basis für gesundheitspolitische Entscheidungen. Vorrangige Aufgaben liegen in der wissenschaftlichen

Untersuchung, der epidemiologischen und medizinischen Analyse und Bewertung von Krankheiten mit hoher Gefährlichkeit, hohem Verbreitungsgrad oder hoher öffentlicher oder gesundheitspolitischer Bedeutung. Im Rahmen seiner Aufgaben erfasst und bewertet das RKI kontinuierlich die Corona-Lage einschließlich des Risikos für die Bevölkerung und stellt im Rahmen seiner Aufgaben Informationen für gesundheitspolitische Entscheidungsträger und die Fachöffentlichkeit bereit. Zudem ist das RKI in seinem Aufgabenbereich für die Information der Bevölkerung zuständig (§ 4 Abs. 4 BGA-NachfG).

Das RKI ist auch der Herausgeber der Apps CovPass, CovPassCheck und der Corona-Datenspende-App sowie Betreiber und Verantwortlicher des Zertifikatsservice.

5.9.2 Entwickler und Betreiber

SAP und TSI haben die CWA im Auftrag des BMG gemeinsam mit dem RKI entwickelt. SAP und TSI haben auch das EFGS im Auftrag der EU-Kommission entwickelt.

Für den Betrieb der Backend-Systeme ist TSI zuständig. Die von den CWA-Serverkomponenten bereitgestellten Dienste laufen in Containern in Kubernetes-Clustern der **Open Telekom Cloud** (OTC). In diesem Zusammenhang verarbeitet TSI etwa die über die CWA App erzeugten technischen Zugriffsdaten, die über den Portalserver und die über die Schnittstelle zu den Laboren (Lab Server) sowie das CDN-Magenta erzeugten Daten.

TSI ist auch für den 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. TSI unterhält mit schriftlicher Genehmigung des RKI (Art. 28 Abs. 2 S. 1 DSGVO) Unterauftragsverhältnisse mit folgenden Dienstleistern als weitere Auftragsverarbeiter, die ebenfalls mit personenbezogenen Daten der CWA-Nutzer oder Anrufenden in Berührung kommen können:

- Deutsche Telekom Individual Solutions & Products GmbH (1st & 1,5 Level Support für OTC)
- weiterer Auftragsverarbeiter: GULP Solutions Services GmbH & Co.KG (Servicedesk für OTC)
- Deutsche Telekom Systems Solutions Hungary Kft. (Operation, 1st & 2nd Level Support für OTC)
- Deutsche Telekom IT GmbH (User support MyWorkplace für OTC)
- Deutsche Telekom Security GmbH (Leistungen im Bereich Security, RED Team Einsatz, Penetrationstests)
- Deutsche Telekom Individual Solutions & Products GmbH (DC Hardware disposal and replace für OTC)
- Axivas Deutschland GmbH (Call-Center für Hotline)

5.9.3 Bundesregierung

Die CWA ist ein Projekt im Auftrag der Bundesregierung.⁶³ Die Bundesregierung unterstützt die Verbreitung der CWA App durch Werbemaßnahmen und stellt Informationsangebote zur CWA für die Öffentlichkeit bereit.

Das BMG ist innerhalb der Bundesregierung für den Gesundheitsbereich einschließlich dem Infektionsschutz zuständig. Sein Geschäftsbereich umfasst auch das RKI. Der Aufgabenbereich des BMG umfasst die Erarbeitung von Gesetzesentwürfen, Rechtsverordnungen und Verwaltungsvorschriften sowie die Zusammenarbeit mit anderen Akteuren des Gesundheitsbereichs auf nationaler, europäischer und internationaler Ebene. Auf europäischer Ebene ist das BMG unter anderem als Mitglied des eHealth Network aktiv, das gemäß Art. 14 Abs. 3 der Richtlinie 2011/24/EU über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung errichtet wurde.

Das BMG hat die Unternehmen SAP und TSI mit der Entwicklung und dem Betrieb der CWA für das RKI beauftragt und unterrichtet das RKI regelmäßig über für die CWA relevante Entwicklungen und Gesetzesvorhaben auf nationaler und EU-Ebene, so dass das RKI diese Informationen bei der Weiterentwicklung der CWA berücksichtigen kann.

Auf europäischer Ebene hat sich das BMG im Rahmen seiner Mitgliedschaft im eHealth Network aktiv an der Entwicklung der Empfehlung 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, beteiligt, welche die Kommission am 08.04.2020 angenommen hat. Zudem hat das BMG im Rahmen des eHealth Network an der Entwicklung der Leitlinien und Spezifikationen für interoperable nationale Corona-Apps mitgewirkt. Hinsichtlich der COVID-Zertifikate hat das BMG auf die Schaffung der für die COVID-Zertifikate erforderlichen nationalen Rechtsgrundlagen im IfSG unter Beratung durch den BfDI und eine mit der deutschen Anwendungspraxis des Datenschutzes vereinbare europäische Lösung im Rahmen der Abstimmungen zur DCC-VO hingewirkt. In Bezug auf die im Rahmen der Online-Validierung stattfindende Übermittlung von COVID-Zertifikaten aus den Wallet-Apps des RKI (CovPass-App und CWA App) an einen Validierungsdienst führt das BMG die Liste der anerkannten Validierungsdienste.⁶⁴ Ziel dieser Maßnahme ist es, ein angemessenes Datenschutzniveau bei der Datenverarbeitung durch die Validierungsdienste sicherzustellen.

⁶³ 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 11.10.2022).

⁶⁴ Auswirkungen auf die datenschutzrechtliche Verantwortlichkeit hat dies mangels Personenbezug der lokalen Datenverarbeitung für das RKI im Rahmen der Online-Validierung und wegen der gesetzlichen Verantwortlichkeitszuweisung an das RKI nicht, siehe Abschnitt 7.5.2.1.2.

5.9.4 BfDI

Der BfDI ist die für das RKI zuständige Datenschutzaufsichtsbehörde. Zu den Aufgaben des BfDI gehört unter anderem die Beratung des Deutschen Bundestags und des Bundesrats, der Bundesregierung und anderer Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten (§ 14 Abs. 1 Nr. 3 BDSG). Im EDSA fungiert der BfDI als gemeinsamer Vertreter für die deutschen Datenschutzaufsichtsbehörden.

An der Entwicklung der CWA wurde der BfDI von Anfang an in beratender Funktion beteiligt. Auch nach dem ersten Release der CWA App hat das RKI die Beratung des BfDI vor der Einführung neuer Funktionen regelmäßig in Anspruch genommen. Darüber hinaus nimmt der BfDI in Bezug auf die CWA die datenschutzrechtliche Aufsicht wahr und bearbeitet Beschwerden aus der Bevölkerung.⁶⁵

Das RKI hat die datenschutzrechtliche Beratung des BfDI auch bei der Durchführung von Fachverfahren und sonstigen Projekten im Zusammenhang mit der Corona-Pandemie in Anspruch genommen. Relevant für die vorliegende DSFA ist insbesondere die Beratung des BfDI bei der Entwicklung der ebenfalls vom RKI verantworteten CovPass-App, der Zertifikats-Prüfanwendung CovPassCheck-App und des Zertifikatsservice.⁶⁶

5.9.5 BSI

Das BSI ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern und für Heimat und die Cyber-Sicherheitsbehörde des Bundes. Es unterstützt die Entwicklung der CWA durch entwicklungsbegleitende Tests der CWA App und der Server-Komponenten und ist maßgeblich an der Gestaltung des Sicherheitskonzepts der CWA beteiligt.

5.9.6 Teststellen / Testeinrichtungen

Teststellen sind Einrichtungen, die einen Antigen- oder PCR-Schnelltest durchführen. Eine Teststelle, die ein Teststellen-System betreibt oder nutzt, wird für dessen Verarbeitung als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO angesehen.

⁶⁵ Vgl. die Zusammenfassungen des BfDI über seine Tätigkeiten und Bewertungen in Bezug auf den Datenschutz bei der CWA im Jahr 2020 im 29. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit 2020, Nr. 4.1.1, S. 26 f. und im Jahr 2021 im 30. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit 2021, Nr. 4.1.1, S. 30 ff.

⁶⁶ Vgl. BfDI, 30. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit 2021, Nr. 4.1.3, S. 32 f.

Testeinrichtungen sind Einrichtungen, die für einen PCR-Test (auch sog. Labortest) notwendige Bioprobe entnehmen und zur Analyse an ein Labor weiterleiten.

Während Schnelltests in Teststellen durch geschultes Personal durchgeführt werden können, werden Probenentnahmen in Testeinrichtungen von medizinischen Fachkräften durchgeführt, die gemäß § 203 StGB zur Verschwiegenheit verpflichtet sind.

5.9.7 Labore

Die Labore erhalten die von Testeinrichtungen entnommene Bioproben und analysieren diese nach dem PCR-Verfahren. Die Beschäftigten der Labore sind gemäß § 203 StGB zur Verschwiegenheit verpflichtet. Ein Labor, das einen Lab Client betreibt oder nutzt, wird insoweit als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO angesehen.

Labore müssen gemäß § 14 Abs. 8 IfSG das Deutsche Elektronische Melde- und Informationssystem für den Infektionsschutz (DEMIS) für die namentliche Meldung von positiven PCR-Testungen an das zuständige Gesundheitsamt verwenden.

5.9.8 Öffentlicher Gesundheitsdienst der Länder

Die Gesundheitsbehörden der Länder und insbesondere die lokalen Gesundheitsämter sind die zuständigen Behörden für die Gesundheitsaufgaben der Länder. In den Zuständigkeitsbereich der Gesundheitsämter fallen auch die äußerst zeit- und ressourcenintensiven Aufgaben der lokalen Kontaktpersonennachverfolgung und des lokalen Fall- und Kontaktpersonenmanagements.

Im Rahmen der CWA können Gesundheitsämter und andere Landesbehörden, wenn sie PCR-Tests für CWA-Nutzer durchführen, auch die Rolle einer Testeinrichtung haben. Zudem können die Beschäftigten der Gesundheitsämter die technische Rolle eines CWA-Nutzers in Bezug auf die Funktion „In Vertretung warnen“ einnehmen.

5.9.9 Hotline-Betreiber

Das RKI bietet für CWA-Nutzer eine technische Support-Hotline und die Verifikations-Hotline an. Mit dem Betrieb dieser Hotlines ist TSI als Auftragsverarbeiter beauftragt.

TSI unterhält mit schriftlicher Genehmigung des RKI (Art. 28 Abs. 2 S. 1 DSGVO) ein Unterauftragsverhältnis mit der ALEX & GROSS Inside Sales Deutschland GmbH, die wiederum die 3wphone GmbH als weiteren Auftragsverarbeiter beauftragt hat.

5.9.10 Dienstleister für Support- und Pflegeleistungen

Mit technischen Support- sowie Pflegeleistungen in Bezug auf die CWA-Komponenten sind SAP und TSI beauftragt.

TSI ist für den 1st- und 2nd-Level-Support sowie die Pflege der CWA-Backendsysteme zuständig. Hierzu gehören insbesondere die Anwendungsüberwachung, die Ticketerstellung, Problemlösung, die Ursachenanalyse und Problembehandlung sowie der Betrieb und die Verwaltung der technischen CWA-Infrastruktur. TSI unterhält mit schriftlicher Genehmigung des RKI (Art. 28 Abs. 2 S. 1 DSGVO) Unterauftragsverhältnisse mit folgenden Dienstleistern als weitere Auftragsverarbeiter, die im Einzelfall mit personenbezogenen Daten der CWA-Nutzer in Berührung kommen können:

- Deutsche Telekom Individual Solutions Products GmbH (1,5 level support für OTC, Partner Management Schnelltestpartner-Onboarding)
- Deutsche Telekom Systems Solutions Hungary Kft (OTC – Operation, 1st & 2nd level support)
- Operational services GmbH & Co. KG (1st level support für Public Cloud Services)
- Deutsche Telekom Technik GmbH (für das Content Delivery Network (CDN-Magenta))
- BS software development GmbH & Co. KG (Leistungen für die Laboranbindung)
- Deutsche Telekom Security GmbH (Security, RED Team Einsatz, Penetrationstest gegen Wirkreferenzumgebung (WRU), RED Team Einsatz gegen Wirkumgebung (PROD))
- Alex & Gross Inside Sales GmbH (Leistungen Partner Management Schnelltestpartner-Onboarding)
- Deutsche Telekom IT GmbH (Leistungen Betrieb der technischen Komponenten des Security Information und Event Management Lösung (SIEM) und des M-SAS (Magenta Security Analytics System))

SAP ist für den 3rd-Level-Support sowie die Pflege der CWA App zuständig. Davon umfasst sind insbesondere Leistungen zur Fehlerbehebung innerhalb der CWA App, Funktionsverbesserungen, Codeänderungen und -optimierungen, Stabilisierungsmaßnahmen und Migrationen. Personenbezogene Daten von CWA-Nutzern werden dabei regelmäßig nur von CWA-Nutzern, die die Fehlerberichte-Funktion verwenden und mit dem Support unter Nennung der ID des Fehlerberichts in Kontakt treten, verarbeitet. Eine Zugriffsmöglichkeit kann im Rahmen des zu leistenden Supports nicht gänzlich ausgeschlossen werden. SAP unterhält mit schriftlicher Genehmigung des RKI Unterauftragsverhältnisse mit folgenden Dienstleistern als weitere Auftragsverarbeiter, die im Einzelfall mit personenbezogenen Daten der CWA-Nutzer in Berührung kommen können:

- SAP România SRL
- SAP Bulgaria Ltd.
- SAP Ireland Limited

5.9.11 Hersteller der Smartphones / Betriebssysteme

Apple und Google sind die Hersteller und Anbieter des ENF. Sie haben das ENF nach ihren Vorstellungen und Designkriterien entwickelt und als Systemkomponente in ihre jeweiligen Betriebssysteme integriert.

5.9.12 Akteure 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 TSI und SAP als Unterauftragsverarbeiter mit der technischen Bereitstellung und Verwaltung des EFGS beauftragt.

Für die Datenverarbeitung im Rahmen des EFGS zur Ermöglichung der Interoperabilität zwischen den Corona-Apps der teilnehmenden Mitgliedstaaten sind die teilnehmenden Mitgliedstaaten, jeweils vertreten durch die benannten nationalen Behörden oder Stellen gemeinsam verantwortlich. Die teilnehmenden Mitgliedstaaten legen die Zwecke und Mittel in Bezug auf die Datenverarbeitung im Zusammenhang mit dem EFGS gemeinsam fest.

Die technischen und organisatorischen Einzelheiten der Zusammenarbeit, insbesondere die Verteilung der Zuständigkeiten zwischen den teilnehmenden Mitgliedstaaten sowie die Aufgaben der EU-Kommission als Auftragsverarbeiter werden in einem Beschluss der EU-Kommission festgelegt (Durchführungsbeschluss (EU) 2020/1023 vom 15. Juli 2020, dort insbesondere Anhang II und III, abrufbar unter https://eur-lex.europa.eu/eli/dec_impl/2020/1023/oj).

5.9.13 Akteure des CHGS

Für den Betrieb und die Wartung des CHGS ist nach Maßgabe der zwischen dem RKI und dem Eidgenössischen Departement des Innern der Schweizerischen Eidgenossenschaft

abgeschlossen Behördenvereinbarung das BAG zuständig. Auftragsverarbeiter darf das BAG nur mit Zustimmung des RKI für den Betrieb des CHGS einsetzen.

Die Wirksamkeit der vom BAG getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung im CHGS wird vom BAG unter Beteiligung des Nationalen Zentrums für Cybersicherheit NCSC und des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) regelmäßig, mindestens jedes halbe Jahr, und anlassbezogen geprüft, beurteilt und bewertet.

Das RKI und das BAG haben sich jeweils im Rahmen der Behördenvereinbarung verpflichtet, deren Inhalt auf ihren jeweiligen Websites zu veröffentlichen.

Für die Datenverarbeitung durch den CHGS zur Ermöglichung der Interoperabilität zwischen der deutschen und der Schweizer Corona-App ist das RKI gemeinsam mit dem Schweizer BAG verantwortlich. Zur Regelung der Zusammenarbeit wurde eine Behördenvereinbarung zwischen dem RKI und dem Eidgenössischen Departement des Innern der Schweizerischen Eidgenossenschaft abgeschlossen. Die Behördenvereinbarung dient auch der Erfüllung der Pflicht aus Art. 26 Abs. 1 S. 2 DSGVO zum Abschluss einer transparenten Vereinbarung über die gemeinsame Verarbeitung.

Das Schweizer BAG ist für den technischen Betrieb des CHGS zuständig.

5.9.14 Prüfer von COVID-Zertifikaten / Leistungsanbieter

Prüfer von COVID-Zertifikaten sind Personen, Behörden, Unternehmen und sonstige Leistungsanbieter, die ein Prüfsystem zur Prüfung von in der CWA App angezeigten COVID-Zertifikaten (z. B. CovPassCheck-App) oder einen Validierungsdienst für die Zertifikatsüberprüfung im Rahmen von Online-Buchungsprozessen einsetzen.

5.9.15 Betreiber von Validierungsdiensten (Prüfpartner)

Prüfpartner betreiben einen Validierungsdienst, der von Leistungsanbietern wie beispielsweise Reise- und Veranstaltungsunternehmen zur Prüfung von COVID-Zertifikaten in einen Online-Buchungsvorgang integriert werden kann. Um Zertifikate aus einer Wallet-App des RKI zur Prüfung erhalten zu können, muss der Validierungsdienst in der Liste der anerkannten Validierungsdienste des BMG enthalten sein.

5.9.16 Betroffene Personen

Die von der personenbezogenen Datenverarbeitung betroffenen Personen sind die Nutzer. Dies umfasst begrifflich sowohl Personen, die die CWA App verwenden (CWA-Nutzer), als auch Personen, die eine andere nationale Corona-App verwenden.

Weitere potenziell betroffene Personen sind Personen, auf die sich die Kontakt-Tagebuch-Einträge des CWA-Nutzers beziehen, sofern diese Personen für den CWA-Nutzer bestimmbar sind, die Zertifikatsinhaber von Familienzertifikaten sowie Anrufende der Hotlines.

5.10 Begleitdokumente zur Beschreibung des Prüfgegenstands

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)	2.24
2	Datenschutzkonzept der CWA der Bundesrepublik Deutschland – Verifikation und Testergebnis	2.24
3	Datenschutzkonzept der CWA der Bundesrepublik Deutschland – CWA App	2.24
4	Datenschutzkonzept der CWA der Bundesrepublik Deutschland – CWA Server	2.24
5	Datenschutzkonzept der CWA der Bundesrepublik Deutschland – Verifikations-Hotline	2.24
6	Designentscheidungen bei der Entwicklung der Corona-Warn-App der Bundesrepublik Deutschland und des European Federation Gateway Service (EFGS)	2.24 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	/
10	Vereinbarung zwischen Robert Koch-Institut, Bundesinstitut im Geschäftsbereich des Bundesministeriums für Gesundheit der Bundesrepublik Deutschland und dem Eidgenössischen Departement des Innern der Schweizerischen Eidgenossenschaft betreffend Corona-Apps (Austausch von Schlüsseln über einen auf schweizerischer Seite betriebenen Gateway Server zur grenzüberschreitenden Interoperabilität)	/

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 der in Rede stehenden Verarbeitung zu fördern.

Die potenziell von der Verarbeitung betroffenen Personen sind im Fall der CWA alle sich in Deutschland oder einem anderem am EFGS teilnehmenden Land und in der Schweiz aufhaltenden Personen, die über ein ENF-kompatibles Smartphone verfügen. Aufgrund dieses weiten Betroffenenkreises war eine sachgerechte Einholung ihres Standpunkts im Sinne von Art. 35 Abs. 9 DSGVO weder bei der Entwicklung des ersten Releases der CWA App noch bei der späteren Entwicklung weiterer App-Funktionen aus praktischen, insbesondere zeitlichen Gründen nicht möglich. Um dennoch Einblicke und Hinweise auf die Erwartungen und Prioritäten der betroffenen Personen und eventuell vom RKI übersehene Aspekte der Verarbeitung zu erhalten, hat das RKI verschiedene Quellen ausgewertet. Diese Quellen umfassen insbesondere:

- Individuelles und öffentliches Feedback aus der Entwicklungs-Community auf die Veröffentlichung von Quellcodes und Dokumentationen auf der GitHub-Projektseite der CWA,⁶⁷
- Fehlerberichte, die von CWA-Nutzern bereitgestellt werden,
- Medienberichterstattung,
- Fachveröffentlichungen,
- Stellungnahmen und Leitlinien von europäischen Datenschutzbehörden und Datenschutzgremien (z. B. EDSA, eHealth Network)⁶⁸ und
- Stellungnahmen von Verbänden und Interessensgruppen⁶⁹.

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

7 Datenschutzrechtliche Bewertung

Nachfolgend wird die Verarbeitung aus datenschutzrechtlicher Sicht eingeordnet, sodass die datenschutzrechtlichen Rollen und Verantwortlichkeiten identifiziert werden können.

⁶⁷ <https://github.com/corona-warn-app> (abgerufen am 11.10.2022).

⁶⁸ Siehe z. B. 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 11.10.2022); https://ec.europa.eu/health/ehealth-digital-health-and-care/eu-cooperation/ehealth-network_de (abgerufen am 11.10.2022).

⁶⁹ 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 11.10.2022); 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 11.10.2022).

7.1 Personenbezug der 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 teilweise, je nach ihrer Funktion, einen direkten oder indirekten Personenbezug. In welchem Umfang personenbezogene Daten verarbeitet werden, wird im Folgenden dargestellt.

7.1.1 Verarbeitung durch zentrale CWA-Dienste (Serversystem der CWA)

Es wird angenommen, dass in folgenden Fällen personenbezogene Daten verarbeitet werden:

- In Form von Zugriffsdaten bei Zugriffen auf das Serversystem der CWA,
- in Form von Positivschlüsseln, Check-ins und eindeutigen Kennungen (Registration Token, TANs) beim Warnen anderer Nutzer,
- in Form eindeutiger Kennungen (GUID) beim Registrieren eines Tests,
- in Form von Anwendungsdaten in geteilten Fehlerberichten und
- in Form von Nutzungsdaten der Datenspende,

jedoch jeweils nur so lange, wie die vom CWA-Nutzer für die Übermittlung dieser Daten verwendete IP-Adresse auf dem CWA Server und CWA Data Donation Server bzw. CDN-Magenta gespeichert ist. Der Personenbezug besteht für das RKI.

Unabhängig davon, ob es sich bei den Positivschlüsseln, den Check-ins 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.⁷⁰ 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.

⁷⁰ EuGH, Urt. v. 19.10.2016, Rs. Breyer, C-582/14.

Da seitens des RKI die IP-Adressen aus den Server-Logfiles auf dem CWA Server, dem CWA Data Donation 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 nur für wenige Sekunden.

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 eine 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.

Auch sofern CWA-Nutzer freiwillig an der Datenspende teilnehmen, können das RKI (oder die technischen Umsetzungspartner) anhand der im Zusammenhang mit der Echtheitsprüfung der jeweiligen Verifikations-Dienste erzeugten Token oder Nutzungsdaten über die Verwendung der CWA App keine Identifizierung des jeweiligen CWA-Nutzers vornehmen. Da allerdings keine gesicherte Aussage möglich ist, ob die Betriebssystemhersteller nicht anhand der Token CWA-Nutzer potenziell re-identifizieren können, wird vorsorglich von einer pseudonymen Verarbeitung ausgegangen. Zudem werden im Rahmen der Nutzungsdaten unterschiedlichste Datenpunkte zur Verwendung der CWA App erfasst, so dass trotz der vorgenommenen Normierungen (z.B. keine Erfassung genauer Zeitpunkte, sondern nur Erfassung des Datums eines exposure windows) Datensätze sehr spezifische Informationen enthalten, die insgesamt eine Verarbeitung personenbezogener Daten nicht ausgeschlossen erscheinen lassen. Ein realistisches Risiko der Re-Identifizierung besteht dennoch nicht.

Ein Risiko der Re-Identifizierung für CWA-Nutzer ist auch bei Teilnahme an Befragungen hinreichend ausgeschlossen. Eine Verknüpfung mit innerhalb der CWA App verarbeiteten personenbezogenen Daten ist auf Basis der im Rahmen der Befragung später erhobenen Daten nicht möglich. Die von den Befragungsteilnehmern optional angegebene E-Mail-Adresse zur Ermöglichung einer Folgebefragung ist nicht geeignet, um die Verknüpfung mit in der CWA App erhobenen Daten herzustellen. Die IP-Adressen der Befragungsteilnehmer – als potenziell zur Identifizierung geeignete Daten – werden bereits an der Firewall zum Befragungs-Server des RKI maskiert. Die vom Befragungs-Server automatisiert erhobenen Nutzungsdaten (Useragent, Referrer-URL) werden zudem mit Ende der Websession der jeweiligen Befragung durch entsprechende Datenbanktrigger gelöscht. Die im Rahmen der Befragung erhobenen Befragungsdaten bzw. die Fragen wurden unter Berücksichtigung des Grundsatzes der Erforderlichkeit ausgewählt. Insbesondere werden keine Standortdaten

erfasst; auf Freitextfelder wird verzichtet. Zur Gewährleistung der Sicherheit des Befragungs-Systems außerhalb der CWA wird neben Strict Transport Security (HSTS) lokal zusätzlich ein Intrusion Prevention und Intrusion Detection System betrieben.

7.1.2 Verarbeitung für die Online-Validierung

Wenn der CWA-Nutzer zur Online-Validierung bei einem Leistungsanbieter in der CWA App gespeicherte COVID-Zertifikate nutzen möchte, initialisiert er den Vorgang aus Sicht der CWA App durch den Scan des Initialisierungs-QR-Codes und willigt sodann in die Verarbeitung der Validierungsanforderungen durch die CWA App ein, die beim Leistungsanbieter abgeholt werden. Anhand der Validierungsanforderungen wird in der CWA App ein für das jeweilige Validierungsverfahren geeignetes COVID-Zertifikat aus der Wallet identifiziert und dem CWA-Nutzer vorgeschlagen. Willigt der CWA-Nutzer sodann in der CWA App in die Übermittlung der gespeicherten Zertifikatsaussagen des COVID-Zertifikats und der zum Buchungsvorgang vom Leistungsanbieter bereitgestellten Online-Validierungsdaten an einen Validierungsdienst ein, werden die Daten aus der CWA App an den Validierungsdienst übermittelt. Die gesamte in der CWA App erfolgende Verarbeitung im Rahmen der Online-Validierung erfolgt ohne Zugriffsmöglichkeit oder Kenntnis des RKI. Für die anschließend beim Validierungsdienst erfolgende Datenverarbeitung ist der jeweilige Anbieter (sog. Prüfpartner) verantwortlich. Das RKI hat keinen Einfluss auf das Ob und Wie der Validierung, es wählt den Validierungsdienst nicht aus, erhält keine Daten in Form der Ergebnisse aus dem Vorgang und kann keine Weisungen gegenüber den an der Online-Validierung weiteren Beteiligten erteilen.

7.1.3 Lokale Verarbeitung auf dem Smartphone

Die lokale Datenverarbeitung betrifft insbesondere den Austausch von RPIs zwischen Smartphones per BLE, die Kontaktprotokollierung im Kontaktprotokoll, die Erzeugung von Tagesschlüsseln und RPIs, die Speicherung der Check-in-Details und Event-Details, die Ermittlung des Risikos für den CWA-Nutzer, die Verarbeitung von Kontakt-Tagebuch-Einträgen und die Speicherung und Verwendung von Schnelltest-Profilen und COVID-Zertifikaten. Auch die Aufzeichnung von Anwendungsdaten für Fehlerberichte findet zunächst rein lokal statt.

Soweit es sich bei den insoweit nur lokal verarbeiteten Daten um vom CWA-Nutzer bereitgestellte Informationen über ihn selbst oder Dritte (z. B. Kontaktpersonen, Familienangehörige) handelt, handelt es sich jedenfalls für den CWA-Nutzer um personenbezogene Daten.

Der konkrete Ablauf und Inhalt der lokalen Datenverarbeitungsvorgänge liegt hingegen außerhalb des direkten Einflussbereichs des RKI. Dies gilt sowohl für die von der CWA App auf technischer Ebene selbst verarbeiteten Daten als auch für die betriebssystemseitige Datenverarbeitung durch das ENF. Für das RKI haben die rein lokal verarbeiteten Daten somit keinen Personenbezug. Gleichwohl werden sie teilweise als innerhalb des Verantwortungsbereichs des RKI liegend behandelt.

Eine Besonderheit besteht hinsichtlich der COVID-Zertifikate. Da diese auf dem vom RKI betriebenen Zertifikatsservice generiert werden, müssen die von der das COVID-Zertifikat ausgebenden Stelle übermittelten Angaben zur Zertifikatsaussage für einen kurzen Zeitraum während der Erstellung aus technischen Gründen im Klartext, also in personenbezogener Form, verarbeitet werden. Nach der Generierung des COVID-Zertifikats werden alle im Zusammenhang mit dem COVID-Zertifikat erhaltenen oder generierten Daten sofort gelöscht, so dass der Personenbezug für das RKI entfällt.

7.2 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** im Sinne von Art. 9 Abs. 1 DSGVO.

7.2.1.1 Tagesschlüssel

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, 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. Entsprechend sind Check-in-Details zu besuchten Events noch nicht mit einer Aussage über den Gesundheitszustand oder ein bestimmtes Erkrankungsrisiko des CWA-Nutzers verbunden. Erst im Rahmen der Warnung erhalten die Check-ins einen konkreten Gesundheitsbezug.

7.2.1.2 Weitere Kategorien von Gesundheitsdaten

Als Gesundheitsdaten anzusehen sind folgende Datenkategorien der CWA:

- Positivschlüssel
- TAN, teleTAN, PIW-TAN, GUID, Registration Token
- Daten im Rahmen des Verifikations-Hotline-Prozesses
- teilweise Daten der Datenspende
- Daten zum Zwecke des namentlichen Schnelltest-Nachweises
- COVID-Zertifikate (Zertifikatsaussage)
- Online-Validierungsdaten

Bei der vom CDN-Magenta heruntergeladenen Liste der Positivschlüssel sowie der Check-ins 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 (zuvor Tagesschlüssel) bzw. den Check-ins (zuvor Check-in-Details) stehen, schließen lassen. Sofern man (vorsorglich) davon ausgeht, dass auch die anschließende lokale Verarbeitung der heruntergeladenen Positivschlüssel (bzw. Check-ins) 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 (und Check-ins) anderer Nutzer um Gesundheitsdaten. Gleches 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, PIW-TAN, 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 Infektionsrisiko 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.

Auch bei der Verarbeitung von im Rahmen der Datenspende übermittelten Nutzungsdaten handelt es sich teilweise um Gesundheitsdaten. Die Nutzungsdaten enthalten beispielsweise Informationen über die Höhe des ermittelten Infektionsrisikos, die Testregistrierung sowie das mittels der CWA App abgefragte Testergebnis. Auch wenn diese Informationen nicht enthalten wären oder sie nicht auf eine Erkrankung hindeuten, so lassen sie dennoch potenziell den Schluss auf den Gesundheitszustand des CWA-Nutzers zu, nämlich dass dieser gesund ist.

Die COVID-Impfzertifikate und die in diesem Zusammenhang verarbeiteten Impfdaten geben Aufschluss über den Impfstatus und sind damit als Gesundheitsdaten einzustufen. Dies gilt entsprechend für die im Zusammenhang mit den Test- und Genesenenzertifikaten verarbeiteten Zertifikatsaussagen zum Test- bzw. Genesenestatus und die mit der CWA App erstellten Druckversionen von Impfzertifikaten. Die Verarbeitung dieser Daten findet im Rahmen der Wallet-Funktion ausschließlich lokal auf dem Smartphone des CWA-Nutzers statt.

Nicht als Gesundheitsdaten anzusehende Datenkategorien sind Token, die im Rahmen der Echtheitsprüfung isoliert verarbeitet werden. Denn die Verarbeitung des Tokens lässt allenfalls den Schluss zu, dass eine Person CWA-Nutzer ist. Die Echtheitsprüfung findet sowohl in Zusammenhang mit der Datenspende als auch bei Teilnahme an einer Befragung statt. Nur die Teilnahme an der Befragung ist an das Vorliegen der Anzeige eines erhöhten Risikos in der CWA App geknüpft. Da die Datenspende unabhängig von einem Erkrankungsrisiko genutzt werden kann, ist allein mittels der Verarbeitung des Tokens kein Rückschluss auf den Gesundheitszustand des CWA-Nutzers möglich.

7.3 Verantwortlichkeit

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“. Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten festgelegt werden.

7.3.1 Verarbeitung durch zentrale CWA-Dienste

Das RKI ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO für die mit dem Betrieb des Prüfgegenstands einhergehende Verarbeitung von personenbezogenen Daten der Nutzer durch das Serversystem der CWA. Ebenfalls ist das RKI für die Datenverarbeitung durch den Zertifikatsservice verantwortlich.

7.3.2 Lokale Verarbeitung durch die CWA App

7.3.2.1 Lokale Verarbeitung von Tages-/Positivschlüsseln

Da die CWA App keine allgemeinen, also alle CWA-Nutzer gleichermaßen einbeziehenden Tracking- oder Nutzungsanalyse-Funktionalitäten für alle CWA-Nutzer vorsieht und die im Rahmen der freiwilligen Datenspende umgesetzte Übermittlung von Nutzungsdaten mangels hierbei gemeinsam erfasster, eindeutig identifizierender Kennungen (identifier) kein fortlaufendes Hinzuspeichern von Daten zu einem Profil ermöglicht, kann das RKI die durch in anderen Teilen der CWA App lokal verarbeiteten Daten (etwa im Rahmen der Risiko-Ermittlung) weder mit einem Nutzungsprofil noch mit einzelnen Nutzungsdatenpunkten aus der Datenspende verknüpfen. Rückschlüsse auf die Person des CWA-Nutzers werden damit nicht ermöglicht. Für das RKI sind die nur lokal in der CWA App verarbeiteten Kennungen und sonstigen Daten der Nutzer (z. B. Tagesschlüssel bzw. Positivschlüssel) unauflösbare Pseudonyme und somit faktisch anonym. Eine Ausnahme hiervon bilden die im Rahmen des namentlichen Schnelltest-Nachweises verarbeiteten Daten des CWA-Nutzers sowie die

Kontakt-Tagebuch-Einträge, da diese, sollten sie dem RKI im Einzelfall zugänglich gemacht werden, einen direkten Rückschluss auf bestimmte Personen erlauben.

Das RKI legt jedoch durch die Programmierung und das Verbreiten der CWA App die Mittel und in gewissem Umfang die 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 eine Verantwortlichkeit des RKI im Sinne von Art. 4 Nr. 7 DSGVO begründet, obwohl die lokal verarbeiteten Daten aus Sicht des RKI im Sinne einer unauflösbaren **Pseudonymisierung** faktisch anonym sind.

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 Drittwissen und die für Dritte zur Verfügung stehenden Mittel prinzipiell zurechnen lassen. Dies allerdings nur, soweit das Wissen und die Mittel durch das RKI vernünftigerweise eingesetzt werden (können). Mit der Rechtsprechung des EuGH wird man nach allgemeinem Ermessen davon ausgehen müssen, dass Verantwortliche (insbesondere, wenn es sich um eine öffentliche Stelle handelt) grundsätzlich keine rechtswidrigen Mittel einsetzen, um die faktische Anonymität oder Unauflöslichkeit von Pseudonymen aufzuheben.⁷¹ 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 mangels Verarbeitung *personenbezogener* Daten 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 Risikobehandlungen reduziert werden.

Der BfDI hat im Rahmen seiner projektbegleitenden Beratung datenschutzrechtliche Bedenken an einer solchen Sichtweise geäußert. Das RKI hat sich daher entschieden, für die Verarbeitung von für die CWA App freigegebenen Tages- und ggf. Positivschlüsseln für die Zwecke der Risiko-Ermittlung, der Testregistrierung und der Warnfunktion *vorsorglich* von der eigenen datenschutzrechtlichen Verantwortlichkeit auszugehen. Damit soll auch der Eindruck

⁷¹ Vgl. zusammenfassend und m.w.N. bei: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 4 Nr. 1 Rn. 61 und 64.

vermieden werden, dass sich das RKI als Anbieter der CWA App nicht für den Schutz der für diese zentralen Funktionen der CWA App lokal verarbeiteten Daten zuständig fühlt.⁷²

7.3.2.2 Lokale Verarbeitung von COVID-Zertifikaten

Nach der Generierung eines COVID-Zertifikats durch den Zertifikatsservice des RKI werden alle im Zusammenhang mit dem COVID-Zertifikat erhaltenen oder generierten Daten sofort von diesem gelöscht, so dass der Personenbezug für das RKI entfällt. Die in der Wallet der CWA App abgelegten COVID-Zertifikate entziehen sich der Kenntnis und dem direkten Zugriff des RKI. Infolgedessen können die lokal durch die CWA App verarbeiteten COVID-Zertifikate für das RKI keinen Personenbezug mehr haben.

Zwar kann das RKI durch die Bereitstellung beispielsweise von Business Rules und Widerrufslisten auf die Darstellung und Zweckdienlichkeit der COVID-Zertifikate für den CWA-Nutzer einen gewissen Einfluss nehmen. Diese Einflussnahme findet jedoch rein lokal auf dem Endgerät statt und die spezifische Darstellung und Verwendung des einzelnen COVID-Zertifikats entzieht sich ebenso der Kenntnis des RKI. Die Annahme einer datenschutzrechtlichen Verantwortlichkeit des RKI für die gespeicherten COVID-Zertifikate wäre daher nicht sachgerecht. Insbesondere wäre das RKI als Verantwortlicher für die Gewährleistung der Betroffenenrechte der Zertifikatsinhaber in Bezug auf ihre in der Wallet eines CWA-Nutzers gespeicherten COVID-Zertifikate anzusehen, auf die es jedoch keinen Zugriff hat.

Auch im Hinblick auf die Erneuerung (infolge des Auslaufens der technischen Gültigkeit) oder den Austausch (infolge der Änderung der Codierungsstandards) von Zertifikaten ergeben sich keine abweichenden Ergebnisse. Ob ein Zertifikat erneuert oder ausgetauscht werden kann, wird ausschließlich lokal anhand der gespeicherten Zertifikate überprüft. Entscheidet sich der CWA-Nutzer für den Austausch bzw. die Erneuerung werden Zertifikatsaussagen an den Zertifikatsservice übermittelt, dort aber nichtpersistiert. Soweit dabei die R-Werte der ausgetauschten bzw. erneuerten Zertifikate gespeichert werden, um bereits erfolgte, oder zukünftige Sperrungen auch hinsichtlich der neuen Zertifikate umsetzen zu können und die Anzahl der Neuausstellung pro Zertifikat begrenzen zu können, ändert sich an der Annahme der Unauflöslichkeit der Pseudonymität nichts. Aus dem R-Wert können keine Zertifikatsaussagen abgeleitet werden. Zertifikatsinhaber können anhand der R-Werte nicht identifiziert werden. Es lässt sich lediglich anhand eines konkret vorliegenden COVID-Zertifikats ermitteln, ob in der Sperrliste oder der Austauschliste gespeicherte R-Werte aus

⁷² 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 erschien 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.“

diesem Zertifikat generiert wurden. Im Rahmen des Austauschs bzw. der Erneuerung von COVID-Zertifikaten verbleiben daher keine Daten beim RKI, aus denen sich für die lokal gespeicherten COVID-Zertifikate für das RKI ein Personenbezug ergäbe.

7.3.2.3 Lokale Verarbeitung von anderen Daten

Die Kontakt-Tagebuch-Einträge des CWA-Nutzers sind dem RKI zu keinem Zeitpunkt zugänglich. Für sie sind, soweit sie für den CWA-Nutzer einen Personenbezug aufweisen, die Annahme einer datenschutzrechtlichen Verantwortlichkeit des RKI weder gerechtfertigt noch sachgerecht. Die Nutzung des Kontakt-Tagebuchs durch den CWA-Nutzer findet in jeder Phase lokal und außerhalb des Einfluss- und Kenntnisbereichs des RKI statt. Das RKI hat auch zu einem späteren Zeitpunkt keine Möglichkeit festzustellen, ob und, falls ja, wie und zu welchen konkreten Zwecken ein CWA-Nutzer das Kontakt-Tagebuch nutzt. Das RKI kann zu keinem Zeitpunkt auf die Kontakt-Tagebuch-Einträge zugreifen. Die konkrete Datenverarbeitung soll den persönlichen Zwecken des CWA-Nutzers (Gedächtnisstütze) dienen, der allein über die Erstellung, den Inhalt und den Umfang von personenbezogenen Einträgen sowie deren Weitergabe an das Gesundheitsamt und die Löschung der Einträge entscheidet. Die Festlegung der konkreten Zwecke, für die die Einträge des Kontakt-Tagebuchs tatsächlich verwendet werden, erfolgt durch den CWA-Nutzer und kann vom RKI nicht beschränkt werden. Alle Kontakt-Tagebuch-Einträge weisen aus der Perspektive des RKI sowohl in Bezug auf den CWA-Nutzer als auch die von den Einträgen betroffenen Kontaktpersonen des CWA-Nutzers keinen Personenbezug auf und sind daher für das RKI anonym. Für die Datenverarbeitung für das Kontakt-Tagebuch besteht auch keinerlei technische Abhängigkeit von Dritten, die somit einen direkten Einfluss auf die Datenverarbeitung nehmen könnten. Eine datenschutzrechtliche Verantwortlichkeit des RKI für die Einträge eines CWA-Nutzers in seinem Kontakt-Tagebuch kann vor diesem Hintergrund nicht angenommen werden.⁷³

Auch die namentlichen Schnelltest-Nachweise des CWA-Nutzers (im Sinne der Detailansicht in der CWA App) und die mit der CWA App erstellten Druckversionen von COVID-Zertifikaten sind dem RKI nicht zugänglich. Zwar weisen sie sowohl für den CWA-Nutzer als auch für etwaige Dritte einen direkten Personenbezug auf. Ebenso wie das Kontakt-Tagebuch verwendet der CWA-Nutzer auch die namentlichen Schnelltest-Nachweise und die Druckversionen von COVID-Zertifikaten grundsätzlich ausschließlich lokal und damit außerhalb des Kenntnisbereichs des RKI. Auch der namentliche Schnelltest-Nachweis und die Druckversionen dienen allein den persönlichen Zwecken des CWA-Nutzers, der diese

⁷³ Dies entbindet das RKI jedoch nicht von der Pflicht, die notwendigen und angemessenen Maßnahmen zur Verhinderung von Datenschutzverletzungen durch eigenverantwortliche Handlungen eines CWA-Nutzers zu treffen. Im Rahmen der technischen Ausgestaltung des Kontakt-Tagebuchs wurde daher sichergestellt, dass die diesbezügliche Datenverarbeitung möglichst auf den Zweck des Kontakt-Tagebuchs beschränkt wird, die Daten unzugänglich für Dritte gespeichert sind und der CWA-Nutzer durch geeignete Hinweise auf den privaten Hintergrund der Datenverarbeitung hingewiesen wird. Dabei wird der CWA-Nutzer ausdrücklich auch darauf hingewiesen, dass die Einträge im Kontakt-Tagebuch nicht für Dritte bestimmt sind und private Personen oder Unternehmen die Herausgabe der Daten nicht verlangen können. Siehe hierzu auch Abschnitt 9.5.1.3.

verwenden kann, um gegenüber Dritten die Durchführung eines negativen Schnelltests zu belegen oder eine erfolgte Impfung, Genesung oder Testung nachzuweisen. Der CWA-Nutzer entscheidet allein darüber, ob und wie er sein Schnelltest-Ergebnis und Druckversionen von COVID-Zertifikaten verwendet und insbesondere, wem er sie vorzeigt. Das RKI hat hierauf keinen Einfluss. Die den Personenbezug unmittelbar herstellenden Daten (Name und Geburtsdatum) werden im Fall der namentlichen Schnelltest-Nachweise über den QR-Code von der Teststelle direkt an die App übergeben. Eine Persistierung auf Servern des RKI erfolgt hierbei nicht. Namentliche Schnelltest-Nachweise haben aus Sicht des RKI daher keinen Personenbezug. So wie auch im Fall des Kontakt-Tagebuchs sind die Schnelltest-Nachweise auf technischer Ebene nicht von den Schnittstellen oder technischen Vorgaben des ENF abhängig, sondern könnten theoretisch auch ohne dieses bzw. in einer eigenen Anwendung bereitgestellt werden. Daher ist hier die (vorsorgliche) Annahme einer datenschutzrechtlichen Verantwortlichkeit des RKI nicht geboten.

Die unmittelbarste Einflussmöglichkeit hinsichtlich des Ablaufs der lokalen Datenverarbeitung durch die CWA App und das ENF haben einerseits der CWA-Nutzer, beispielsweise durch die Änderung von Systemeinstellungen des Smartphones, das Scannen oder Erstellen von QR-Codes im Rahmen der Event-Registrierung, das Speichern von COVID-Zertifikaten oder das manuelle Löschen des Kontaktprotokolls oder erfasster Events, und andererseits Apple bzw. Google, die als Hersteller des Betriebssystems die Möglichkeit zur nachträglichen Änderung des ENF und insoweit auf technischer Ebene prinzipiell auch zur Verknüpfung der dort verarbeiteten Tagesschlüssel und APIs mit einer geräte- (z. B. Werbe-ID) oder nutzerspezifischen Kennung (z. B. Apple-ID oder Google-Konto) haben. Vor diesem Hintergrund sind auch diese, d. h. im Zusammenhang mit dem ENF stehenden, in der CWA App gespeicherten Daten jedenfalls für das RKI faktisch anonym.

Wenn ein CWA-Nutzer in seinem Kontakt-Tagebuch Einträge zu Personen oder Orten macht, die er direkt oder unter Hinzuziehung weiterer ihm zugänglichen Informationen auf eine für ihn bestimmbare Person beziehen kann, kommt insoweit eine datenschutzrechtliche Verantwortlichkeit des eintragenden CWA-Nutzers für die Verarbeitung der anfallenden Kontakt-Tagebuch-Einträge prinzipiell in Betracht. Da das Kontakt-Tagebuch eine Funktion zur Unterstützung der persönlichen Erinnerung des CWA-Nutzers darstellt, wird die Nutzung des Kontakt-Tagebuchs bei bestimmungsgemäßem und jedenfalls naheliegendem Gebrauch aber regelmäßig in den Anwendungsbereich der sogenannten Haushaltsausnahme gem. Art. 2 Abs. 2 lit. c DSGVO fallen, so dass eine datenschutzrechtliche Verantwortlichkeit des CWA-Nutzers für die Verarbeitung der von ihm gespeicherten Kontakt-Tagebuch-Einträge ausscheidet. Eine Verarbeitung von personenbezogenen Daten fällt unter die Haushaltsausnahme, wenn sie nach der Verkehrsanschauung der Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten dient, sie also ohne jeden Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird (Erwägungsgrund 18 DSGVO). Da es in keinem Wirtschaftsbereich eine gesetzliche Pflicht zur Kontaktnachverfolgung mittels des Kontakt-Tagebuchs der CWA App gibt und Privatpersonen keiner Pflicht zur Kontaktdokumentation unterliegen, wird die Verwendung des Kontakt-Tagebuchs der CWA App ebenso wie die Erfassung von Kontakten in einem herkömmlichen Tagebuch regelmäßig als rein persönliche Tätigkeit anzusehen sein. Da die Haushaltsausnahme auf den Zweck der Verarbeitung abstellt, gilt sie grundsätzlich auch dann, wenn die CWA App auf einem dienstlichen Smartphone verwendet wird oder die Einträge (auch) berufliche Kontakte des

CWA-Nutzers betreffen. Eine datenschutzrechtliche Verantwortlichkeit des CWA-Nutzers kommt somit regelmäßig nur in Betracht, sofern und sobald der CWA-Nutzer das Kontakt-Tagebuch (auch) für nach außen gerichtete, über den persönlichen oder familiären Kreis hinaustretende Tätigkeiten verwenden will, etwa um die erfassten Kontakt-Tagebuch-Einträge zu Kontaktpersonen an Arbeitgeber oder andere berufliche Kontakte weiterzugeben. Entsprechendes gilt hinsichtlich der Verwendung der Wallet-Funktion für die Speicherung von Familienzertifikaten.

7.3.3 Lokale Verarbeitung durch das ENF

Soweit personenbezogene Daten nur lokal 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 nicht ersichtlich.

Apple und Google haben das ENF nach ihren Vorstellungen und Designkriterien entwickelt und als Systemkomponente in ihre jeweiligen Betriebssysteme integriert. 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 von Google und Apple festgelegt. Corona-Apps können nur dann auf die ENF-Schnittstelle zugreifen, wenn die von Apple bzw. Google formulierten Vorgaben eingehalten und die ENF-Schnittstellen im Einzelfall freigegeben werden. Änderungen an Verfahren und Vorgaben werden allein von Google und Apple festgelegt. Als Hersteller der mobilen Betriebssysteme haben sie zudem die 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 können insoweit als Verantwortliche angesehen werden.

Daneben sind Apple und Google auch für Teile der Verarbeitung von Daten in Zusammenhang mit der Echtheitsprüfung über die jeweiligen Verifikations-Dienste verantwortlich. Sowohl Apple DeviceCheck als auch Google SafetyNet stellen Dienste der Betriebssystemanbieter dar. Apple und Google legen fest, welche Informationen über die Endgeräte der CWA-Nutzer bei Verwendung der Dienste erhoben und geprüft werden, auf welche Art und Weise Daten mit Apple und Google ausgetauscht werden und wie lange Daten gespeichert werden. Dabei werden den Entwicklern die technischen Voraussetzungen von Apple und Google vorgegeben. Insoweit bestimmen Apple und Google Zweck und wesentliche Mittel der Verarbeitung im Rahmen der Verifikations-Dienste.

7.3.4 Verarbeitung durch den EFGS

Für die Datenverarbeitung durch den EFGS zur Ermöglichung der Interoperabilität von nationalen Corona-Apps der EU-Länder 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.

7.3.5 Verarbeitung durch den CHGS

Für die Datenverarbeitung durch den CHGS zur Ermöglichung der Interoperabilität zwischen der deutschen und der Schweizer Corona-App ist das RKI gemeinsam mit dem Schweizer BAG verantwortlich. Zur Regelung der Zusammenarbeit wurde eine Behördenvereinbarung zwischen dem RKI und dem Eidgenössischen Departement des Innern der Schweizerischen Eidgenossenschaft abgeschlossen. Die Behördenvereinbarung dient auch der Erfüllung der Pflicht aus Art. 26 Abs. 1 S. 2 DSGVO zum Abschluss einer transparenten Vereinbarung über die gemeinsame Verarbeitung.

7.3.6 Verarbeitung durch Lab Server / Teststellen-Informationssysteme

Für den Betrieb des Lab Servers und der Teststellen-Informationssysteme sind die jeweiligen Labore bzw. Teststellen verantwortlich.

7.3.7 Verarbeitung durch Prüfsysteme

Die Verantwortlichkeit für die lokale Datenverarbeitung durch ein Prüfsystem liegt bei dem jeweiligen Leistungsanbieter als prüfende Stelle.

7.3.8 Verarbeitung durch Validierungsdienste

Validierungsdienste werden vom Prüfpartner betrieben. Dieser ist für die Datenverarbeitung durch seinen Validierungsdienst verantwortlich.

7.4 Auftragsverarbeiter

Auftragsverarbeiter des RKI für den Betrieb der CWA sind SAP und TSI. Für die jeweiligen Auftragsgegenstände siehe unter Abschnitt 5.9.

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 TSI und SAP als Unterauftragsverarbeiter mit der technischen Bereitstellung und Verwaltung des EFGS beauftragt.

Für den Betrieb und die Wartung des CHGS ist nach Maßgabe der zwischen dem RKI und dem Eidgenössischen Departement des Innern der Schweizerischen Eidgenossenschaft abgeschlossen Behördenvereinbarung das BAG zuständig. Auftragsverarbeiter darf das BAG nur mit Zustimmung des RKI für den Betrieb des CHGS einsetzen.

7.5 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.

7.5.1 Anforderungen an eine Rechtsgrundlage

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

7.5.1.1 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.⁷⁴

7.5.1.2 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.

7.5.2 Rechtsgrundlagen der CWA

Die in Betracht kommenden Rechtsgrundlagen der personenbezogenen Verarbeitung 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.

7.5.2.1 Verarbeitung von Daten der CWA-Nutzer

7.5.2.1.1 Risiko-Ermittlung, Testregistrierung, Warnfunktion, Schnelltest-Nachweis

Rechtsgrundlage für die Verarbeitung personenbezogener Daten von CWA-Nutzern für die Zwecke der Risiko-Ermittlung, der Testregistrierung und der Warnfunktion sowie der Übermittlung der Daten für den namentlichen Schnelltest-Nachweis ist jeweils die Einwilligung des betroffenen CWA-Nutzers (Art. 4 Nr. 7 DSGVO, Art. 6 Abs. 1 S. 1 lit. a DSGVO). Da im

⁷⁴ Siehe zu diesen Anforderungen im Einzelnen EDSA, 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 11.10.2022).

Zusammenhang dieser Funktionen in weiten Teilen Gesundheitsdaten verarbeitet werden, gelten insoweit ergänzend die Anforderungen von Art. 9 Abs. 2 lit. a DSGVO. Für die Verarbeitung im Zusammenhang mit den unterschiedlichen Anwendungsphasen und Funktionen 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.

7.5.2.1.2 COVID-Zertifikate

Hinweis: Die Verarbeitung für die Generierung der COVID-Zertifikate durch den Zertifikatsservice liegt außerhalb des Prüfgegenstands und wird hier lediglich der Vollständigkeit halber erwähnt, da sie ebenfalls im Verantwortungsbereich des RKI stattfindet.

Für die Verarbeitung personenbezogener Daten von CWA-Nutzern für die Ermöglichung der elektronischen Nutzung von Impfzertifikaten kann sich das RKI auf zwei Rechtsgrundlagen im Sinne von Art. 6 Abs. 1 lit. c DSGVO und, soweit Gesundheitsdaten verarbeitet werden, Art. 9 Abs. 2 lit. g DSGVO stützen, nämlich § 22a Abs. 5 S. 4 IfSG und seit dem 01.07.2021 auch Art. 10 Abs. 2 DCC-VO.

§ 22a Abs. 5 IfSG lautet:

„Zusätzlich zu der Impfdokumentation ist auf Wunsch der geimpften Person die Durchführung einer Schutzimpfung gegen das Coronavirus SARS-CoV-2 in einem digitalen Zertifikat (COVID-19-Impfzertifikat) durch folgende Personen zu bescheinigen:

1. *durch die zur Durchführung der Schutzimpfung berechtigte Person oder*
2. *nachträglich von jedem Arzt oder Apotheker*

Die Verpflichtung nach Satz 1 Nummer 2 besteht nur, wenn dem Arzt oder Apotheker eine Impfdokumentation über eine Schutzimpfung gegen das Coronavirus SARS-CoV-2 vorgelegt wird und er sich zum Nachtrag unter Verwendung geeigneter Maßnahmen zur Vermeidung der Ausstellung eines unrichtigen COVID-19-Impfzertifikats, insbesondere um die Identität der geimpften Person und die Authentizität der Impfdokumentation nachzuprüfen, bereit erklärt hat. Zur Erstellung des COVID-19-Impfzertifikats übermittelt die zur Bescheinigung der Schutzimpfung gegen das Coronavirus SARS-CoV-2 verpflichtete Person die in Absatz 2 Satz 1 und Absatz 4 genannten personenbezogenen Daten an das Robert Koch-Institut, das das COVID-19-Impfzertifikat technisch generiert. Das Robert Koch-Institut ist befugt, die zur Erstellung und Bescheinigung des COVID-19-Impfzertifikats erforderlichen personenbezogenen Daten zu verarbeiten.“

Art. 10 Abs. 2 DCC-VO lautet:

„Die personenbezogenen Daten, die in den gemäß dieser Verordnung ausgestellten Zertifikaten enthalten sind, dürfen für die Zwecke dieser Verordnung ausschließlich zum Zwecke des Abrufs und der Überprüfung der im Zertifikat enthaltenen Informationen verarbeitet werden, um die Ausübung des Rechts auf Freizügigkeit innerhalb der Union während der COVID-19-Pandemie zu erleichtern. Nach dem Ende der Geltungsdauer dieser Verordnung findet keine weitere Verarbeitung mehr statt.“

Die entsprechende nationale Rechtsgrundlage in Bezug auf Testzertifikate ist § 22a Abs. 7 S. 3 IfSG und in Bezug auf Genesenenzertifikate § 22a Abs. 6 S. 4 IfSG.

Rechtsgrundlage für die Verarbeitung von Zugriffsdaten der CWA App in Zusammenhang mit dem Download von öffentlichen Schlüsseln, Business Rules und Value Sets ist Art. 6 Abs. 1 lit. e DSGVO in Verbindung mit § 3 BDSG.

Für die Verarbeitung zur Erstellung von Druckversionen von COVID-Zertifikaten wird keine Rechtsgrundlage benötigt, da es sich hierbei nicht um eine personenbezogene Datenverarbeitung durch das RKI handelt (siehe Abschnitt 7.3.2.2). Gleiches gilt für die Übermittlung von Daten im Rahmen der Online-Validierung an Leistungsanbieter und Validierungsdienste auf Wunsch des CWA-Nutzers. Aus Transparenzgründen hat sich das RKI jedoch zur Einholung der Zustimmung des CWA-Nutzers in der Gestalt einer förmlichen Einwilligung entschieden.

7.5.2.1.3 Statistik-Kacheln

Die Rechtsgrundlage für die Verarbeitung der Zugriffsdaten, die beim Download der Coronastatistik-Daten anfallen, ist Art. 6 Abs. 1 lit e. DSGVO i.V.m § 3 BDSG i.V.m. § 4 Abs. 4 BGA-NachfG. Gemäß § 4 Abs. 4 BGA-NachfG hat das RKI die Aufgabe, die Öffentlichkeit über die in seinem Zuständigkeitsgebiet liegenden Themen zu informieren. Die in den Statistik-Kacheln angezeigten Informationen zum aktuellen Infektionsgeschehen und zur Nutzung der CWA App sind das Ergebnis von infektionsepidemiologischen Auswertungen und liegen somit im Zuständigkeitsgebiet des RKI. Die Verarbeitung der Zugriffsdaten ist daher notwendig, um die CWA-Nutzer als Teil der Öffentlichkeit im Rahmen der App-Nutzung über das aktuelle Infektionsgeschehen informieren zu können.

7.5.2.2 Verarbeitung von Daten anderer Nutzer

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

Soweit die 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 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.

Im Fall der Schweizer Corona-App beruht die Verarbeitung zur Warnung von Nutzern ebenfalls auf der ausdrücklichen Einwilligung der Nutzer (Art. 6 Verordnung über das Proximity-Tracing-System für das Coronavirus Sars-CoV-2).

7.5.3 Begründung der Einwilligung als Rechtsgrundlage

Von verschiedenen Seiten wurden im Vorfeld der Veröffentlichung des ersten Release der CWA App Zweifel am Vorliegen der Wirksamkeitsvoraussetzungen einer Einwilligung für die Datenverarbeitung im Rahmen der CWA geäußert.⁷⁵ Daher wird nachfolgend dargestellt, auf welchen Erwägungen die Entscheidung des RKI für die Einwilligung als Rechtsgrundlage trotz der geäußerten Bedenken beruhte.

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

7.5.3.1 Wirksamkeitsvoraussetzungen

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.

⁷⁵ 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 11.10.2022) wenn möglich, die Nutzung einer gesetzlichen Rechtsgrundlage, da es an der Freiwilligkeit fehlen könnte.

Vgl. auch [netzpolitik.org: EU-Abgeordnete hinterfragen Contact Tracing](https://netzpolitik.org/2020/eu-abgeordnete-hinterfragen-contact-tracing/), abrufbar unter: <https://netzpolitik.org/2020/eu-abgeordnete-hinterfragen-contact-tracing/> (abgerufen am 11.10.2022).

7.5.3.1.1 Zweckbestimmtheit

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“⁷⁶.

Die Einwilligungen werden jeweils für die zur Inanspruchnahme der folgenden App-Funktionen bzw. CWA-Services notwendigen Verarbeitungen eingeholt:

- Risiko-Ermittlung
- Testregistrierung (einschließlich des Testabrufs) und die Warnung anderer,
- namentlicher Schnelltest-Nachweis,
- Nutzung der Verifikations-Hotline,
- Einchecken bei Events
- Teilnahme an der Datenspende
- Teilnahme an Befragungen
- Überprüfung von COVID-Zertifikaten
- Aktualisierung und Erneuerung von COVID-Zertifikaten

Da die Zwecke der oben genannten Funktionen klar abgrenzbar und aus der Sicht eines CWA-Nutzers, der sich bewusst für die Installation der CWA App bzw. die Nutzung der jeweiligen Funktionen entscheidet, jeweils nachvollziehbar sind, ist nicht anzunehmen, dass die Zwecke der jeweiligen Einwilligungen nicht ausreichend bestimmt werden können. Die Einwilligungen werden situativ im jeweiligen Zusammenhang mit der Auslösung einer App-Funktion oder der Inanspruchnahme eines CWA-Service eingeholt und jeder Einwilligung geht eine konkrete Erläuterung des Zweckes und Verarbeitungszusammenhangs voraus.

Dies gilt auch in Bezug auf die seit Release 1.9 gleichzeitig eingeholten Einwilligungen für die Testregistrierung (Testabruf) einerseits und die länderübergreifende Warnung anderer Nutzer andererseits. Zwar handelt es sich um verschiedene Abschnitte im Ablauf, so dass die Einwilligungen auch getrennt voneinander eingeholt werden könnten. Dies schließt es jedoch nicht aus, diese Einwilligungen zukünftig gleichzeitig einzuholen, um die Warnquote nach Abruf eines positiven Testergebnisses zu verbessern, eine übersichtliche und einfache strukturierte Nutzerführung umzusetzen und die für die konkrete Einwilligung zur Warnung anderer Nutzer sowie den damit verfolgten Zweck der Unterbrechung von Infektionsketten erforderlichen Informationen und Erläuterungen auf einen Zeitpunkt vorzuverlegen, zu dem der Nutzer möglichst aufnahme- und entscheidungsbereit ist. Nach Erwägungsgrund 32 S. 4 DSGVO soll eine Einwilligung grundsätzlich zweckbezogen erteilt werden und alle Verarbeitungsvorgänge, die demselben Zweck dienen, umfassen. Vorliegend dienen beide Funktionen dem gleichen Zweck, nämlich der frühzeitigen Unterbrechung von Infektionsketten gemäß Zweckdefinition (2) (siehe Abschnitt 5.3). Die Einwilligungserteilung erfolgt jeweils durch eine dem jeweiligen Kontext entsprechende geeignete und eindeutige bestätigende

⁷⁶ Klement in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, DSGVO Art. 7, Rn. 68.

Handlung (z.B. durch Antippen eines entsprechenden Buttons, mündliche Erklärung im Rahmen der Verifikations-Hotline oder Erklärung zum Testabruf im Rahmen eines Tests).

Im Rahmen der Verifikations-Hotline wird die Einwilligung telefonisch 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 Verifikations-Hotline 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. Die Einwilligung wird auf dem Begleitdokument dokumentiert. Er erhält hierzu ein erläuterndes Begleitdokument, das den Zweck der Übermittlung erläutert.

Bei einem Schnelltest wird der CWA-Nutzer von der Teststelle gefragt, ob er der Übermittlung des Testergebnisses an die CWA zustimmt, damit das Testergebnis in der CWA App angezeigt werden kann. Zusätzlich wird er gefragt, ob er der namentlichen Anzeige seines Testergebnisse in der CWA App zustimmt. Die Einwilligung wird im Teststellen-System dokumentiert.

Die spezifische Zweckbindung für die länderübergreifenden Aspekte der Funktionen im Zusammenhang mit dem EFGS ist in Art. 7a Abs. 1 des Durchführungsbeschlusses (EU) 2019/1765 der EU-Kommission vorgeschrieben. Für die länderübergreifende Komponente der Risiko-Ermittlung wird keine separate Einwilligung eingeholt, auch wenn die CWA App seit 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 nach einem Update auf eine Version höher als 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 möglicherweise lediglich zusätzliche Positivschlüssel, nämlich die von Nutzern anderer nationaler Corona-Apps. Entsprechendes gilt in Bezug auf die länderübergreifenden Funktionen im Zusammenhang mit dem CHGS.

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 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 Warnfunktion die länderübergreifende Übermittlung an die Verantwortlichen der anderen nationalen Corona-Apps durch die mit Nationalflaggen bebilderte Länderliste unterstrichen.

7.5.3.1.2 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.⁷⁷ 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 Kontaktnachverfolgung, der länderübergreifenden Risiko-Ermittlung, der Abläufe im Zusammenhang mit einem durchgeföhrten Test und der Warnfunktion sowie die Verarbeitung zur Erstellung eines namentlichen Schnelltest-Nachweises 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 explizit auf die Datenverarbeitung durch die am EFGS bzw. CHGS teilnehmenden weiteren für die anderen nationalen Corona-Apps Verantwortlichen hingewiesen. Beim Hinzutreten oder Ausscheiden eines neuen teilnehmenden eine andere nationale Corona-App Verantwortlichen wird über einen internen Prozess sichergestellt, dass die Information der Änderung der Liste der teilnehmenden für die anderen nationalen Corona-Apps

⁷⁷ Buchner/Kühling, in: Kühling/Buchner, 3. Aufl. 2020, DS-GVO Art. 7 Rn. 59.

Verantwortlichen in der CWA App rechtzeitig aktualisiert wird und die jeweilige Einwilligungserklärung stets den aktuellen Stand abbildet.

Eine Einwilligung, die sich auf die Verarbeitung von Gesundheitsdaten bezieht, muss ausdrücklich erteilt werden. Der Gesundheitszusammenhang muss zwar nicht ausdrücklich benannt werden. Die verwendeten Einwilligungstexte weisen aus Transparenzgründen dennoch ausdrücklich auf den Gesundheitsbezug hin.

Im Zusammenhang mit der Einwilligung in den Testabruf, die länderübergreifende Warnung und in die Übermittlung im Rahmen der Validierung wird aus Transparenzgründen explizit herausgestellt, dass es sich bei den zu verarbeitenden Daten um Angaben mit einem Gesundheitsbezug handelt. In Bezug auf die Interoperabilität der CWA App ist zudem entscheidend, dass der CWA-Nutzer nachvollziehen kann, dass das RKI und die am EFGS bzw. CHGS teilnehmenden weiteren für die anderen nationalen Corona-Apps Verantwortlichen gemeinsame Verantwortliche sind. Die Informationstexte und die Einwilligungserklärung im Rahmen der länderübergreifenden Warnung erläutern den Bedeutungsinhalt der Tagesschlüssel und weisen 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 Kategorien 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.

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.

7.5.3.1.3 Freiwilligkeit

Das Freiwilligkeitsprinzip gliedert sich neben dem Unterprinzip „Informiertheit“ auch in das Prinzip „Freiheit von Zwang“.⁷⁸ 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 (DSGVO-Erwägungsgrund 42).

Von verschiedenen Seiten und in der öffentlichen Diskussion⁷⁹ wurden insbesondere im Vorfeld des ersten Release der CWA App grundsätzliche Bedenken an der Eignung der Einwilligung als Rechtsgrundlage für die Datenverarbeitung der CWA geäußert. Diese Bedenken wurden damit begründet, dass es an der Freiwilligkeit der Einwilligung fehlen würde:

Teilweise wurde eine fehlende Freiwilligkeit im Fall der CWA daraus hergeleitet, 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 auf fehlende Freiwilligkeit geschlossen werden.⁸⁰ 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 wäre naheliegend, wenn gesetzliche Vorgaben zur Nutzung der CWA App gemacht werden oder seitens einer Behörde ein bestimmter Verbreitungsgrad der CWA App zur Bedingung beispielsweise für Lockerungsmaßnahmen oder Zutrittsvoraussetzungen gemacht würde. Eine solche Situation bestand jedoch nicht und ist auch nicht geplant. Dies gilt auch

⁷⁸ Heckmann/Paschke in Ehmann/Selmayr, DSGVO Kommentar, 2. Aufl. 2018, DS-GVO Art. 7, Rn. 48.

⁷⁹ So auch 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 11.10.2022); 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: Krempel, 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 11.10.2022) mit Verweis auf eine 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).

⁸⁰ 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 11.10.2022);

mit Blick auf die später hinzugekommene Wallet-Funktion. Der Nachweis von COVID-Zertifikaten ist und war zu jedem Zeitpunkt sowohl mit der Papier- als auch mit der elektronischen Fassung eines COVID-Zertifikats möglich. Die Papier- und die elektronische Form des COVID-Zertifikats sind gleichwertig. Selbst wenn die CWA App nur zum Mitführen eines COVID-Zertifikats verwendet werden sollte, wäre dies möglich, ohne dass andere Funktionen der CWA App genutzt werden müssen. Die Freiwilligkeit in der CWA App abgegebener Einwilligungen wird daher hierdurch nicht tangiert. Für Dritte ist auch 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. Dies gilt auch bei Nutzung des Schnelltest-Nachweises. Dies lässt nämlich zum einen keinen Schluss darauf zu, ob auch die weiteren Funktionen der CWA App, wie die Risiko-Ermittlung, genutzt werden. Zudem kann der Schnelltest-Nachweis auch auf anderem Wege, beispielsweise durch Vorlage eines Papierdokuments, erbracht werden. Die Vorlage des namentlichen Schnelltest-Nachweises in der CWA App muss und soll daher nicht zur (einzig) Bedingung für den Zugang zu Leistungen oder Vorteilen gemacht werden. Hierauf wird der Nutzer auch in CWA App an verschiedenen Stellen ausdrücklich hingewiesen.

Teilweise wird die Eignung der Einwilligung als Rechtsgrundlage in Frage gestellt, weil für die Annahme der Freiwilligkeit eine echte Wahlmöglichkeit vorausgesetzt wird und nur so die Schutzwirkung der Einwilligung erfüllt werden kann.⁸¹ An einer echten Wahlmöglichkeit kann es im Fall der CWA fehlen, wenn sich einzelne Personen einem erheblichen gesellschaftlichen Druck ausgesetzt sehen, die CWA App zu nutzen. Wenn beispielsweise Familienmitglieder oder Arbeitskollegen die CWA App nutzen und sich herausstellt, dass eine Person aus ihrem Kreis dies verweigert, kann dies zu einem moralischen Vorwurf und sozialem Druck führen, sodass sie die CWA App schließlich trotz innerer Ablehnung nutzt, um sich dem Druck zu entziehen. Dies kann auch dann eintreten, wenn von der Nutzung der CWA App von staatlicher Seite Lockerungsmaßnahmen oder von privaten Akteuren (z. B. Arbeitgeber, Versicherungen, Veranstalter, Kultureinrichtungen) die Gewährung bestimmter Vorteile oder zumindest das Fernbleiben von Nachteilen abhängig gemacht würden, insbesondere wenn es dann tatsächlich von der einzelnen Person abhängen würde, ob auch ihr persönliches Umfeld von weiteren Lockerungsmaßnahmen oder Vorteilen profitieren oder es Nachteile erleiden kann. Hier käme dann neben einem sozialen und beruflichen Druck unter Umständen auch ein staatlicher Druck zum Tragen. Dem RKI sind seit der Veröffentlichung der CWA App allerdings keine Anhaltspunkte bekannt geworden, die Anlass geben, zu vermuten, dass – abgesehen von praktisch unvermeidlichen Einzelfällen im privaten Bereich – ein nicht nur unerheblicher Druck oder gar Zwang zur Nutzung der CWA App ausgeübt wird. Auch mit Blick auf die Funktion des namentlichen Schnelltest-Nachweises sowie des Zertifikatsnachweises ist davon nicht auszugehen. Denn soweit der Nachweis dieser Dokumente erforderlich ist, kann er stets auch weiterhin ohne die CWA App erbracht werden, etwa durch Vorlage eines entsprechenden Papierdokuments und im Fall der COVID-Zertifikate auch durch Nutzung der CovPass-App als

⁸¹ 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 11.10.2022), mit weiterem Verweis auf Article 29 Data Protection Working Party 2018, S. 5.

reine Wallet-App. Selbst bei einem unterstellten anfänglichem Bestehen eines nicht nur unerheblichen Drucks zur Nutzung der CWA App für namentliche Schnelltest-Nachweise wäre dieser durch die zwischenzeitliche Einführung und Verbreitung von COVID-Testzertifikaten sowie die erfolgten Lockerungen von Schutzmaßnahmen für geimpfte und genesene Personen nunmehr erheblich reduziert.

Die Zweifel an der Freiwilligkeit der eingeholten Einwilligungen haben sich rückblickend auf die Entwicklungen seit dem Release der ersten CWA App-Version nicht bestätigt. Insbesondere ist die Nutzung der CWA App aufgrund der konsequenten Weiterführung des anfänglich festgelegten Privacy-by-Design-Ansatzes nach wie vor nicht überprüfbar, ohne dass der Nutzer die CWA App vorzeigt. Weder dem RKI noch Dritten ist es ohne Mitwirkung des CWA-Nutzers möglich einzusehen, ob die CWA App auf einem Smartphone installiert und volumnäßig genutzt wird. Eine solche Veröffentlichung von Daten ist weiterhin nicht vorgesehen und geplant. Auch gibt es weiterhin keine Pläne oder gesetzliche Normierungen, die bspw. die Ausweitung von staatlichen Lockerungsmaßnahmen von der Nutzung der CWA App abhängig machen. Zwar können CWA-Nutzer die CWA App verwenden, um bestimmte gesetzliche Anforderungen zu erfüllen (bspw. den Schnelltest- oder Zertifikatsnachweis). Die CWA App war und ist hierfür aber zu keinem Zeitpunkt das einzige Mittel, so dass die gesetzlichen Voraussetzungen stets auch auf anderem Wege, der für alle Teile der Bevölkerung zugänglich ist, erfüllt werden können. Ein erheblicher Teil der Bevölkerung verfügt auch nicht über ein geeignetes, d. h. ENF-kompatibles Smartphone (z. B. Huawei).

Nach den plausiblen Schätzungen des RKI wird die CWA App „nur“ von ca. 28 Millionen Personen bzw. einem Drittel der Bevölkerung aktiv genutzt, d. h. die Mehrheit der Bevölkerung nutzt die CWA App nicht oder jedenfalls nicht aktiv.⁸² Dies weist deutlich darauf hin, dass es einen sozialen Nutzungsdruck oder jedenfalls einen sozialen Nutzungsdruck in einem die Freiwilligkeit der Einwilligungen gefährdendem Ausmaß nicht gibt. Im Ergebnis haben sich die geäußerten Bedenken hinsichtlich der Freiwilligkeit von für die CWA eingeholten Einwilligungen daher nicht bestätigt. Dem RKI sind auch sonst keine Anhaltspunkte bekannt geworden, die Anlass zu ernsthaften Zweifeln an der Freiwilligkeit der im Rahmen des Prüfgegenstands eingeholten Einwilligungen geben können.

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 klar darauf hingewiesen, dass die Verweigerung einer Einwilligung keine negativen Folgen für den jeweiligen CWA-Nutzer hat und es wird, soweit möglich, auf die Möglichkeit und die praktische Ausübung des Widerrufsrechts hingewiesen.

In Bezug auf die optionale Angabe zum Symptombeginn im Rahmen der Warnfunktion wird durch die zusätzliche Entscheidungsmöglichkeit ("weiter mit Symptom-Abfrage" oder "weiter ohne Symptom-Abfrage") sowie die ausdrücklichen Erklärungen in dem Eingabeschritt und bei

⁸² CWA-Team, „Wie viele aktive Nutzende hat die Corona-Warn-App?“, Kennzahlen zur Evaluation (Beitrag vom 03.03.2022) abrufbar unter: <https://www.coronawarn.app/de/science/2022-03-03-science-blog-5/> (zuletzt abgerufen am 11.10.2022).

Abgabe der Einwilligungserklärung am Ende des Eingabedialogs auf die Freiwilligkeit hingewiesen.

Dass seit der CWA App-Version 1.9 mit der Einwilligung für die Testregistrierung (Testabruf) auch die Einwilligung für die Warnung eingeholt wird, um im Fall eines positiven Testergebnisses die Warnung anderer Nutzer zu ermöglichen, steht der Freiwilligkeit der Einwilligung für die Warnung nicht entgegen. Zwar handelt es sich um unterschiedliche App-Funktionen, so dass die Einwilligungen auch getrennt voneinander eingeholt werden könnten. Die Einholung einer gesonderten Einwilligungserklärung für das Teilen des Testergebnisses wäre in Hinblick auf Erwägungsgrund 43 S. 2 DSGVO aber nur angebracht, wenn der CWA-Nutzer infolge der frühzeitigen Einwilligungseinhaltung gegen seinen Willen gezwungen würde, sein Testergebnis im Fall eines positiven Befunds mit anderen Nutzern zu teilen. Dies ist jedoch nicht der Fall, da der CWA-Nutzer seine Einwilligung in das Teilen seines Testergebnisses vor dessen Abruf jederzeit in der CWA App widerrufen kann und zudem dem ENF explizit die Freigabe seiner Tagesschlüssels für die CWA App erlauben muss, bevor die CWA App eine Warnung auslösen kann. Hierauf wird der CWA-Nutzer bei Abgabe der Einwilligungserklärung ausdrücklich hingewiesen. Zudem wird der CWA-Nutzer unmittelbar vor dem Auslösen einer Warnung situativ mit seiner zuvor getroffenen Entscheidung nochmals konfrontiert und kann seinen Einwilligungsstatus unmittelbar vor der Freigabe seiner Tagesschlüssel für die CWA App überprüfen und bei Bedarf anpassen. Die vorstehenden Erwägungen zur Freiwilligkeit lassen sich auf die Einwilligung für die Verarbeitung der personenbezogenen Daten in Zusammenhang mit der Verifikations-Hotline übertragen. Der standardmäßige Datenschutzhinweis des Hotline-Mitarbeiters zu Beginn des Gesprächs enthält auch hier ausdrückliche Hinweise auf die Freiwilligkeit der Einwilligung.

Vor diesem Hintergrund gibt es im Hinblick auf die obigen Erwägungen weiterhin keinen Grund zu der Annahme, dass die Freiwilligkeit der Einwilligungen der CWA-Nutzer nicht ausreichend gewährleistet ist.⁸³

⁸³ 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 EDSA, sofern eine tatsächliche Möglichkeit zur Verweigerung und dem Widerruf der Einwilligung gegeben ist. 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. 32, S. 9, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_de.pdf (zuletzt abgerufen am 07.10.2022).

7.5.3.2 Besondere Einwilligungsfälle

7.5.3.2.1 Minderjährige

Die CWA App richtet sich gemäß ihren Nutzungsbedingungen an Personen, die das 16. Lebensjahr vollendet haben. Eine besondere Einwilligung für unter 16-jährige CWA-Nutzer ist nicht vorgesehen. Da die CWA keine Nutzerverwaltung vorsieht, kann jedoch grundsätzlich jeder mit einem kompatiblen Smartphone die CWA App installieren und nutzen. Insofern besteht das Risiko, dass Einwilligungen in der CWA von nicht einwilligungsfähigen minderjährigen CWA-Nutzern erteilt werden und diese Einwilligung in der Folge keine wirksame Rechtsgrundlage darstellt.

Es gibt keine praktikable, datensparsame Möglichkeit, dies zu verhindern. Eine zuverlässige Altersverifikation würde die Erhebung weiterer, identifizierender Datenpunkte erfordern. Jede Erstellung von „Nutzeraccounts“ und Einführung einer zentralen Nutzerverwaltung 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 in den Nutzungsbedingungen vorgesehenen Altersbeschränkung führt allerdings nicht zwangsläufig zur Unwirksamkeit einer eingeholten Einwilligung. Unwirksam wäre die Einwilligung nur bei fehlender Einsichtsfähigkeit, wenn also dem minderjährigen CWA-Nutzer die Reichweite der erteilten Einwilligung nicht klar ist. 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 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.

7.5.3.2.2 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 CWA-Nutzers durch 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.⁸⁴ Da es sich bei dem RKI um eine öffentliche Stelle handelt und jedenfalls eine personenbezogene Verarbeitung 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 Erheben von Daten im Sinne von Art. 4 Nr. 2 DSGVO ein aktives Tun voraus.⁸⁵ 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 EuGH⁸⁶ ist zwar nicht erforderlich, „dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer

⁸⁴ Ernst in: Paal/Pauly, § 1 BDSG Rn. 18; Klar in Kühling/Buchner, 3. Aufl. 2020, § 1 BDSG Rn. 34.

⁸⁵ Vgl. nur Roßnagel in: Simitis/Hornung/Spiecker gen. Döhmann. Art. 4 Nr. 2, Rn. 15.

⁸⁶ EuGH, Urt. v. 19.10.2016, Rs. Breyer, C-582/14, Rn. 42 ff.

einigen 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 beteiligten Akteure indes nicht, sodass 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.

7.5.3.3 Nachteile anderer Rechtsgrundlagen

Eine Einwilligung als Rechtsgrundlage ist aufgrund der mit ihr verbundenen höheren Transparenz und Rechtssicherheit gegenüber den CWA-Nutzern und der ihr innewohnenden Warnfunktion im Ergebnis datenschutzfreundlicher und wird daher gegenüber den in Betracht kommenden gesetzlichen Zulässigkeitstatbeständen als vorzugswürdig angesehen.

7.5.3.3.1 § 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.

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.

7.5.3.3.2 § 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 (also ohne EFGS und CHGS) darstellen kann. Es ist zudem unklar, ob auch die Verarbeitung besonderer Kategorien personenbezogener Daten erfasst wäre.

7.5.3.3.3 § 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 umfassend 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.⁸⁷ 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. Nach teilweise in der Literatur vertretener Auffassung werden die Rechtsgrundlagen in § 22 BDSG diesem Anspruch nicht gerecht.⁸⁸ Vorliegend kann die Entscheidung dieser Streitfrage dahinstehen, die spezifischen Einwilligungen für die einzelnen Datenverarbeitungsvorgänge sind jedenfalls gegenüber dem Auffangtatbestand der Rechtsgrundlage in § 22 BDSG vorzugswürdig.

7.6 Bewertung der Drittlandübermittlung

Mit Ausnahme der für die Interoperabilität zwischen CWA und der Schweizer Corona-App naturgemäß notwendigen Übermittlung von Daten in die Schweiz ist die Verarbeitung so gestaltet, dass die Kernfunktionen ohne eine Übermittlung von Daten in Drittländer, das heißt Länder außerhalb der EU/EWR, auskommen.

Im Rahmen der Echtheitsprüfung kann es dagegen zu einer Drittlandübermittlung kommen. Die Echtheitsprüfung ist derzeit nur für die freiwillige Teilnahme an der Datenspende sowie die

⁸⁷ Vgl. Frenzel in: Paal/Pauly/Frenzel, 3. Aufl. 2021, BDSG § 22 Rn. 2.

⁸⁸ Weichert in Kühling/Buchner, 3. Aufl. 2020, § 22 Rn. 8; Heckmann/Scheuer in Gola/Heckmann/Scheurer, 13. Aufl. 2019, BDSG § 22 Rn. 5; weiterführend Rose in Taeger/Gabel/Rose, 4. Aufl. 2022, BDSG § 22 Rn. 8; das BMI erachtet die Norm im Evaluationsbericht für verfassungsgemäß (Evaluierung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Oktober 2021, S. 22f).

Teilnahme an Befragungen notwendig. Zukünftig können weitere Funktionen hinzukommen, die ebenfalls eine Echtheitsprüfung erfordern.

Die Datenübermittlung erfüllt die Voraussetzungen von Art. 44 ff DSGVO. Mangels anderer Optionen wird die Drittlandübermittlung auf die ausdrückliche Einwilligung der CWA-Nutzer gem. Art. 49 Abs. 1 lit. a DSGVO gestützt.

Da das Privacy-Shield-Abkommen durch das Urteil des EuGH in der Rechtssache C-311/18 „Schrems II“ für ungültig erklärt wurde, besteht derzeit kein Angemessenheitsbeschluss für die USA gem. Art. 45 DSGVO.

Nach Maßgabe der EuGH-Entscheidung in der Rechtssache „Schrems II“ und unter Berücksichtigung der hierzu ergangenen EDPB-Guidelines 01/2020 ist eine Übermittlung personenbezogener Daten allein auf Grundlage der in Art. 46 DSGVO benannten Mechanismen zudem nicht datenschutzkonform möglich. Insbesondere sind auch die Standardvertragsklauseln zwischen Verantwortlichen kein probates Mittel, um ein angemessenes Datenschutzniveau für die Übermittlung sicherzustellen. Weitere technische Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung eines angemessenen Schutzniveaus können durch das RKI nicht sichergestellt werden.

Die Unterausnahme gem. Art. 49 Abs. 3 DSGVO ist zudem auf Datenverarbeitungen in Zusammenhang mit der CWA nicht anwendbar, da das RKI insoweit nicht hoheitlich handelt. Die CWA stützt sich nicht auf „hoheitliche“ Rechtsgrundlagen. Weder beruht der Betrieb der App auf einem konkreten gesetzlichen Auftrag, noch beruht die Verarbeitung auf einer öffentlich-rechtlichen Rechtsgrundlage gem. Art. 6 Abs. 1 lit. c und e Abs. 2, 3 DSGVO sowie Art. 9 Abs. 1 lit. b, g, h, i und j DSGVO. Vielmehr erfolgt die Verwendung der CWA durch die CWA-Nutzer auf Grundlage eines (zivilrechtlichen) Vertrags, die Verarbeitung personenbezogener Daten erfolgt im Rahmen der gesamten CWA auf Grundlage der freiwilligen Einwilligungen der Nutzer.

Der CWA-Nutzer erteilt seine ausdrückliche Einwilligung in die Drittlandübermittlung auch in informierter Weise. Der CWA-Nutzer wird vorab über die für ihn bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet.

Zudem bestehen keine Bedenken gegen die Freiwilligkeit der Einwilligung. Die Einwilligung in die Drittlandübermittlung dient nicht den „Hauptzwecken“ bzw. Kernfunktionen der CWA App, sondern ist nur im Rahmen der Nutzung von „Nebenfunktion“ erforderlich. Weder ist zu erwarten, dass bezüglich der Nutzung dieser Funktionen ein besonderer öffentlicher Druck besteht, noch erwachsen dem CWA-Nutzer aus der Verwendung dieser Funktionen persönliche Vorteile oder aus der Verweigerung Nachteile oder ein geringerer „Schutz“ durch die CWA App. Insbesondere ist die zusätzliche Einwilligung nicht erforderlich, um die Kernfunktionen der CWA App verwenden zu können.

Die Drittlandübermittlung in Zusammenhang mit der Echtheitsprüfung ist auch als erforderlich anzusehen. Die Echtheitsprüfung der Endgeräte dient der Gewährleistung der Datenqualität der im Rahmen der Datenspende und der Befragungen des RKI erhobenen Daten, indem Datenübermittlungen an den Data Donation Server, die nicht unter Einsatz einer CWA App

erfolgten, (sondern z.B. im Rahmen konzertierter Aktionen initiiert wurden) leichter technisch zu erkennen sind. Andere Mittel zur Risikoreduzierung, die gleich geeignet und ebenso datensparsam sind, sind nicht ersichtlich. Die bewährten Verfahren zur Beschränkung von Systemzugängen für ausgewählte Nutzer, mittels derer die Sicherheit erhöht werden könnte, dass die Daten unter Einsatz einer CWA App generiert bzw. die Einladung zur Befragung von CWA-Nutzern von nicht-manipulierten Endgeräten angenommen werden (User-Name/Passwort, Zertifikate, 2-Factor Authentication usw.) eignen sich für die CWA App nicht, da das Datenschutzkonzept der CWA App bewusst kein Nutzerkonzept vorsieht, um eine weitgehend pseudonyme Nutzung zu ermöglichen.

Dabei wird auch der Charakter von Art. 49 DSGVO als Ausnahmetatbestand berücksichtigt. Insbesondere hat sich das RKI zunächst um Möglichkeiten bemüht, die Übermittlung im Rahmen eines der Mechanismen nach den Artikeln 45 und 46 DSGVO abzusichern.⁸⁹ Insbesondere wird die Drittlandübermittlung nur auf die Einwilligung gem. Art. 49 Abs. 1 lit. a DSGVO gestützt, soweit keine anderen Übertragungsmechanismen gem. Art. 44 ff DSGVO ersichtlich sind. Das RKI hat auch berücksichtigt, dass Ausnahmen eng auszulegen sind, damit sie nicht zur Regel werden.

Im Falle der Datenübermittlung an den CHGS in der Schweiz liegt zurzeit ein Angemessenheitsschluss der EU-Kommission nach Art. 45 Abs. 3 DSGVO vor. Für den Fall, dass das neue DSG der Schweiz noch vor Beendigung der Zusammenarbeit im Rahmen des CHGS in Kraft treten wird und infolgedessen der bestehende Angemessenheitsbeschluss wegfallen sollte, haben sich die Parteien der Zusammenarbeit zugrundeliegenden Behördenvereinbarung zur Schaffung anderer geeigneter Garantien im Sinne des Art. 46 DSGVO verpflichtet.

Das BMG beabsichtigt zur Vermeidung einer Drittlandübermittlung im Rahmen der Online-Validierungsmöglichkeit nur solche Validierungsdienste in die Liste anerkannter Validierungsdienste aufzunehmen, deren gesamte Datenverarbeitung in den Anwendungsbereich der DSGVO fällt und vollständig innerhalb der EU stattfindet.

7.7 Rechte der betroffenen Personen

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

⁸⁹ EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679.

zudem die Widerruflichkeit der Einwilligung für die Zukunft sichergestellt werden. Ausnahmen hiervon sind nur unter engen gesetzlichen Voraussetzungen möglich.

7.7.1 Rechte der CWA-Nutzer

7.7.1.1 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 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 bzw. CHGS 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 bestehen gemäß Art. 11 Abs. 2 und Art. 12 Abs. 2 DSGVO die Rechte der betroffenen Person nicht.

7.7.1.1.1 Einwilligung für die Risiko-Ermittlung

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

7.7.1.1.2 Einwilligung für die Testregistrierung und zur Übermittlung des Schnelltest-Nachweises

Zum Widerruf der Einwilligung für die Testregistrierung und zur Übermittlung der Schnelltest-Daten zur Anzeige des namentlichen Schnelltest-Nachweises 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 nunmehr um anonyme Daten handelt. Nach Abrufen des Testergebnis kann das in der CWA App angezeigte Testergebnis grundsätzlich jederzeit gelöscht werden. Im Falle eines abgerufenen positiven Schnelltest-Ergebnisses verbleibt dieses gegenwärtig, bis nach einer etwaigen erfolgten Warnung anderer oder dem Rücksetzen der App. Negative Schnelltest-Ergebnisse und namentliche Schnelltest-Nachweise verlieren nach 48 Stunden ihre Gültigkeit, die Schnelltest-Daten werden dann nicht mehr angezeigt.

7.7.1.1.3 Einwilligung für die Warnfunktion

Solange der CWA-Nutzer noch keine Warnung ausgelöst hat, kann er seine im Rahmen der Testregistrierung erteilte Einwilligung für die Warnfunktion jederzeit in der CWA App widerrufen, indem er auf dem Teststatus-Screen seinen Einwilligungsstatus aufruft und dort den Schieberegler für sein Einverständnis für die Funktion „Andere warnen“ deaktiviert. Auch nach dem Widerruf der Einwilligung wird der CWA-Nutzer über sein Testergebnis informiert, sobald dieses bereitsteht.

Sobald der CWA-Nutzer eine Warnung ausgelöst hat, ist zum Widerruf der Einwilligung das Löschen oder Zurücksetzen der CWA App erforderlich. 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 nach Auslösen einer Warnung bietet die CWA App nicht an, da eine Löschung von bereits an andere Nutzer verteilten Positivschlüssel und Check-ins (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.

Zudem kann ein CWA-Nutzer, der sein Testergebnis nicht mit anderen Nutzern teilen möchte, auch die Freigabe seiner im ENF gespeicherten Tagesschlüssel für die CWA App ablehnen. In diesem Fall wird ebenfalls keine Warnung ausgelöst, ohne dass die CWA App gelöscht oder zurückgesetzt werden muss. Die Check-in-basierte Warnung kann für einzelne oder alle Events durch den CWA-Nutzer verhindert werden, indem die Events unter „Meine Check-ins“ entfernt werden.

7.7.1.1.4 Einwilligung für die Event-Registrierung

Der Widerruf der Einwilligungen im Rahmen der Event-Registrierung nur lokal durch das Entfernen eines gespeicherten Events durch den CWA-Nutzer erfolgen. Nach der Entfernung eines oder aller Einträge in der CWA App wird eine spätere Check-in-basierte Warnung eines

anderen CWA-Nutzers keine Übereinstimmung im Rahmen der Risikoermittlung mehr erzielen.

7.7.1.1.5 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.

7.7.1.1.6 Einwilligung für die Datenspende

Widerruf der CWA-Nutzer die Einwilligung für die Datenspende im Einstellungsmenü der CWA App, wird die Übermittlung von Nutzungsdaten sofort eingestellt. Da die bereits übermittelten Daten keine Identifizierung des CWA-Nutzers zulassen, ist keine Löschung erforderlich und auch nicht möglich, sodass die übermittelten Nutzungsdaten weiterhin für die Auswertung im Rahmen der Datenspende zur Verfügung stehen.

7.7.1.1.7 Einwilligung für die Echtheitsprüfung

Ein Widerruf der CWA-Nutzer hinsichtlich der Einwilligung für die Echtheitsprüfung ist nicht möglich und daher auch nicht vorgesehen, da die Echtheitsprüfung sofort nach Erteilung der Einwilligung durchgeführt wird und es sich um einen einmaligen Vorgang handelt. Hierauf wird der CWA-Nutzer im Rahmen der Datenschutzerklärung der CWA App hingewiesen.

7.7.1.1.8 Einwilligung für die Übermittlung der Fehlerberichte

Der Widerruf der Einwilligung in die Übermittlung der Fehlerberichte ist über den technischen Support möglich, sofern der CWA-Nutzer zuvor die Fehlerbericht-ID mitgeteilt hat. IN diesem Fall würde der Widerruf umgesetzt und der Fehlerbericht vorzeitig gelöscht werden. Ist keine Fehlerbericht-ID mitgeteilt worden, wird im Allgemeinen eine Zuordnung zu einem bestimmten CWA-Nutzer nicht möglich sein, die Löschung wird dann nach Ablauf von 14 Tagen automatisiert erfolgen.

7.7.1.1.9 Einwilligungen für die Online-Validierung

Betroffenenrechte in Bezug auf die Datenverarbeitung im Rahmen der Online-Validierung können faktisch nur beim Leistungsanbieter und ggf. dem Validierungsdienst geltend gemacht werden. Das RKI verarbeitet selbst keine für das RKI personenbezogenen Daten in diesem Zusammenhang. Ein Widerrufsrecht hinsichtlich der beiden für die Online-Validierung in der Form von Einwilligungserklärungen erteilten Zustimmungen in die Verarbeitung der CWA App und Übermittlung der Online-Validierungsdaten aus der CWA App an einen Validierungsdienst besteht daher nicht und würde ohnehin leerlaufen, weil die Validierung unmittelbar nach dem Antippen des Einverständnis-Buttons durch den CWA-Nutzer erfolgt und umgehend abgeschlossen ist. Ein Abbruch der Online-Validierung ist in der CWA App vor der Übermittlung zwar jederzeit möglich, wodurch alle lokal gespeicherten Daten zum Buchungsvorgang gelöscht werden. Mit erfolgter Einwilligung finden Übermittlung und Validierung jedoch in wenigen Augenblicken statt, so dass die maßgebliche Datenverarbeitung praktisch nicht mehr durch einen Widerruf unterbunden wird.

7.7.1.1.10 Einwilligung für die Zertifikaterneuerung und den Zertifikatsaustausch

Ein Widerruf der CWA-Nutzer hinsichtlich der im Rahmen der Erneuerung oder des Austauschs von Zertifikaten abgegebenen Einwilligung ist nicht möglich und daher auch nicht vorgesehen, da die mit der Erneuerung und dem Austausch verbundene Datenverarbeitung sofort nach Erteilung der Einwilligung durchgeführt wird, das aktualisierte Zertifikat umgehend an die CWA App zurückübermittelt und auf dem Server des RKI unverzüglich wieder gelöscht wird.

7.7.1.2 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- bzw. CHGS-)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 bzw. CHGS 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.

7.7.2 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 7.7.1 entsprechend. Denn auch die Verarbeitung im EFGS und im daraus abgeleiteten CHGS 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 jeweiligen Verantwortlichen verhindert wird.

7.7.3 Rechte von Dritten

Soweit von einem CWA-Nutzer mit der CWA App personenbezogene Daten von Dritten, beispielsweise von Angehörigen, verarbeitet werden, fällt diese Verarbeitung regelmäßig nicht in den Anwendungsbereich des Datenschutzrechts, so dass die gesetzlich geregelten Betroffenenrechte nicht zur Anwendung kommen.

Auf technischer Ebene besteht für den CWA-Nutzer unabhängig von der Anwendbarkeit der Betroffenenrechte die Möglichkeit, die von ihm gespeicherten personenbezogenen Daten Dritter in der CWA App zu löschen.

7.8 Data Protection by Design and by Default

Verantwortliche sind nach Art. 25 DSGVO angehalten, bei der Gestaltung von Verarbeitungsvorgängen von Anfang an technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Datenschutzniveau zu gewährleisten und die den Grundsätzen des Datenschutzes durch Technik (Data Protection by Design) und durch datenschutzfreundliche Voreinstellungen (Data Protection by Default) Genüge tun (Erwägungsgrund 78 DSGVO).

Für die technische Realisierung der CWA und des EFGS bzw. CHGS wurde daher von Anfang an 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 Designmaßnahmen führen zu einem konzeptionsbedingten Datenschutz der CWA.

Eine Übersicht aller Designentscheidungen für die CWA werden in dem Dokument „Designentscheidungen der CWA der Bundesrepublik Deutschland“ (Anlage 1) dargestellt.

7.9 Weitere datenschutzrechtliche Anforderungen

Bei der Entwicklung und Weiterentwicklung der CWA wurde und wird konsequent angestrebt, 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 2020⁹⁰
- Chaos Computer Club (CCC), 10 Prüfsteine für die Beurteilung von „Contact Tracing“-Apps vom 6. April 2020⁹¹
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FlfF), Datenschutz-Folgenabschätzung (DSFA) für eine Corona-App, Version 1.6 vom 29. April 2020⁹²
- eHealth Network, diverse Guidelines und Spezifikationen zu COVID-Zertifikaten⁹³
- Digitalcourage e.V., Einordnung zur geplanten „Corona-Kontakt-Tracing-App“ des RKI, Stand 4. Mai 2020⁹⁴
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FlfF), Analyse und konstruktive Kritik der offiziellen Datenschutzfolgenabschätzung der Corona-Warn-App, Version 1.0 vom 29. Juni 2020⁹⁵

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

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

⁹⁰ 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 11.10.2022).

⁹¹ 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 11.10.2022).

⁹² Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FlfF), 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 11.10.2022).

⁹³ Siehe https://ec.europa.eu/health/ehealth/covid-19_de (zuletzt abgerufen am 11.10.2022).

⁹⁴ 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 11.10.2022).

⁹⁵ Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FlfF), 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 11.10.2022).

8 Bewertung der Notwendigkeit und Verhältnismäßigkeit

Die Verarbeitung von personenbezogenen Daten muss in Anbetracht des jeweils verfolgten Zwecks notwendig und verhältnismäßig sein. Die Notwendigkeit setzt dabei voraus, dass die eingesetzten Daten und sonstigen Mittel für die vollständige und rechtmäßige Erreichung des jeweils verfolgten Zwecks erforderlich sind. Die Verhältnismäßigkeit der Verarbeitung setzt voraus, dass es keine alternativen und datenschutzrechtlich weniger eingreifenden Verarbeitungsformen gibt, um den jeweils verfolgten Zweck mit gleicher Wirksamkeit zu erreichen.

Die Erforderlichkeit der verarbeiteten Daten für bestimmte Funktionen der CWA App wurde überwiegend bereits im Rahmen der Beschreibung des Prüfgegenstands dargelegt, so dass an dieser Stelle auf eine Bewertung der Erforderlichkeit von einzelnen Datenkategorien weitestgehend verzichtet werden kann. Insoweit gelten die nachfolgenden Ausführungen ergänzend zur Darstellung im Abschnitt 5.

8.1 Zweck 1

8.1.1 Legitimer Zweck

Die frühzeitige Information von Einzelpersonen darüber, dass für sie ein erhöhtes Infektionsrisiko besteht, so dass Infektionsketten frühzeitig unterbrochen und das Gesundheitssystem vor einer Überlastung bewahrt werden können, dient dem legitimen Zweck des Schutzes der Gesundheit der Nutzer und der Bevölkerung.

8.1.2 Eignung

Die grundsätzliche Eignung einer ENF-basierten Tracing-App wurde in Labor-Experimenten vom Fraunhofer IIS in Zusammenarbeit mit dem RKI untersucht und bestätigt.

Aufgrund des datensparsamen Konzepts der CWA kann die tatsächliche Effektivität der Risiko-Ermittlungsfunktion nur mittelbar auf Grundlage der vorliegenden Kennzahlen und Nutzungsdaten aus der Datenspende geschätzt werden.

Die bisherigen Evaluationsergebnisse (Stand: März 2022) weisen darauf hin, dass die Risiko-Ermittlung in der Praxis zur Förderung des Zwecks 1 geeignet ist.⁹⁶ Die zuletzt durchgeführte

⁹⁶ CWA-Team, „Wie viele aktive Nutzende hat die Corona-Warn-App?“, Kennzahlen zur Evaluation (Beitrag vom 03.03.2022) abrufbar unter: <https://www.coronawarn.app/de/science/2022-03-03-science-blog-5/> (zuletzt abgerufen am 11.10.2022); CWA-Team, „Über die Wirksamkeit und den Nutzen der Corona-Warn-App“, Ausgangspunkt der Evaluation (Beitrag vom 15.06.2021) abrufbar unter <https://www.coronawarn.app/de/science/2021-06-15-science-blog-1/> (zuletzt abgerufen am 11.10.2022).

Evaluation hat ermittelt, dass die CWA App von ca. 46% der in Frage kommenden Bevölkerung genutzt wird (ca. 1/3 der Gesamtbevölkerung) und ca. 70% der positiv getesteten CWA-Nutzer bereits eine Warnung ausgelöst haben. Dies entsprach zum Evaluationszeitpunkt einem Anteil von 16,8% der positiven Testergebnisse in Deutschland. Die CWA-Nutzer gaben ganz überwiegend an, ihr Verhalten nach Erhalt einer Warnung im Sinne der Empfehlungen des RKI angepasst zu haben. Die Auswertung der Nutzerdaten hat weiter ergeben, dass pro Warnung durchschnittlich 23 andere Nutzer erreicht werden, etwa jeder fünfte CWA-Nutzer, der im Rahmen der Risiko-Ermittlung über einen „roten“ Risikostatus informiert wurde, ist anschließend positiv getestet worden. Bei CWA-Nutzern ohne roten Risikostatus war der Anteil nach den Erkenntnissen aus den Nutzerbefragungen hingegen nur halb so hoch. Daraus lässt sich ableiten, dass die Eignung der Verarbeitungsvorgänge für die Risiko-Ermittlung für Zweck 1 bejaht werden kann. Die Evaluation hat belastbare Erkenntnisse dazu ergeben, dass CWA-Nutzer infolge der Risiko-Ermittlung unmittelbar ihr Verhalten so anpassen, dass Infektionsketten frühzeitig beendet werden können.⁹⁷

Der Austausch von Daten mit für die anderen nationalen Corona-Apps Verantwortlichen über den EFGS und den vergleichbaren CHGS erlaubt die länderübergreifende Risiko-Ermittlung und Warnung. Die Weitergabe der Informationen über die gemeinsame technische Infrastruktur des EFGS bzw. CHGS 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.

Sowohl die Datenspende als auch die Befragungseinladungen dienen dem RKI dazu, für die Bekämpfung der Corona-Pandemie konkret verwertbare Erkenntnisse über das allgemeine, auch regionale Nutzungsverhalten der CWA-Nutzer zu gewinnen. Anhand der gewonnenen Informationen wird das RKI die Wirksamkeit der allgemeinen Nutzung und Nutzerführung der CWA bewerten und auf Basis der gewonnenen Erkenntnisse kurzfristig sowohl inhaltliche Verbesserungen (etwa durch andere inhaltliche/regionale Schwerpunktsetzungen oder anders präsentierte Verhaltensempfehlungen, die den von den CWA-Nutzern tatsächlich gewünschten oder benötigten Informationen besser entsprechen) als auch Verbesserungen hinsichtlich der Bedienbarkeit und Nutzerführung der CWA App (Usability) vornehmen. Anhand der aus der Datenspende und aus Befragungen gewonnenen Erkenntnisse werden typische Hürden, die aus Nutzersicht der Brauchbarkeit der in der CWA App angezeigten Informationen und dem Auslösen von Warnungen im Weg stehen, in kurzer Zeit identifiziert und zielgerichtet abgebaut werden können. Die Datenspende und die Funktion zur Einladung

⁹⁷ Im Rahmen des Evaluationsberichtes des Sachverständigenausschusses nach § 5 Abs. 9 IfSG vom 30.06.2022, dort S. 79 wird der Kontaktpersonennachverfolgung grundsätzlich ein positiver, Infektionsketten durchbrechender Effekt bescheinigt. Die Evidenz der Unterstützung der Nachverfolgung durch digitale Tools kann jedoch anhand der vorhandenen Kennzahlen nicht final bewertet werden; Evaluation der Rechtsgrundlagen und Maßnahmen der Pandemiepolitik – Bericht des Sachverständigenausschusses nach § 5 Abs. 9 IfSG, abrufbar unter: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/S/Sachverstaendigenausschuss/220630_Evaluationsbericht_IFSG_NEU.pdf (zuletzt abgerufen am 11.10.2022).

zu Befragungen leisten damit einen erheblichen Beitrag zur Erreichung des Zwecks 1. Gleichermaßen gilt für die Funktion für Fehlerberichte, die mit Release 2.2 eingeführt wird. Denn anhand der Fehlerberichte gewonnene Erkenntnisse können genutzt werden, Fehler im Ablauf der CWA zu erkennen, deren Ursachen zu analysieren und zu beheben. Technische Fehler der CWA sind ein Grund dafür, dass CWA-Nutzer die CWA App deinstallieren. Berichte über Fehler führen auch dazu, dass Personen, die Bedenken oder Vorbehalte gegen die CWA App hegen und sie daher noch nicht installiert haben, sie auch weiterhin nicht installieren werden. Fehlerberichte können damit zur Verbesserung der App und somit zu einer höheren Akzeptanz der CWA beitragen, wodurch die Erreichung des Zwecks gefördert wird.

8.1.3 Erforderlichkeit

Die Verarbeitungsvorgänge der vorgenannten Funktionen sind 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 anonymen 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, mildereres 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 getester 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 Begegnungshistorie des Kontakt-Tagebuchs ist erforderlich, um die CWA-Nutzer in die Lage zu versetzen, ihr persönliches Umfeld vor einer potenziellen Ansteckung zu warnen und somit Infektionen zu verhindern.⁹⁸ Wird in der Begegnungshistorie bspw. angezeigt, dass an einem Tag in der Vergangenheit ein erhöhtes Risiko bestand, kann der CWA-Nutzer einschätzen, ob er an oder nach diesem Tag noch Personen getroffen hat, die er – im (ungewissen) Falle einer eigenen Ansteckung – ebenfalls einem Infektionsrisiko ausgesetzt hat. Der CWA-Nutzer kann seine persönlichen Kontakte vorsorglich über diesen Umstand informieren. Dies entspricht dem sozialüblichen Verhalten im privaten Bereich und wird durch die frühzeitige, spezifische Information der CWA-Nutzer über die App erleichtert oder gar erst ermöglicht. Eine Infektionskette kann – auch ohne Zutun der Gesundheitsbehörden im Rahmen der Kontaktverfolgung – durch die Selbst-Isolation der CWA-Nutzer erreicht werden. Die aggregierte Darstellung ohne konkrete Wiedergabe des Datums des erhöhten Risikos würde dies nicht ermöglichen.

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 CHGS und die nachfolgenden Verarbeitungen durch die Verantwortlichen der daran jeweils 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 Funktionen zur Teilnahme an der Datenspende sowie zur Einladung an Befragungen sind erforderlich, um detaillierte und zuverlässige Erkenntnisse über das allgemeine Nutzungsverhalten sowie die Bedürfnisse der CWA-Nutzer zu gewinnen. Der Einsatz von anderen in Betracht kommende Verfahren (z. B. analoge Befragungen, Face-to-Face-Interviews, reine Web-Befragungen) würde nicht nur erhebliche Hürden für die Kooperationsbereitschaft der CWA-Nutzer schaffen und einen erheblichen zeitlichen Mehraufwand bedeuten, sondern auch zu unzuverlässigeren Informationen (insbesondere zum Nutzungsverhalten) sowie zu einer deutlich kleineren Datenbasis führen, die weniger aussagekräftig ist. Die Möglichkeit zur freiwilligen Bereitstellung von Fehlerberichten durch Anwender, um dem Entwickler bei der Verbesserung seiner Software zu helfen, ist eine übliche Vorgehensweise zur Verbesserung von Software. Zwar wäre eine automatische Übersendung von Fehlerberichten zur Erreichung dieses Zwecks effektiver, ohne die (zu dokumentierende) Einwilligung des CWA-Nutzers jedoch unzulässig. Daher ist die Umsetzung in der CWA App, bei denen die Fehlerberichte ausdrücklich aktiviert und erst in einem weiteren Schritt nach

⁹⁸ Die grundsätzliche Bedeutung der schnellstmöglichen Benachrichtigung von engen Kontaktpersonen im privaten Umfeld durch die infizierte Person selbst wird im Rahmen des Evaluationsberichtes des Sachverständigenausschusses nach § 5 Abs. 9 IfSG vom 30.06.2022 (aaO), dort S. 79 betont. Das Kontakt-Tagebuch kann die Benachrichtigung effizient unterstützen.

einer Echtheitsprüfung optional (im Sinne einer Datenspende) an das RKI gesendet werden können das mildeste Mittel für das RKI, um an zuverlässige Fehlerberichte zu gelangen.

Die Echtheitsprüfung unter Verwendung der Drittdienste Apple DeviceCheck und Google SafetyNet ist als risikoreduzierende Maßnahme erforderlich. Sie dient dazu, zu verhindern, dass die Ergebnisse der Auswertung der im Rahmen der Datenspende oder bei den Befragungen durch das RKI erhobenen Daten durch massenhaft durch Dritte übermittelte Daten (z.B. im Rahmen konzertierter Angriffe) beeinträchtigt werden. Aufgrund des frei zugänglichen Quellcodes der CWA App wäre es grundsätzlich möglich an der Datenspende und den situativen Befragungen des RKI auch ohne jede Nutzung der CWA App teilzunehmen. Die Echtheitsprüfung dient somit als risikoreduzierende Maßnahme, indem der jeweilige Hersteller bestätigt, dass die CWA App, von der die Daten im Rahmen der Datenspende gesendet werden oder die verwendet wird, wenn ein CWA-Nutzer einer Befragungseinladung folgt, in einer nicht-manipulierten Umgebung ausgeführt wird. Ein beliebiges und skalierbares Verfälschen der Daten wird durch den Einsatz der Echtheitsprüfung daher erheblich erschwert, ggf. sogar unterbunden. Ohne die Echtheitsprüfung wäre es indes ohne größere technische Hürden möglich, „unechte“ Daten in die Datenspende bzw. in Befragungen einfließen zu lassen und somit die Datenqualität erheblich zu beeinträchtigen. Es ist davon auszugehen, dass sämtliche im Rahmen der Datenspende und im Rahmen von Befragungen übermittelte Daten dann fachlich nicht mehr nutzbar wären (insoweit wird darauf hingewiesen, dass offene Endpunkte, wie z.B. frei verfügbare URLs zu Befragungen des RKI bereits in der Vergangenheit durch Unbekannte ausgenutzt wurden und Befragungsergebnisse dadurch erheblich verfälscht wurden und die Befragungen schließlich ergebnislos abgebrochen werden mussten.). Ein alternativer und ebenso zuverlässiger Dienst zur Echtheitsprüfung, der auf sämtlichen von der CWA App unterstützten Betriebssystemen zur Verfügung steht, existiert nicht.

Die Erweiterung der Risiko-Ermittlung in Form der Event-Registrierung folgt ebenfalls dem dezentralen Ansatz. Eine weitere Datenminimierung ist nicht möglich, ohne die Eignung der Check-in-basierten Warnungen für die Risiko-Ermittlung zu beseitigen. Insbesondere Verfahren zur Warnung auf Basis eines – potenziell datensparsamen – rein technischen und lokal umsetzbaren Verfahrens sind derzeit nicht ersichtlich. Auch technische Luftmessungen anhand der Sensoren eines Smartphones kommen nicht in Betracht. Eine Warnung der CWA-Nutzer in Zusammenhang mit Begegnungen in Innenräumen ist daher gegenwärtig nur auf Basis der im Rahmen der Risiko-Ermittlung beschriebenen Verarbeitungen möglich.

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 dazu, dass Nutzer schnell vor möglichen Ansteckungsrisiken gewarnt werden können. Gewarnte 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 dem mit der Risiko-Ermittlung verfolgten Zweck würde es daher sprechen, wenn die CWA gegenüber der durch die Gesundheitsämter durchgeführten Ermittlung und Kontaktierung von Kontaktpersonen keinerlei Vorteil bringt. Davon ist jedoch nicht auszugehen. Die Evaluation hat ergeben, dass der Anteil der nach Mitteilung eines hohen Risikostatus positiv getesteten CWA-Nutzer deutlich höher ist als bei anderen CWA-Nutzern. Zu diesem Zeitpunkt gab es in der Regel noch keinen Kontakt zum Gesundheitsamt. Allerdings soll die CWA gerade keinen Ersatz, sondern eine Ergänzung der übrigen staatlichen Maßnahmen wie etwa der Kontaktnachverfolgung durch die zuständigen Gesundheitsämter sein.

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 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 Abschnitt 7.8). 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 wurde und wird niemand von staatlichen Stellen dazu gezwungen werden, die CWA App zu nutzen. Es steht jedem frei, 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.

Auch die Teilnahme an der Event-Registrierung ist freiwillig. Der CWA-Nutzer kontrolliert selbst, bei welchen Events oder Orten er sich eincheckt. Zudem kann er Events- und Orte, bei denen er eingecheckt ist, löschen und so verhindern, dass er Warnungen von anderen Nutzern, die am selben Ort eingecheckt waren, erhält oder diese Nutzer gewarnt werden, wenn er eine Warnung auslöst. Es ist zwar denkbar, dass Organisatoren auf die Nutzung der Event-Registrierung bestehen. Eine weitergehende Verarbeitung im Rahmen der Risiko-Ermittlung und der Warnung anderer ist damit jedoch nicht unbedingt verbunden, da der Nutzer die volle Kontrolle über die eingecheckten Orte und Events behält.

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 natürlich 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 geringen Risikostatus 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 App zu einem faktischen Zwang durch sozialen Druck umwandeln. Rückblickend kann jedoch festgestellt werden, dass ein faktischer Nutzungszwang nicht eingetreten ist. Darauf weisen die Evaluationsergebnisse hin. Zwar wurde und wird die CWA App von einem großen Teil der Bevölkerung genutzt. Zu keinem Zeitpunkt hat jedoch eine Mehrheit der Bevölkerung die CWA App bzw. die Risiko-Ermittlung genutzt. Auch standen der Bevölkerung stets alternative Mitteln zu den Funktionen der CWA App zur Verfügung und wurden auch breit genutzt.

Auch die Verarbeitungsvorgänge im EFGS und CHGS und die nachfolgenden Verarbeitungen durch die Verantwortlichen der daran jeweils angeschlossenen nationalen Corona-Apps sind vor diesem Hintergrund als angemessen zu bewerten. 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 des EFGS wird entsprechend die Freiwilligkeit der Nutzung durch die gemeinsam verantwortlichen, am EFGS 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 EFGS 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. Das Fehlen einer Wahlmöglichkeit in Bezug auf die Datenübermittlung an den CHGS ist entsprechend der oben genannten Erwägungen ebenfalls angemessen. Es wäre sachlich nicht begründbar, weshalb die Nutzer der Schweizer Corona-App von einer Warnung durch CWA-Nutzer ausgeschlossen werden. Dies würde die Effektivität der Interoperabilität wegen der naturgemäß grenzüberschreitenden Übertragung des Coronavirus insbesondere in Grenzregionen entscheidend beeinträchtigen.

Hinsichtlich der Echtheitsprüfung unter Verwendung der Drittdienste Apple DeviceCheck und Google SafetyNet ist damit zu rechnen, dass Daten des CWA-Nutzers von den Drittanbietern auch in Drittländern (insbesondere USA) verarbeitet werden. Dies könnte gegen die Angemessenheit der Echtheitsprüfung sprechen, wenn sie ohne Zutun des CWA-Nutzers durchgeführt würde. Vorliegend wird die Echtheitsprüfung jedoch nur nach einer entsprechenden Einwilligung des CWA-Nutzers durchgeführt. Vor Erteilung der Einwilligung wird der Nutzer explizit über die Datenschutzrisiken der Drittlandübermittlung informiert. An der Freiwilligkeit der Einwilligung bestehen keine Bedenken. Die Einwilligung dient nicht den „Hauptzwecken“ bzw. Basisfunktionen der CWA, sondern ist nur im Rahmen der Nutzung von optionalen „Zusatzfunktion“ erforderlich. Weder ist zu erwarten, dass bezüglich der Nutzung dieser Funktionen ein öffentlicher Druck besteht, noch erwachsen dem CWA-Nutzer aus der Verwendung dieser Funktionen persönliche Vorteile oder aus der Verweigerung Nachteile oder ein geringerer „Schutz“ durch die CWA App. Insbesondere ist die zusätzliche Einwilligung nicht erforderlich, um die Basisfunktionen der CWA App verwenden zu können.

8.2 Zweck 2

8.2.1 Legitimer Zweck

Bezweckt wird die zeitnahe Benachrichtigung der CWA-Nutzer über ihr (positives) Testergebnis sowie die frühzeitige Warnung anderer Nutzer. Damit wird der legitime Zweck

des Schutzes der Gesundheit der Nutzer sowie die frühzeitige Unterbrechung von Infektionsketten verfolgt.

8.2.2 Eignung

Die vorliegenden Evaluationsergebnisse belegen eindeutig, dass die Verarbeitungsvorgänge für den Testabruf und die Warnfunktionen die zeitnahe Mitteilung von Testergebnissen an **Testpersonen** und die zeitnahe Warnung anderer Nutzer ermöglicht haben, so dass sie zur frühzeitigen Unterbrechung von Infektionsketten geeignet ist.

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 von Testergebnissen nur an den betreffenden berechtigten CWA-Nutzer geeignet ist.

Es wird weiter angenommen, dass die mit Version 1.9 der CWA App vorverlegte Einwilligungseinholung für die Warnung anderer Nutzer bereits auf den Zeitpunkt der Testregistrierung die Wahrscheinlichkeit dafür, dass nach dem Abruf eines positiven Testergebnisses eine Warnung ausgelöst wird, spürbar erhöht hat, so dass das geänderte Einwilligungsverfahren gegenwärtig weiterhin als geeignet zur frühzeitigen Unterbrechung von Infektionsketten angesehen werden darf.

Es wird davon ausgegangen, dass die mit Version 1.13 der CWA App eingeführte Datenspende und die Möglichkeit zur Einladung zu Befragungen dem RKI Erkenntnisse über das Nutzungsverhalten und die Bedürfnisse der CWA-Nutzer ermöglicht, die zur Verbesserung der CWA App und somit zur weiteren Steigerung der Warnbereitschaft führen werden. Entsprechendes gilt für die mit Version 2.2 eingeführte Fehlerberichtsfunktion, da auch diese zur Verbesserung der CWA App führen wird.

Die Effektivität der Verarbeitung des Namens, der Telefonnummer sowie der Antworten auf die Plausibilitätsfragen ist im Hinblick auf den Zweck der Verringerung der Gefahr des Missbrauchs im Rahmen der Nutzung der Verifikations-Hotline begrenzt. 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 Angreifern mit Social Engineering-Techniken 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.

8.2.3 Erforderlichkeit

Mit Hilfe der CWA App können Personen, die CWA-Nutzer sind, deutlich schneller über ihr Testergebnis 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 den Testabruf über die CWA App zur schnellen Bekanntgabe des Testergebnisses an den CWA-Nutzer 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 Testergebnisabruf 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 Testabrufs durch die tatsächliche Testperson dar. Ein vollständiger anonymer Testergebnisabruf 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 getesteter Person auf das minimal erforderliche Maß reduziert und ein Missbrauch oder falsche Bekanntgabe von Testergebnissen deutlich unwahrscheinlicher.

Die Umsetzung der Warnfunktion für das Teilen eines (positiven) Testergebnisses ermöglicht die kurzfristige niedrigschwellige Warnung anderer Nutzer vor einer möglichen Ansteckung bei einem positiv getesteten CWA-Nutzer. Da anzunehmen ist, dass eine gesonderte Einwilligungseinhaltung für das Teilen eines positiven Testergebnisses nach dessen Erhalt einen erheblichen Teil der positiv getesteten CWA-Nutzer vom Auslösen einer Warnung abhält, weil sich diese unmittelbar nach der Mitteilung der Diagnose in einer emotionalen Ausnahmesituation befinden, ist die frühzeitige Einwilligungseinhaltung für die Warnfunktion im Zusammenhang mit dem Testabruf erforderlich, um eine hohe und insofern effektive Warnquote zu ermöglichen und den Zweck der frühzeitigen Unterbrechung von Infektionsketten erreichen zu können.

Die Erforderlichkeit der Verarbeitungstätigkeit der Verifikations-Hotline wird im Ergebnis ebenfalls bejaht. Eine zunächst angedachte Alternative zur Verifikations-Hotline war es, 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 wären Angriffe auch mit diesem Verfahren nicht vollkommen ausgeschlossen, etwa durch sog. Call ID Spoofing (also das Anzeigen einer falschen Telefonnummer). Die Missbrauchsmöglichkeit erscheint jedoch wesentlich aufwendiger und kann durch entsprechende Gegenmaßnahmen seitens der Verifikations-Hotline, etwa dem Einsatz entsprechender Endgeräte, effektiv verhindert werden. Dieses alternative Verfahren wäre allerdings mit einem erheblichen technischen und insbesondere organisatorischen Aufwand insbesondere auf Seiten der Ärzteschaft verbunden gewesen (insbesondere bei steigenden Inzidenzwerten), weshalb seine Akzeptanz bzw. Eignung als gering bewertet und es nicht weiter verfolgt wurde. Rückblickend lässt sich feststellen, dass die bei Einführung des Hotline-Verfahrens nicht vorhersehbare Dauer und Verbreitung der Corona-Pandemie sowie die unvorhersehbaren Schwierigkeiten bei der Anbindung der Labore bei Wahl des alternativen Verfahrens zu nicht tragbaren Mehrbelastungen der Ärzte geführt hätten. Somit wird die Erforderlichkeit der Verarbeitungstätigkeit der Verifikations-Hotline weiterhin bejaht.

Zur Erforderlichkeit der Verarbeitungstätigkeit im Zusammenhang mit den Funktionen für die Datenspende, die Einladung zu Befragungen sowie Fehlerberichtsfunktion siehe unter Abschnitt 8.1.3.

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 und dem Teilen des Testergebnisses und die dadurch wegen der Zeitkritikalität des Zwecks entstehende Chance zur früheren Unterbrechung von Infektionsketten ist die Verarbeitung für den Testergebnisabruf und die Warnfunktion angemessen.

Zur Angemessenheit der Verarbeitungstätigkeit im Zusammenhang mit den Funktionen für die Datenspende, die Einladung zu Befragungen sowie die Fehlerberichtsfunktion siehe entsprechend unter Abschnitt 8.1.4.

8.3 Zweck 3

8.3.1 Legitimer Zweck

Die Datenverarbeitung für die Anzeige von Statistiken auf der Statistik-Kachel auf dem Home-Screen der CWA App bezweckt die Information der CWA-Nutzer über Neuinfektions- und Impfzahlen sowie Kennzahlen zur CWA, die von allgemeinem Interesse sind. Die Datenverarbeitung dient damit dem legitimen Zweck der Information der Öffentlichkeit durch das RKI über das aktuelle Infektionsgeschehen sowie die Verbreitung und Nutzung der CWA App.

8.3.2 Eignung

Die Datenverarbeitung ermöglicht dem RKI die Bereitstellung von aktuellen Statistiken und Kennzahlen aus seinem eigenen Geschäftsbereich und ist geeignet, um CWA-Nutzern aktuelle und zuverlässige Informationen im Zusammenhang mit dem Pandemiegeschehen über einen zeitgemäßen und etablierten Kommunikationskanal und somit niedrigschwellig zur Verfügung zu stellen.

8.3.3 Erforderlichkeit

Für die Anzeige der aktuellen Statistiken werden lediglich diejenigen Zugriffsdaten verarbeitet, auf die für das Laden der aktuellen Coronastatistik-Daten aus technischen Gründen nicht verzichtet werden kann. Eine Speicherung der Zugriffsdaten über den konkrete Abrufvorgang hinaus erfolgt nicht. Da die Coronastatistik-Daten ebenso wie die Positivschlüssel-Pakete vom CDN-Magenta heruntergeladen werden, fallen die Zugriffsdaten in der Regel ohnehin, also unabhängig von der Funktion der Statistik-Kachel an. Das Herunterladen der vom CWA-Nutzer eingestellten lokalen Statistiken erfolgt maximal auf Bundeslandebene, so dass dem RKI keine genauere Identifikation der vom CWA-Nutzer ausgewählten Landkreise oder Bezirke möglich ist. Ein mildereres Mittel zur niedrigschwälligen Information der CWA-Nutzer, welches mit einer spürbar geringeren Datenerhebung oder -verarbeitung verbunden wäre, steht daher nicht zur Verfügung. Somit kann die Erforderlichkeit bejaht werden.

8.3.4 Angemessenheit

Die Datenverarbeitung ist zur Erreichung des Informationszwecks auch angemessen. Da der Abruf der Coronastatistik-Daten für die Statistik-Kachel lediglich den Zweck der für die Risiko-Ermittlung ohnehin stattfindenden Verarbeitung von Zugriffsdaten erweitert, werden die Interessen der CWA-Nutzer an der Vermeidung von unnötigen Verarbeitungen der sie betreffenden personenbezogenen Daten nicht spürbar beeinträchtigt. Insbesondere ist nicht ersichtlich, dass die Datenverarbeitung zu dem verfolgten Informationszweck zu zusätzlichen, weitergehenden oder intensiveren Datenschutzrisiken für die CWA-Nutzer führen kann, die bei Verzicht auf den Abruf der Coronastatistik-Daten nicht eintreten würden. Demgegenüber steht das legitime Interesse des RKI an der Information der Öffentlichkeit und insbesondere der CWA-Nutzer über das aktuelle Infektionsgeschehen und die Verbreitung der CWA App. Durch die Anzeige von wichtigen Statistiken und Kennzahlen auf dem Home-Screen CWA App kann das RKI auch solche Personen erreichen und kontinuierlich mit zuverlässigen Informationen versorgen, die über die herkömmlichen Kommunikationskanäle des RKI oder die Presseberichterstattung nicht erreicht werden können. Die Anzeige der Statistiken kann auch den Mehrwert der CWA App für einen Teil der CWA-Nutzer erhöhen und somit einen zusätzlichen Anreiz zur regelmäßigen aktiven Verwendung der CWA App schaffen. Zudem ist zu erwarten, dass die Darstellung von aktuellen Kennzahlen zur Verbreitung der CWA App beiträgt und die Anzahl der über sie ausgelösten Warnungen erhöht und somit schließlich zur Wirksamkeit der CWA App beiträgt. Vor diesem Hintergrund ist die Verarbeitung der Zugriffsdaten durch den CDN-Magenta für die Bereitstellung der Statistik-Kachel angemessen.

8.4 Zweck 4

8.4.1 Legitimer Zweck

Mit dem Nachweis von COVID-Zertifikaten soll es Personen, die von Erleichterungen und Ausnahmen erfasst sind, erleichtert werden, diese in Anspruch zu nehmen und insoweit von ihren Grundrechten und Grundfreiheiten wieder möglichst umfassend Gebrauch zu machen. Dies stellt einen legitimen Zweck dar.

8.4.2 Eignung

Die Verarbeitungsvorgänge für die Wallet-Funktionen und die Funktionen zum Nachweis von negativen Testergebnissen der CWA App sind für die Erreichung des Zwecks 4 geeignet.

Sie ermöglichen dem CWA-Nutzer einen anerkannten Nachweis dafür, dass er ein negatives Testergebnis erhalten hat. In Verbindung mit einem Identitätsnachweis (z. B. Ausweis) kann der CWA-Nutzer mit hinreichender Sicherheit nachweisen, dass er nicht ansteckend ist. Der im Schnelltest-Nachweis angegebene Testzeitpunkt erlaubt es Dritten zu erfassen, wann der Schnelltest vorgenommen wurde. Es kann zwar vorgebracht werden, dass der Schnelltest-

Nachweis möglicherweise nicht alle in den Verordnungen der Bundesländer aufgestellten Anforderungen erfüllt. Sollte dies nicht der Fall sein, so steht es dem CWA-Nutzer jedoch frei, andere Nachweisformen, zum Beispiel in Papierform, zu verwenden, um diesen bundeslandspezifischen Maßgaben gerecht zu werden. Im Sinne der Datensparsamkeit ist der in der CWA App angezeigte Datensatz als ausreichend anzusehen, um ein negatives Schnelltest-Ergebnis zu belegen. Die Prüfung der Gültigkeit der Zertifikate ermöglicht den Nutzern einzuschätzen, ob Ihre Zertifikate den geltenden Business Rules entsprechen und somit als gültig akzeptiert werden.

Die Funktionen der Zertifikatswallet zur elektronischen Verwendung von COVID-Zertifikaten sowie die Gültigkeitsprüfung der COVID-Zertifikate sind zur Förderung des Zwecks ebenfalls geeignet, denn sie erleichtern Geimpften, Genesenen und negativ Getesteten die Inanspruchnahme von Erleichterungen und Ausnahmen von Schutzmaßnahmen. Ein großer Teil der Bevölkerung besitzt ein Smartphone und führt dieses ständig mit sich. Die Walletfunktionen für COVID-Zertifikate machen das Mitführen und Vorzeigen des (gelben) Impfausweises oder einer Impf-, Test- oder Genesenenbescheinigung im Papierformat überflüssig und beschränken die zu offenbarenden Daten auf den erforderlichen Mindestdatensatz. Durch die Möglichkeit des Scannens des COVID-Zertifikats (QR-Code) per App können Ladengeschäfte und Dienstleister die Prüfung des Impf-/Genesenen-/Teststatus deutlich vereinfachen und beschleunigen, ohne dass weitere personenbezogene Daten der betroffenen Person (z. B. der Status anderer Schutzimpfungen) offenbart werden. Die praktische Erleichterung des Nachweises stellt somit sicher, dass die ungehinderte Ausübung der Grundrechte und Grundfreiheiten möglichst umfassend sichergestellt ist. Die Prüfung der technischen und fachlichen Gültigkeit der COVID-Zertifikate ermöglicht den CWA-Nutzern selbst zu beurteilen, ob Ihre COVID-Zertifikate verwendbar sind und den geltenden Business Rules entsprechen und sie somit geeignet sind, die erforderlichen Nachweise zu erbringen oder ob andere COVID-Zertifikate oder Nachweise erforderlich sind. Solange die Pandemielage die Aufrechterhaltung der Schutzmaßnahmen und somit Kontrollen des Impf-/Genesenen oder Teststatus erfordert, wird somit möglichst umfassend verhindert, dass ein nicht mitgeführtes Dokument die Teilhabe am öffentlichen Leben verhindert. Durch die nachträglich eingeführte Funktion für die Online-Validierung wird die Möglichkeit eröffnet, die vorgenannten Vorteile der COVID-Zertifikate auch im Online-Bereich zu nutzen und zugleich die große Nachfrage der Bürgerinnen und Bürger nach einer Lösung für den sicheren und einfachen Zertifikatsnachweis im Rahmen von alltäglichen Online-Buchungsprozessen zu befriedigen. Zugleich wird dadurch der Entstehung von weniger datensparsamen und mitunter datenschutzrechtlich kritischen Parallelangeboten für den Online-Nachweis von Zertifikaten vorgebeugt.

8.4.3 Erforderlichkeit

Die im Schnelltest-Nachweis angezeigten Daten sind auf das geringstmögliche Maß begrenzt. Die Anzeige von Vor-, Nachname und Geburtsdatum sowie des Testzeitpunkts ist erforderlich, um einem Dritten die Prüfung zu ermöglichen, ob der CWA-Nutzer vor kurzer Zeit einen Schnelltest hat durchführen lassen und insoweit ein negatives Ergebnis vorliegt. Der Schnelltest-Nachweis kommt zudem ohne eine zusätzliche Übermittlung von

personenbezogenen Daten an die CWA Server aus. Mildere Mittel sind insoweit nicht ersichtlich. Weder könnte auf im Zuge des Schnelltest-Nachweises angezeigte Daten verzichtet werden, ohne die Erreichung des Zwecks zu verhindern, noch sind datensparsamere Übertragungswege denkbar. Die Schnelltest-Nachweise werden nach Ablauf von 48 Stunden seit Testdurchführung automatisch ungültig, da ein Schnelltest-Ergebnis ab diesem Zeitpunkt nach epidemiologischen Erkenntnissen keine verlässliche Aussage mehr über die Infektionsfreiheit einer Person trifft. Auch in Zusammenhang mit der Prüfung der Gültigkeit der Zertifikate ist die Datenverarbeitung auf das geringstmögliche Maß begrenzt. Es werden immer die Regelwerke sämtlicher Mitgliedsländer heruntergeladen, sodass ein Rückschluss auf mögliche Reiseroute des CWA-Nutzers ausgeschlossen ist. Die Prüfung der Zertifikate gegen die Business Rules des ausgewählten Mitgliedslandes findet lokal auf dem Endgerät des Nutzers statt.

Die Verarbeitungsvorgänge der Wallet-Funktionen für COVID-Zertifikate sind für die Erfüllung des in Rede stehenden Zwecks ebenfalls erforderlich. Gleich geeignete mildere Mittel sind nicht ersichtlich. Es wird eine konzeptionsbedingt datensparsame Systemarchitektur eingesetzt. Die Verarbeitung ist auf die Ermöglichung der elektronischen Bestätigung, Überprüfung sowie Gültigkeitsprüfung der COVID-Zertifikate unter Verwendung eines QR-Codes beschränkt. Bei Bedarf steht auch die Detailansicht zu einem COVID-Zertifikat zur Verfügung. Eine dauerhafte Verarbeitung der Daten auf einem zentralen Server erfolgt jedoch nicht, so dass die Datenverarbeitung mit Blick auf den verfolgten Zweck minimal ist. Es wird auch keine zentrale Datenverwaltung eingeführt. Die verwendeten Datenfelder werden durch die Interoperabilitätsrichtlinien des eHealth-Netzwerks vorgegeben und sind erforderlich, um die Interoperabilität zu ermöglichen. Durch die Verwendung der eindeutigen Zertifikatskennung 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 eindeutige Zuordenbarkeit der COVID-Zertifikate verhindern und dadurch das Ziel der Sicherstellung der Authentizität ausgestellter COVID-Zertifikate vereiteln. Sie kann daher kein gleich geeignetes, mildereres Mittel darstellen.

Durch die Schaffung einer Funktion zur Nutzung der Online-Validierungsmöglichkeit bei Leistungsanbietern wird die Verwendung der COVID-Zertifikate auch bei alltäglichen Online-Buchungen ermöglicht. Die Möglichkeit ein COVID-Zertifikat schon vor Eintritt in eine Präsenzsituation zu prüfen (z.B. im Rahmen eines Check-Ins), kann sicherstellen, dass Bürgerinnen und Bürgern mit ungültigen oder zum Einlass nicht ausreichenden Zertifikaten frühzeitig Kenntnis von diesem Umstand erhalten und sich daher nicht erst dem Kontakt zu anderen wartenden Personen am Einlass aussetzen. Die zeitnahe Prüfung vor dem Einlass kann überdies dazu beitragen, die Bürgerinnen und Bürger frühzeitig für das Erfordernis eines gültigen Zertifikats zu sensibilisieren. Dies kann insbesondere bei sich akut ändernde Einlassbedingungen aufgrund aktualisierter Vorgaben der Corona-Schutzverordnungen oder anderer relevanter Gesetze von Vorteil sein.

Die Datenverarbeitung im Rahmen der Online-Validierung orientiert sich dabei eng an den Vorschlägen des eHealth-Netzwerks und gewährleistet, dass der Personenbezug bei der Verarbeitung auf ein Minimum reduziert wird. Insbesondere wird dadurch ein Personenbezug

für das RKI ausgeschlossen. Dass ein Personenbezug für die Leistungsanbieter besteht, liegt hingegen in der Natur der Sache und ist daher erforderlich. Durch die Einbeziehung eines vom Leistungsanbieter unterschiedlichen Prüfpartners wird allerdings gewährleistet, dass der Leistungsanbieter nur die tatsächlich zur Erfüllung seiner Prüfungs-/Dokumentationspflichten erforderlichen Daten, nämlich das reine Validierungsergebnis erfährt und eine Erhebung von Zertifikatsaussagen, die mit weiteren Daten des Leistungsanbieters über den CWA-Nutzer als seinen Kunden verknüpft werden könnten, ausgeschlossen wird.

8.4.4 Angemessenheit

Die Verarbeitung der Daten im Rahmen des Schnelltest-Nachweises ist auch angemessen. Durch die automatisierte und dezentrale Bereitstellung von Vor-, Nachname und Geburtsdatum in der CWA App mittels QR-Code/Link wird die Datenverarbeitung auf das für eine zuverlässige Zuordnung des Testergebnisses zum CWA-Nutzer minimal erforderliche Maß reduziert. Das RKI erhält zu keinem Zeitpunkt Zugriff auf diese Daten. Zwar besteht das Risiko des Missbrauchs, indem der Nachweis von Schnelltest-Ergebnissen auch für den Zugang zu Einrichtungen gefordert wird, die dies auf Grundlage des Gesetzes nicht verlangen dürfen. Dieses Risiko besteht jedoch zum einen außerhalb der CWA, denn der Schnelltest-Nachweis kann auch mit anderen Mitteln erbracht werden. Zum anderen wird der CWA-Nutzer in der CWA App an verschiedenen Stellen deutlich darauf hingewiesen, dass von ihm nur in den gesetzlich vorgesehenen Fällen die Vorlage eines entsprechenden Schnelltest-Nachweises verlangt werden kann. Er wird auch darauf hingewiesen, dass hierfür nicht die CWA App genutzt werden muss. Insoweit bleibt auch die Entscheidungsfreiheit darüber, ob personenbezogene Daten verarbeitet werden, gewahrt, da die Nutzung des Testergebnisabrufs und des Schnelltest-Nachweises freiwillig ist. Der Schnelltest-Nachweis steht im Einklang mit der Zielsetzung der nationalen Teststrategie und fördert deren Zweck. Vor diesem Hintergrund besteht die Chance, dass durch schnell und sicher verfügbare Schnelltest-Nachweise das Infektionsrisiko für den CWA-Nutzer beim Besuch von öffentlichen Einrichtungen reduziert wird und er von seinen verfassungsrechtlich gewährten Freiheiten wieder Gebrauch machen kann. Im Ergebnis ist der Schnelltest-Nachweis daher angemessen.

Im Ergebnis gilt dies auch für die Walletfunktionen zur elektronischen Nutzung von COVID-Zertifikaten. Es soll und wird niemand von staatlichen Stellen dazu verpflichtet werden, den digitalen Impf-/Genesen-/Testnachweis in elektronischer Form mit einer bestimmten App zu nutzen.⁹⁹ Es steht jedem frei, die Nutzung eines COVID-Zertifikats mit einer App abzulehnen und das COVID-Zertifikat in der Papierversion zu nutzen. Zudem ist die Dauer der Verarbeitungsvorgänge zeitlich beschränkt. Dies gilt auch für die Prüfung der Gültigkeit der COVID-Zertifikate. An der Freiwilligkeit der Nutzung der Funktionen der CWA App für die

⁹⁹ Dies schließt eine gesetzliche Pflicht zur Nutzung von COVID-Zertifikaten in bestimmten Situationen nicht grundsätzlich aus. Auch im Fall einer gesetzlichen Nutzungspflicht kann der Zertifikatsinhaber aber auf die elektronische Nutzung der COVID-Zertifikate mit der CWA App (oder einer anderen Wallet-App) verzichten und das COVID-Zertifikat in der Papierversion nutzen, denn die DCC-VO differenziert nicht zwischen der elektronischen und der Papierversion eines COVID-Zertifikats. Vgl. so auch Erwägungsgrund 20 der DCC-VO („Die Ausstellung von Zertifikaten gemäß dieser Verordnung sollte nicht zu Diskriminierung aufgrund des Besitzes einer bestimmten Art von Zertifikat führen.“).

elektronische Verwendung von COVID-Zertifikaten bestehen keine Bedenken. Die Integration der COVID-Zertifikatsfunktionen und die Prüfung der Gültigkeit der COVID-Zertifikate im Rahmen der CWA ermöglicht auch keine Profilerstellung oder Bewegungsverfolgung und führt auch keinen zentralverwalteten Datenbestand im Sinne einer zentralen Impf-/Genesenens-/Testdatenbank ein. Eine Verarbeitung der erhobenen Daten zu einem anderen Zweck ist gemäß der DCC-VO verboten. Somit ist die Verarbeitung im Rahmen der CWA im Hinblick auf Zweck, Umfang und Dauer eng beschränkt. Auch die Angemessenheit der Verarbeitung im Rahmen der CWA ist damit gewahrt.

Angesichts des hohen Bedarfs unter Zertifikatsinhabern nach einer sicheren Nachweismöglichkeit der COVID-Zertifikate auch im Rahmen von Online-Buchungen wird auch die Funktion zur Nutzung der CWA App für die Online-Validierung bei Dritten als angemessen beurteilt. Die Nutzbarmachung der Vorteile der COVID-Zertifikate bei Onlinebuchungen trägt der großen Relevanz von Onlinegeschäften im Alltag vieler Zertifikatsinhaber Rechnung und ist daher konsequent. Zwar birgt eine Übermittlung an vom RKI nicht kontrollier- und steuerbare eigenverantwortliche Dritte (Leistungsanbieter, Validierungsdienste) zusätzliche Risiken durch die Ermöglichung einer missbräuchlichen, intransparenten oder unsicheren Verarbeitung in deren Verantwortungsbereich. Dieses Risiko besteht allerdings auch bei der Verwendung der CWA App bzw. von COVID-Zertifikaten im Papierformat in Präsenzsituationen sowie bei der Verwendung von anderen Prüfsystemen Dritter für den Online-Bereich, die vom RKI weder untersagt noch kontrolliert werden können. Durch das Angebot einer Funktion für die Teilnahme an Online-Validierungsverfahren durch das RKI im Rahmen seiner Wallet-Apps kann daher ein bestehender und nachvollziehbarer Bedarf befriedigt und die Wahrscheinlichkeit eines Ausweichens auf potenziell weniger datensparsame oder problematische Drittangebote zu diesem Zweck reduziert werden.

8.5 Zweck 5

8.5.1 Legitimer Zweck

Die Unterstützung der Bürgerinnen und Bürger bei der Durchführung von präventiven Corona-Tests (Bürgertestungen gemäß § 4a TestV) dient dem legitimen Zweck des Schutzes der öffentlichen Gesundheit durch die frühzeitige Unterbrechung von Infektionsketten verfolgt.

8.5.2 Eignung

Mit der Funktion des Schnelltest-Profil werden die praktischen Hürden für die Inanspruchnahme von Corona-Tests im Sinne der Corona-Testverordnung (TestV) für CWA-Nutzer reduziert.

Der CWA-Nutzer muss vor jedem Schnelltest gegenüber der Teststelle die im Schnelltest-Profil enthaltenen Angaben (erneut) mitteilen, da die Teststelle diese Angaben zur Prüfung der Anspruchsberechtigung des CWA-Nutzers auf die Testung sowie zur Mitteilung des

Schnelltest-Ergebnisses und ggf. zur Ausstellung eines Schnelltest-Nachweises benötigt. Mit Hilfe des QR-Codes, der das Schnelltest-Profil enthält, kann die Erhebung der Daten durch die Teststelle vereinfacht und beschleunigt werden, da das Vorzeigen des QR-Codes gegenüber der Teststelle für den CWA-Nutzer mit weniger Zeit und Mühe verbunden ist als eine (wiederholte) mündliche oder schriftliche Bereitstellung seiner Daten. Dadurch wird der „bürokratische Aufwand“ für die Schnelltest-Durchführung und in der Folge auch die durchschnittliche Aufenthaltsdauer an der Teststelle reduziert, so dass die Schnelltestungen leichter in den Alltag integriert werden können. Folglich stellt das Schnelltest-Profil ein geeignetes Mittel dar, um die Niedrigschwelligkeit der Schnelltest-Angebote zu fördern.

8.5.3 Erforderlichkeit

Das Schnelltest-Profil wird ausschließlich im Speicher der CWA App, also lokal auf dem Smartphone des CWA-Nutzers gespeichert. Der CWA-Nutzer hat jederzeit die volle Kontrolle über sein Schnelltest-Profil, insbesondere kann er vor jeder Schnelltestung entscheiden, ob er sein Schnelltest-Profil nutzen will oder nicht. Da es keine Pflichtangaben gibt, kann der CWA-Nutzer auch selbst entscheiden, welche Angaben er in sein Schnelltest-Profil aufnimmt. Eine datenschutzfreundlichere Lösung ist nicht ersichtlich.

8.5.4 Angemessenheit

Die Verarbeitung der Daten im Rahmen des Schnelltest-Profiles ist angemessen. Durch die dezentrale lokale Bereitstellung des Schnelltest-Profils in der CWA App mittels QR-Codes wird die Datenerhebung für die Inanspruchnahme von Schnelltestangeboten auf das erforderliche Maß reduziert. Das RKI erhält zu keinem Zeitpunkt Zugriff auf diese Daten. Der Schaffung eines zentralverwalteten Datenbestands mit den Profildaten der CWA-Nutzer, der Begehrlichkeiten und Missbrauchsrisiken auslösen würde, wird bereits auf technischer Ebene wirksam vorgebeugt, indem das Schnelltest-Profil vollständig lokal, also nur auf dem Smartphone des CWA-Nutzers gespeichert und nicht geteilt werden kann. Das Schnelltest-Profil steht auch im Einklang mit der Zielsetzung der nationalen Teststrategie, indem ein wesentliches Hindernis für die Inanspruchnahme von Bürgertestungen, nämlich der damit verbundene Zeitaufwand, reduziert wird.

9 Risikoanalyse

9.1 Methodik

Grundlage und Hilfsmittel für die Planung, Durchführung und Dokumentation der Risikoanalyse im Rahmen dieser DSFA ist eine Excel-Arbeitsmappe, 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-Arbeitsmaßße 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.

Zur Durchführung der Risikoanalyse wurde der Prüfgegenstand in verschiedene Verarbeitungstätigkeiten (VT) aufgeteilt:

- VT 1: App-seitige Verarbeitung Kontaktbereignisse
- VT 2: Kontaktfall
- VT 3: Testing
- VT 4: Infektfall + Event-Registrierung
- VT 5: EFGS, PPA_EDUS (Datenspende)
- VT: Verifikations-Hotline
- VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Wallet-Funktionen

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-Risikoanalyse, 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 Risikoanalyse in Bezug auf die VT 1, 2 und 4 eingeflossen. Die EFGS-bedingten Ergänzungen sind blau hinterlegt.

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 angelehnt¹⁰⁰ – 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 bezwecken, können ein Risiko darstellen.

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.)

¹⁰⁰ Martin/Friedewald/Schiering/Mester/Hallinan: „Die Datenschutzfolgenabschätzung nach Art. 35 DSGVO – Ein Handbuch für die Praxis“, Frauenhofer Verlag, 2020.

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.¹⁰¹

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

Auch werden die Arten von Angriffen beschrieben:

¹⁰¹ 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 11.10.2022).

A	B	C	D
Arten des Angriffes	Beschreibung	X	
Passiv	Passiv Angreife betreffen die unauthorisierte Informationsgewinnung und zielen auf den Verlust der Vertraulichkeit ab. Hier und hauptsächlich auf die Informationsverarbeitung abgestellt. Der Angreifer sendet selbst keine Daten. Er erhält sich mehr passiv, indem er lediglich den Datenverkehr anderer Teilnehmer beobachtet, ohne diesen aktiv zu stören. Damit erhält er wichtige Vermittlungs- und Benutzertinformationen. Das dient ihm z.B. dazu, Verkehrsflusssanalyse des Netzwerks durchzuführen und somit einen Einblick über die Struktur eines Netzwerkes zu bekommen. Sämtliche abgefangenen Informationen können ihm als Ausgangsbasis für einen aktiven Angriff dienen.	1	
Aktiv	Aktive Angreife benutzen die unauthorisierte Modifizierung von Datenbanken und richten sich somit gegen die Dataverfügbarkeit oder Verfügbarkeit eines Systems. Aktive Angreife gehen dabei über ein passives Beobachten hinaus und beinhalten aktive Eingriffe in die Kommunikation, um Daten, IT Systeme oder Benutzer zu manipulieren. Diese Art von Angreifen beinhaltet folglich die nicht autorisierte Modifikation von Daten und richtet sich somit in erster Linie gegen die Dataverfügbarkeit und die Verfügbarkeit. Nach der erfolgreichen Durchführung einer aktiven Angreife hat der Angreifer direkten Zugang zu jedem Betriebsmittel und kann diese sehr missbrauchen. So kann er durch Vieldelokulation, Verzerrung, Erhöhung, Modifikation und Löschung bestimmter Daten eine falsche Identität vortäuschen und eventuell Rechte und Attribute modifizieren.	2	
Regional	Ein regionaler Angreifer ist in seinem Handlungsspielraum auf einige wenige in seine Gewalt gebrachte Geräte oder Infrastrukturreinheiten beschränkt.	1	
Überregional	Ein überregionaler Angreifer hat dagegen die Kontrolle über mehrere Geräte oder Infrastrukturreinheiten, die über ein überregionales Netzwerk verteilt sind.	2	
Rational	Ein rationaler Angreifer strebt nach persönlichem Profit und ist daher vorstellbar in Bezug auf Angreifstypen und Angreifsmittel.	1	
Bösartig	Ein bösartiger 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 Eintrügerin betrachtet wird. Dadurch ist er in der Vielfalt seiner Angreife eingeschränkt.	1	
Insider	Ein Angreifer wird als Insider bezeichnet, wenn er ein authentisiertes Mitglied des Systems ist, das mit anderen Mitgliedern kommunizieren kann.	2	
Indirekt	Ein direkter Angriff ist dadurch gekennzeichnet, dass dieser nur von einem einzigen Akteur ausgetragen 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	
Entlastig	Für die Durchführung eines indirekten Angriffs nutzt der Angreifer einen Benutzer des Zielsystems, welcher in der Regel bereits am Zielsystem angemeldet ist. Die Unwissenheit des Nutzers wird genutzt, um über dessen Rechte Zugriffe auf weitere Systeme zu erlangen.	2	
Mehrstufig	Benötigt ein Angriff nur einen einzelnen Schritt, um das geplante Ziel anzugehen, so handelt es sich um einstufigen Angriff.	1	
	Mehrstufige Angreiffe kombinieren verschiedene Angriffsarten, um sich dem eigentlichen Ziel schrittweise zu nähern. Hier kann z.B. zunächst zentrale Sicherheitsinfrastrukturen kompromittiert werden, um dann in weiteren Schritten die eigentlichen Ziele anzugehen. Dazu noch ein Beispiel: Ein Angreifer nutzt eine beliebige, unsichere Applikation, um zuerst einmal Inhalt zu gelangen. Im zweiten Schritt dann wird er z.B. von dort auf die datenführenden Systeme zu kommen.	2	

Abbildung 32: Risiko-Matrix

9.3.4 Bewertung der Schadenshöhe

Der potenzielle Schaden für betroffene Personen wird anhand der zu betrachtenden SDM-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.
Integrität	Integrität von Daten ist die Abwesenheit von korrumptierten Daten. Integrität bedeutet insbesondere die Abwesenheit unautorisierter Veränderungen.
Verfügbarkeit	Verfügbarkeit von Informationen und Systemen ist Zugriffbarkeit 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)
Schadenskategorien	Gesellschaftliche und soziale Nachteile (Rücksäßigungen, Ansehensverluste)	Kein oder unbedeutender Verstoß	geringfügige, vorübergehende Peinlichkeit	Verstoß: erheblichen Konsequenzen Beschädigung gesellschaftlicher Teilbereich; Mobbing, erheblicher Gesichtsverlust, aber mit Anstrengungen überwindbar	Fundamentaler Verstoß gegen Vorschriften und Gesetze gesellschaftliche Diskriminierung, schwer öffentlich Bloßstellung mit fundamentalen, irreversiblen Folgen
	Einschüchterungseffekt (wir Angst vor negativen Folgen nicht Betroffener davon ob Rechte auszuüben oder sich persönlich zu entfalten (z.B. Besuch von pol./kulturellen Veranstaltungen))	Keine oder unbedeutende Auswirkung	Eine geringe Betroffenheit bzw. nur örtlich und zeitlich begrenzter Einschüchterungseffekt ist zu erwarten	Ein umfassender Einschüchterungseffekt ist zu erwarten (Umfang, Zeit, Ort), aber jeweils durch Maßnahmen (Befreiung, Lokalisierung...) überwindbar	Ein erheblicher, dauernder und örtlich nicht mehr begrenzbarer Einschüchterungseffekt, eventuell sogar existenzgefährdender Art, ist denkbar.
	Übelbehandlung des Privatsphären (Verlust der Kontrolle über eigene Daten, Überwachung, Veröffentlichung von pD, individuellen Status, Orientierungs- und Verletzung weiterer (Grund-)Rechte (Meinungsfreiheit, Anti-Diskriminierung))	Keine oder unbedeutende Beeinträchtigung	Erheblich, überwindbar	Erhebliche Auswirkungen, überwindbar mit erheblichen 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)	Acute 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 kurzfristige Akzeptanzverlust von mehr als #### Prozent der Nutzer, die Maßnahmen zur Akzeptanzsicherung 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, höhere KV-Beträge)		≤ 1.000.000,-	finanziell: Verluste bis zu 100 EUR	Verluste bis zu 3 Netto-Monatsgehalten, bis 5.000 EUR oder Beeinträchtigung von Karriere-Chancen	Verlust oder langfristiger Verlust von Karriere-Chancen, > drei Netto-Monatsgehalte, 5.000,-

Abbildung 33: Schadensausmaß

Es handelt sich um eine qualitative Bewertung der jeweiligen Bedrohungen bezogen auf das jeweilige Schutzziel/Gewährleistungsziel. Dabei ist die Tabelle lediglich ein Hilfsmittel; die qualitative Bewertung kann unabhängig von der Risikozahl sowohl grundsätzlich als auch für bestimmte Aspekte ergänzend im DSFA-Bericht und in mitgeltenden Dokumenten beschrieben werden, 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	Die Auswirkungen des Schadens für betroffene Personen sind begrenzt und beherrschbar. Das Eintreten einer zu berücksichtigten Schadenssituation erscheint unmöglich.
Mittel	5-7	Der Schadenseffekt wäre nennenswert. Technische und organisatorische Maßnahmen SOLLEN vorgeschlagen werden.

		Als Teil der Kosten-Nutzen-Abwägung der notwendigen Maßnahmen kann das Risiko akzeptiert werden.
	8-10	<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-Datenschutzmodells¹⁰² (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.

¹⁰² DSK, Das Standard-Datenschutzmodell Version 2.0b, abrufbar unter: <https://www.datenschutzzentrum.de/sdm/> (zuletzt abgerufen am 11.10.2022).

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

Risikobewertung Schadensausmaß														
Risiko-Quelle	Nr.	Bedrohung/ Risiko	Schwach Stelle (jahr)	EW	Datennormierung	Vertraulichkeit	Integrität	Vierbarkeit	Authentizität	Resilienz	Interneinheitlichkeit	Transparenz	Zweckbindung/ Nichtverketzung	Risikoklasse
		Bedrohung vom +												
4		Unbefugte oder unrechtmäßige Verarbeitung durch CWA												
5	Rf-CWA-Nutzer	Datenverarbeitungen ohne nach widmerener Einwilligung	Ja	1	4	4	4	4	4	4	4	4	4	4
6	Rf-CWA-Nutzer	Unwirksame Einwilligung durch fehlende Freiwilligkeit ("erzwogene Einwilligung")	Ja	1	4	4	4	4	4	4	4	4	4	4
7	Rf-CWA-Nutzer	Unwirksame Einwilligung aufgrund fehlerhafter / fehlerhafter ausdrückliche Einwilligungserklärung (technischer Einwilligungs-Nkt)	Ja	1	4	4	4	4	4	4	4	4	4	4
8	Rf-CWA-Nutzer	Unwirksame Einwilligung aufgrund fehlender Information über Umfang und Folgen	Ja	2	4	4	4	4	4	4	4	4	4	8
9	Rf-CWA-Nutzer	Unwirksame Einwilligung aufgrund Nichteinreichbarkeit der notwendigen Informationen (sprachliche Barrieren, fehlendes Technikverständnis)	Ja	2	4	4	4	4	4	4	4	4	4	8
10	Rf-CWA-Nutzer F4 - Google/ Apple, CWA-Entwickler	Unwirksame Einwilligung von Minderjährigen unter 16 Jahre (Klärun durch AG)	Ja	4	4	4	4	4	4	4	4	4	4	16
11	Rf-CWA-Nutzer F4 - Google/ Apple, CWA-Entwickler	Abhängigkeiten von Dienstleistem/ Software Herstellern (Ausfall externer Dienstleister, versteckte Funktionen in Software)	Ja	2	3	3	3	1	1	1	1	1	3	5
12	Rf-CWA-Nutzer F4 - Google/ Apple, CWA-Entwickler	Abhängigkeiten von Dienstleistem/ Software Herstellern (Ausfall externer Dienstleister, unberechtigter Zugriff durch deren Mitarbeiter, versteckte Funktionen in Software) TISAP	Ja	1	4	4	4	4	4	4	4	4	4	4
13	Rf-CWA-Nutzer F4 - Google/ Apple, CWA-Entwickler	Fehlende unzureichende vertragliche Regelungen mit Dienstleistem (Auftragsverarbeitung)/ Vertrag zur gemeinsamen Verantwortung - Google/ Apple - Verantwortlichkeiten des Kunden spezielle API	Ja	2	4	4	4	4	4	4	4	4	4	8
14	Riskquellen	Fehlende unzureichende vertragliche Regelungen mit Dienstleistem (Auftragsverarbeitung)/ Vertrag zur gemeinsamen Verantwortung - mit TISAP	Ja	1	4	4	4	4	4	4	4	4	4	4

Abbildung 34: 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 gemeinsam Verantwortlichen ergriffenen oder geplanten Maßnahmen zur Risikobehandlung/-minimierung werden in den Risikomatrizen der jeweiligen Verarbeitungstätigkeiten beschrieben, die als Anlagen 3, 4, 5, 8 (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.¹⁰³

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, thematisch zusammengefasst. 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 (CWA) einerseits (Abschnitt 9.5.1) und der Interoperabilität (EFGS/CHGS) 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.

¹⁰³ Vgl. Dokumentation auf GitHub, abrufbar unter <https://github.com/corona-warn-app/> (zuletzt abgerufen am 11.10.2022).

9.5.1 Hohe Restrisiken der CWA

9.5.1.1 Verwendung von Dritt-Technologien

Der Umstand, dass die CWA App die Konnektivitäten und das ENF von Google und Apple sowie die Echtheitsprüfungsdienste Apple DeviceCheck und Google SafetyNet verwendet, stellt ein erhebliches Datenschutzrisiko dar, welches durch das RKI jedoch praktisch nicht beseitigt und auf technischer Ebene auch nicht reduziert werden kann. Gleiches gilt hinsichtlich des Angewiesenseins der CWA App auf den 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 Bild¹⁰⁴, 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 zumindest mit den Datenschutzrisiken, die mit der Verwendung eines Smartphones oder Betriebssystems dieser Hersteller für persönliche Zwecke einhergehen, akzeptiert und gegebenenfalls 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 CWA-Nutzers zurückgehen, 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 Apps nicht realisierbar.

¹⁰⁴ Vgl. Dokumentation auf github, abrufbar unter <https://github.com/google/exposure-notifications-android> (zuletzt abgerufen am 11.10.2022).

Sofern CWA-Nutzer an der Datenspende teilnehmen oder einer Einladung zu einer Befragung des RKI folgen, werden Daten zu dem verwendeten Endgerät im Rahmen der Echtheitsprüfung von den Drittdiensten Apple DeviceCheck und Google SafetyNet verarbeitet. Dabei ist damit zu rechnen, dass die Daten des CWA-Nutzers auch in Drittländern, insbesondere in den USA, verarbeitet werden. Da die Teilnahme an der Datenspende und an einer Befragung eine Einwilligung des CWA-Nutzers in die Verarbeitung seiner Daten durch die o. g. Drittdienste erfordert, die ausdrücklich auch auf die Drittlandübermittlung eingeht (Art. 49 Abs. 1 lit. a DSGVO), besteht die Gefahr, dass ein CWA-Nutzer die Tragweite seiner Einwilligungserklärung in Bezug auf die Risiken der Drittlandübermittlung verkennt. Dem kann nur durch eine entsprechend transparente Einwilligungserklärung und flankierende Datenschutzhinweise begegnet werden. Der ausdrückliche Hinweis auf Risiken in Verbindung mit Drittlandsübermittlungen findet sich dahingehend sowohl im Text der Einwilligung, unmittelbar über dem Button „Einverstanden“, auf der weiterführenden Informationsebene als auch noch gesondert in der Datenschutzerklärung. Die mit der Echtheitsprüfung verbundenen Funktionen Datenspende und Teilnahme an Befragungen sind überdies nicht mit dem unmittelbaren Nutzen der CWA für die CWA-Nutzer verbunden und insofern rein optional und freiwillig. Sie stellen Zusatzfunktionen dar, die aber keine unmittelbaren Vor- oder Nachteile mit sich bringen. Es ist daher davon auszugehen, dass sich ein CWA-Nutzer für diese nicht unmittelbar mit dem Warnzweck verbundenen Verarbeitungsvorgänge in Ansehung des beschriebenen Risikos ausreichend auseinandersetzen wird und im Zweifel die Übermittlung nicht initiieren wird, wenn er die Funktion nicht oder nicht vollständig einschätzen kann.

Weiterhin birgt die Nutzung der von Google und Apple bereitgestellten Echtheitsprüfungs-Dienste ein Transparenzrisiko. Denn die genaue technische Umsetzung und Funktionsweise dieser Dienste ist der Kontrolle des RKI entzogen, zumal Apple und Google die exakte Funktionsweise dieser Dienste unter Verweis auf Sicherheitsgründe bewusst geheim halten. Daher kann nicht ausgeschlossen werden, dass Apple bzw. Google die erhaltenen Daten zu eigenen weiteren Zwecken nutzen, über die die Öffentlichkeit nicht informiert wird. Es ist anzunehmen, dass Apple und Google jederzeit technische Änderungen vornehmen könnten, die eine Identifizierbarkeit einzelner CWA-Nutzer ermöglichen oder die vom RKI ergriffenen eigenen Pseudonymisierungsmaßnahmen abschwächen oder gar aufheben können. Es kann zudem nicht ausgeschlossen werden, dass Google und Apple die an sie im Rahmen von PPAC übermittelten Daten für weitere Zwecke nutzen. Insbesondere besteht auch die Gefahr, dass Nutzungsdaten mit weiteren den Betriebssystemanbietern über die CWA-Nutzer bekannten Informationen zusammengeführt werden und gegebenenfalls Verhaltensanalysen erfolgen. Es kann auch möglich sein, festzustellen, ob die CWA App von einzelnen Personen genutzt wird.

Diese Risiken bestehen jedoch für alle App-Anbieter, die die Echtheitsprüfungs-Dienste der Betriebssystemhersteller nutzen.

Auch eine Zusammenführung mit den im ENF und im Kontakt-Tagebuch gespeicherten Informationen kann nicht vollends ausgeschlossen werden. So scheinen auch Analysen bezüglich Warnhäufigkeit und damit verbundenen Risikomeldungen der CWA App grundsätzlich möglich. Gleichwohl ist zu berücksichtigen, dass durch den Einsatz von PPAC das Risiko der zweckwidrigen Nutzung von im Rahmen des ENF verarbeiteten Daten durch die Betriebssystemanbieter nicht erhöht wird. Das Token beinhaltet für die Betriebssystemanbieter keinen zusätzlichen Informationswert bzw. keine Informationen, die

nicht bereits aufgrund der allgemeinen Verwendung der Betriebssysteme vorliegen (Device-Informationen und Installation der CWA App). Unter Berücksichtigung der Tatsache, dass der Einsatz der Dienste der Betriebssystemanbieter erforderlich ist, um die Datenqualität möglichst gewährleisten zu können und die Datenverarbeitung für Zweckerreichung erforderlich ist, können die verbleibenden Risiken daher hingenommen werden. Auch in diesem Zusammenhang ist zu berücksichtigen, dass die Funktionen, in deren Kontext die von Google und Apple bereitgestellten Echtheitsprüfungs-Dienste zum Einsatz kommen, rein optionale Zusatzfunktionen der CWA App darstellen, die für die Funktionalität der für den CWA-Nutzer maßgeblichen Warnfunktion nicht relevant sind und für den CWA-Nutzer keine unmittelbaren Vor- oder Nachteile aus der Aktivierung der Funktionen erwachsen. Auf die uneingeschränkte Funktionalität der Hauptfunktionen auch ohne Erteilung der Einwilligung zur Datenspende oder im Rahmen der Befragungseinladungen wird ausdrücklich hingewiesen.

Im Ergebnis ist der Einsatz der Echtheitsprüfungs-Dienste der Betriebssystemhersteller daher hinnehmbar.

9.5.1.2 Bedien-/Technikfehler auf Seiten des CWA-Nutzers

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 vollständig 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 Datenverarbeitungen des CWA-Nutzers

Durch den ausnahmsweise¹⁰⁵ datenschutzrechtlich eigenverantwortlichen Gebrauch des lokalen Kontakt-Tagebuchs der CWA App durch den CWA-Nutzer können Schäden bei Kontaktpersonen entstehen. Falls sich der CWA-Nutzer in diesem Fall seiner Pflichten als Verantwortlicher nicht bewusst ist, besteht eine hohe Wahrscheinlichkeit von Verletzungen des Schutzes personenbezogener Daten von Kontaktpersonen. Dieses Risiko besteht grundsätzlich bei jeder Software, die ihrem Anwender eine lokale Verarbeitung von

¹⁰⁵ Der bestimmungsgemäße Gebrauch des Kontakt-Tagebuchs durch den CWA-Nutzer fällt unter die sog. Haushaltlausnahme des Art. 2 Abs. 2 lit. c DSGVO, so dass eine datenschutzrechtliche Verantwortlichkeit des CWA-Nutzers nicht besteht. Nur für den Fall, dass er diesen Ausnahmetatbestand verlässt, kommen die in diesem Abschnitt dargestellten Risiken in Betracht. Siehe hierzu ausführlich in Abschnitt 7.3.2.3.

(personenbezogenen) Texteingaben ohne Zugriffsmöglichkeit des Herstellers der Software zu selbst festgelegten Zwecken erlaubt (z. B. lokale Textverarbeitungen und E-Mail-Programme). Sie müssen und dürfen daher, soweit sie nicht durch angemessene Maßnahmen weiter reduziert werden können, hingenommen werden.

Zur Reduzierung der Eintrittswahrscheinlichkeit des Risikos trägt die Vorstellung und Charakterisierung der Kontakt-Tagebuch-Funktion als „persönliche Gedächtnissstütze“ für den CWA-Nutzer sowie der erkennbare persönliche Zweck und Charakter der CWA App bei, so dass bei dem naheliegenden bestimmungsgemäßen Gebrauch des Kontakt-Tagebuchs der Bereich ausschließlich persönlicher oder familiärer Tätigkeiten (Art. 2 Abs. 2 lit. c DSGVO) regelmäßig nicht verlassen werden dürfte und infolge eine Verletzung des Schutzes personenbezogener Daten von Kontaktpersonen nicht eintreten kann. Der CWA-Nutzer wird vor der ersten Verwendung des Kontakt-Tagebuchs in der CWA App explizit darauf hingewiesen, dass die Privatsphäre seiner Mitmenschen und deren Wunsch, nicht in das Kontakt-Tagebuch eingetragen zu werden, respektiert werden sollte. Die CWA App löscht Eintragungen über erfolgte Begegnungen automatisch nach 16 Tagen aus dem Kontakt-Tagebuch und ordnet Begegnungen mit Kontaktpersonen nur einem Datum, aber keiner Uhrzeit zu; diese Gestaltung lässt eine Verwendung des Kontakt-Tagebuchs zu anderen als den bestimmungsgemäßen persönlichen Zwecken eher fernliegend erscheinen. Ein CWA-Nutzer, der andere oder weitergehende Zwecke verfolgt, wird mit hoher Wahrscheinlichkeit direkt auf andere Apps, insbesondere auf die auf nahezu jedem Smartphone installierten Standard-Apps (z. B. Kalender-, E-Mail- und Notizbuch-Apps) zurückgreifen.

9.5.1.4 Schnelltest-Anbindung

Wenn ein CWA-Nutzer seinen namentlichen Schnelltest-Nachweis in der CWA App erhalten möchte, erhalten die Teststelle sowie deren Mitarbeiter aufgrund der Auswahl des CWA-Nutzers der jeweiligen Option Kenntnis davon, dass die Testperson ein CWA-Nutzer ist. Diese zusätzliche Information könnte verwendet werden, um CWA-Nutzer in anderem Kontext zu re-identifizieren und ggf. die Wirksamkeit der Pseudonymisierung beeinträchtigen.

Diese Information, dass eine getestete Person CWA-Nutzer ist, erlaubt den Mitarbeitern in den Teststellen jedoch keinen Rückschluss darauf, welche Funktionen der CWA App genutzt werden, also beispielsweise, ob die Risiko-Ermittlung aktiviert ist oder andere gewarnt werden. Spezifische Daten aus der CWA, wie z.B. Tagesschlüssel werden Mitarbeitern in Teststellen im Zusammenhang mit dem Scan des QR-Codes durch den CWA-Nutzer nicht bekannt. Das mit Kenntnis der Information zur CWA-Nutzer-Eigenschaft verbundene Missbrauchsrisiko wird dadurch weiter minimiert, dass die Teststellen und deren Mitarbeiter vertraglich zum vertraulichen Umgang mit personenbezogenen Daten der CWA-Nutzer verpflichtet werden. Zudem ist zu berücksichtigen, dass sich der CWA-Nutzer freiwillig dafür entscheidet, bei einer bestimmten Teststelle einen Schnelltest durchzuführen und das Testergebnis mittels der CWA App abzurufen. Es kann praktisch ausgeschlossen werden, dass ein CWA-Nutzer in diesem Fall nicht erkennt, dass die Teststelle und ihre Mitarbeiter von seiner Eigenschaft als Nutzer der CWA App erfahren werden.

Primäre Funktion des Schnelltest-Nachweises ist es, diesen als Beleg für die Durchführung eines Schnelltests gegenüber Dritten vorzeigen zu können. Dabei sind die Bedingungen, unter denen ein Schnelltest-Nachweis vorgelegt werden muss, in verschiedenen Verordnungen der Länder sowie im IfSG geregelt. Es lässt sich nicht ausschließen, dass Dritte auch in anderen Fällen den Nachweis eines negativen Schnelltests durch die CWA App verlangen werden, auch wenn dies weder sachgerecht noch geboten ist oder gar unzulässig sein sollte.

Insoweit ist jedoch zu berücksichtigen, dass negative Schnelltest-Nachweise auch auf anderem Wege, zum Beispiel mittels eines Papierdokuments, erbracht werden können. Zudem wird in der CWA App an verschiedenen Stellen ausdrücklich darauf hingewiesen, dass die Vorlage eines Schnelltest-Nachweises nur in den gesetzlich vorgesehenen Fällen verlangt werden darf. Es ist daher nicht ersichtlich, warum Dritte gerade die Vorlage des Schnelltest-Nachweises mittels der CWA App verlangen sollten. Insofern besteht das Risiko auch bei jeder anderen Form des Schnelltest-Nachweises. Vor dem Hintergrund der Offenlegung des minimalen Datensatzes im Schnelltest-Nachweis (Vor-, Nachname, Geburtsdatum) wird das verbleibende spezifische Risiko, das durch die Schnelltest-Nachweisfunktion der CWA App geschaffen wird, als akzeptabel bewertet.

9.5.1.5 Einsatz von Auftragsverarbeitern

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.

9.5.1.6 Cyberkriminalität / Sabotageversuche

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, hat sich bislang nicht realisiert.

Der Hotline-Prozess verlief nach Aussagen der zuständigen Dienstleister bisher ohne Auffälligkeiten. 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 Restrisiko des Vortäuschens einer falschen Identität oder falscher positiver Testergebnisse über die Hotline 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 seit Release der CWA App deutlich abgenommen hat.

Ein Organisator eines Events könnte für jeden Gast einen individuellen QR-Code zum Einchecken erstellen und sich anschließend selbst bei allen erstellten Events als Guest einchecken. Wenn einer der Gäste positiv getestet wird und eine Warnung auslöst, kann der

Event-Veranstalter auf diese Weise erkennen, um welche Person es sich handelt. Ein solches Risiko ließe sich nur vermeiden, wenn eine Mindestanzahl von Gästen verlangt wird, um eine Warnung für andere eingecheckte CWA-Nutzer auszulösen. Das wäre aber mit dem dezentralen Ansatz der Event-Registrierung nicht vereinbar. Das Missbrauchsrisiko kann und muss daher – soweit es vom RKI wie vorliegend nicht durch angemessene Maßnahmen weiter reduziert werden können – hingenommen werden. Andernfalls wäre die Event-Registrierung mit dezentralem und datensparsamem Ansatz nicht realisierbar.

9.5.1.7 Minderjährige

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.

9.5.1.8 Fehlfunktionen/Unwirksamkeit der CWA App

Der Einsatz einer Tracing-App zur Bekämpfung einer Virus-Pandemie ist weiterhin technisches Neuland. Daher können Fehlfunktionen oder unzureichende epidemiologische Wirksamkeit der CWA App naturgemäß nicht ausgeschlossen werden.

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.

Die bisher vorliegenden Evaluationsergebnisse lassen überwiegend auf eine relevante Wirksamkeit der CWA schließen.

9.5.1.9 Missbräuchliche Nutzung des Hotline-Verfahrens

Die Verifikations-Hotline geht mit einem Missbrauchspotential einher, wenn diese gewollte oder ungewollte Rechtsfolgen für Einzelne oder Gruppen entfalten sollte. 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.

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 weiterhin, alle Labore schnellstmöglich an den digitalen Prozess (QR-Code-Verfahren) anzuschließen. Bis alle Labore angeschlossen sind, ist die Verifikations-Hotline erforderlich, 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.

9.5.1.10 Re-Identifizierung durch andere CWA-Nutzer

Im Rahmen der Funktion der Event-Registrierung wird dem CWA-Nutzer im Kontakt-Tagebuch angezeigt, ob ein von ihm besuchtes Event ein niedriges oder ein erhöhtes Infektionsrisiko hat. Diese Information, auch zusammen mit den Informationen aus dem Kontakt-Tagebuch und dem Gedächtnis des CWA-Nutzers, erlauben es, Hypothesen bezüglich des Infektionsstatus eines anderen eingecheckten CWA-Nutzers aufzustellen, insbesondere wenn es sich um ein Event mit nur wenigen eingecheckten CWA-Nutzern handelt. Dieses Risiko liegt jedoch in der Natur des Kontakt-Tagebuchs und insbesondere der Begegnungs-Historie der CWA App und würde auch bei einer Aufzeichnung auf Papier oder mit einer anderen App bestehen.

Dieses für den CWA-Nutzer verbleibende Restrisiko wird insgesamt als hinnehmbar bewertet, da die vorgesehenen Maßnahmen zur Risikobehandlung (Beschreibung der Funktionsweise der Event-Registrierung und des Kontakt-Tagebuchs für CWA-Nutzer) angemessen und das Re-Identifizierungsrisiko für den CWA-Nutzer einschätzbar ist.

9.5.1.11 Anbindung an EFGS und CHGS

Das Risiko besteht darin, dass der CWA Server oder das entsprechende Serversystem einer anderen nationalen Corona-App die über den EFGS bzw. CHGS 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 bzw. CHGS 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 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 bzw. CHGS heruntergeladenen Schlüssel nicht erneut an das EFGS bzw. CHGS übermittelt. Hinsichtlich des Risikos für CWA-Nutzer wird der CWA Server so konfiguriert, dass die an den EFGS bzw. CHGS 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 bzw. CHGS verarbeitet werden.

Das identifizierte Restrisiko wird als akzeptabel bewertet, muss jedoch weiter beobachtet und in Zusammenarbeit mit den jeweiligen anderen Verantwortlichen weiter mitigiert werden.

9.6 Hohe Restrisiken der Interoperabilität

Hinweis: Soweit die nachfolgenden Ausführungen nur auf den EFGS Bezug nehmen, gelten sie – vorbehaltlich eines anderslautenden Hinweises – grundsätzlich entsprechend auch für den CHGS, da dieser technisch und funktional äquivalent zum EFGS abläuft. Soweit nur auf den CHGS Bezug genommen wird, gelten die Ausführungen nur für diesen.

9.6.1 Fehlende Rechtsgrundlage

Jeder Verantwortliche trägt die Verantwortung für die Verarbeitung personenbezogener Daten im EFGS.¹⁰⁶ Es besteht daher 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 deshalb 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 Verarbeitung veralteter oder nicht erforderlicher Daten

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 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.

¹⁰⁶ 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).

- 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 in den Designentscheidungen (Anlage 7) sowie den der gemeinsamen Verarbeitung zugrundeliegenden Durchführungsbeschluss (EU) 2020/1023 einschließlich der Anhänge.

Da dem RKI bis heute keine Zuwiderhandlungen einzelner Verantwortlicher gegen die gemeinsam festgelegten bzw. noch festzulegenden Maßnahmen bekannt geworden sind, wird das Risiko als akzeptabel bewertet.

9.6.3 Verwendung und technische Einschränkungen des ENF

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 Zuordnbarkeit 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, wird insoweit als ein Risiko für die gemeinsam verarbeiteten Daten angesehen, 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 im Ergebnis als akzeptabel bewertet. Jedoch sollten die gemeinsamen Verantwortlichen den Dialog mit den ENF-Herstellern suchen, um zukünftig stärker Einfluss auf deren Designentscheidungen nehmen zu können.

9.7 Zertifikats-Wallet

Wenn bei einem Zertifikatswiderruf aller von einer bestimmten bescheinigenden Stelle (z. B. einer bestimmten Apotheke) ausgegebenen COVID-Zertifikate diese anhand der ersten zwei Blöcke ihrer eindeutigen Zertifikatskennung, die bei allen von der bescheinigenden Stelle ausgegebenen COVID-Zertifikate identisch ist, identifiziert und sodann insgesamt widerrufen werden (etwa weil eine systematische Ausgabe von falschen COVID-Zertifikaten erkannt worden ist), besteht das Risiko eines Widerrufs auch von echten bzw. ordnungsgemäß ausgestellten COVID-Zertifikaten ohne ausreichende Rechtsgrundlage.

Das RKI geht davon aus, dass mit Art. 10 Abs. 2 DCC-VO eine ausreichende Rechtsgrundlage gemäß Art. 9 Abs. 2 lit. g DSGVO für den Widerruf ganzer Zertifikatsgruppen jedenfalls dann besteht, wenn die betreffenden COVID-Zertifikate von einer nachweislich unzuverlässigen bzw. nicht vertrauenswürdigen Stelle ausgegeben worden sind und angesichts der hohen Zahl der COVID-Zertifikate die individuelle Überprüfung jedes potenziell falschen COVID-Zertifikats praktisch unmöglich ist. Aus Art. 4 Abs. 2 DCC-VO, Art. 10 Abs. 5 DCC-VO und Erwägungsgrund 51 der DCC-VO ergibt sich, dass ein Widerruf auch zur Vorbeugung von Betrug und insbesondere Fälschungen zulässig ist. Das in der DCC-VO beschriebene Widerrufsverfahren mittels personenbezogener Widerrufslisten stellt insoweit keine Bedingung für den Widerruf dar. Sofern das Widerrufsverfahren keine personenbezogene Datenverarbeitung erfordert, wird keine Rechtsgrundlage für die für den Widerruf erforderliche Datenverarbeitung benötigt.

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 gegeben sein, also etwa die Corona-Pandemie abflauen, muss das RKI bewerten, ob die Aufrechterhaltung des Betriebs der CWA weiterhin erforderlich ist.

Zur Vorbereitung einer solchen Entscheidung werden seitens des RKI regelmäßig die epidemische Lage sowie die Wirksamkeit der CWA bewertet. Eine erstmalige umfassende Evaluierung der CWA ist im ersten Quartal 2021 erfolgt und umfasste neben den öffentlich zugänglichen Kennzahlen (www.coronawarn.app/de/analysis) eine ereignisbezogene Befragung von CWA-Nutzern in Form einer Online-Befragung und die ereignisunabhängige Analyse technischer Nutzungsdaten zur Funktion der Corona-Warn-App.

Die Ergebnisse zur Wirksamkeit der CWA werden regelmäßig im Blogformat auf <https://www.coronawarn.app/de/science> erläutert. Zudem werden die Erkenntnisse für den wissenschaftlichen Diskurs aufbereitet und in Fachzeitschriften publiziert.

10.2 Nächster Prüfungstermin

Die nächste Aktualisierung der DSFA erfolgt spätestens vor dem letzten geplanten Major-Release der CWA App (Version 3.0) vor dem Übergang der CWA in den Wartungsbetrieb.

11 Anlagen

- Anlage 1: Designentscheidungen bei der Entwicklung der Corona-Warn-App der Bundesrepublik Deutschland und Nachweisfunktion (Version 2.24)
- Anlage 2: Technisch-Organisatorische Maßnahmen (Version 1.1)
- Anlage 3: Risikomatrix VT 1, 2, 4 (Version 2.16)
- Anlage 4: Risikomatrix VT 3 Testing mit Laborschnittstelle (Version 2.15)
- Anlage 5: Risikomatrix Verification Hotline (Version 2.9)
- Anlage 6: Risikomatrix VT 5 EFGS (Version 1.5)
- Anlage 7: Risikomatrix VT 5 PPA_EDUS (Version 2.14)
- Anlage 8: Risikomatrix VT 6 (Version 2.24)
- Anlage 9: Glossar (Version 2.24)