Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse + VT2: Kontaktfall + VT4: Infektfall + Eventregistrierung+Stopp der Warnungen (Stand: 22.05.2023)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
	4	**1) Unbefugte oder unrechtmäßige Verarbeitung durch CWA**																		
R8- Behörden	5	Unklare Verantwortlichkeiten in Bezug auf die Datenverarbeitungen (EFGS-Risiko) Noch zu prüfen: Joint Controller Verträge durch Gesetz ersetzt, Joint Controller Verträge mit DIGIT notwendig (nennen der Unterauftragsverarbeiter von DIGIT)?	Zweck und Mittel der Datenverarbeitung werden nicht vom Verantwortlichen bestimmt. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	4	4	4	4	4	4	4	4	4	4	RM	Festlegung eindeutiger Verantwortlichkeiten für die gemeinsam Verantwortlichen, die Kommission und die Auftragsverarbeiter (gemäß bindender EU Entscheidung 2020/1023 und durch Abschluss der erforderlichen Verträge mit den Auftragsverarbeitern (Art. 28 DSGVO)).			akzeptabel
R8- Behörden	6	Unklare Verantwortlichkeiten in Bezug auf die Datenverarbeitungen durch CWA-Anschluss der Schweiz	Zweck und Mittel der Datenverarbeitung werden nicht vom Verantwortlichen bestimmt. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	4	4	4	4	4	4	4	4	4	4	RM	Abschluss eines (völker-)rechtlichen Vertrages mit der Schweiz erfolgt.			akzeptabel
R1-CWA-Nutzer	7	Datenverarbeitungen ohne/ nach widerrufener Einwilligung (Deinstallation der CWA-App)		Ja	1	4	4	4	4	4	0	4	0	4	4	RM	Siehe Designentscheidungen D-2.1-2 (Install) + D-2.1-6 (Upload) + Designentscheidung D-3.1-1 + Designentscheidung D-3.1-8 (Widerruf).			akzeptabel
R8- Behörden	8	Datenverarbeitungen ohne Rechtsgrundlage mittels EFGS: Jede Art von nochmaligem Upload durch empfangende nationale Backends der Mitgliedsstaaten (inkl. Schweiz) auf EFGS-Server. Weitere und von der ursprünglichen Datenverarbeitung zu unterscheidende Datenverarbeitung, die von Rechtsgrundlage nicht umfasst wird (EFGS-Risiko).	Ein nationales Backend lädt personenbezogene Daten vom EFGS herunter. Es kann sich hierbei auf die von dem die Daten erhebenden Mitgliedsstaat geschaffene Rechtsgrundlage berufen. Diese Rechtsgrundlage begründet jedoch nicht einen erneuten Upload durch das heruntergeladene nationale Backend. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	3	4	4	0	0	0	0	4	4	4	12	RM	Klare Trennung der Verarbeitungswege personenbezogener Daten in den nationalen Backends nach der Herkunft der Daten. Vorzugsweise werden die personenbezogenen Daten mit einem Herkunftskennzeichen während der Verarbeitung versehen. Der CWA-Server lädt vom EFGS heruntergeladene Schlüssel nicht erneut hoch.	Eine Prüfung des Vorliegens einer Rechtsgrundlage im Onboarding-Prozess der Joint Controller zum EFGS erfolgt nicht. Vielmehr wird diesen Vertrauen entgegengebracht, Daten nicht ohne Rechtsgrundlage zu verarbeiten. Eine technische Mitigation könnte darin bestehen (bisher nicht geplant), dass der CWA-Server im Rahmen der Paketierung der Diagnoseschlüssel den Parameter rolling_start_interval_number der Schlüssel überprüft und veraltete Schlüssel verwirft. Herdurch würde das Risiko umgangen, Schlüssel zu verteilen, die nur auf Grund des Wiederhochladens noch im System nationale Backends und EFGS verarbeitet werden.	Siehe Anlage 7, Ziff. 2.3.2 (3).	bedingt akzeptabel
R8- Behörden	9	Datenverarbeitungen ohne Rechtsgrundlage mittels Schweizer Gateway	Die CWA könnte Daten über das Scheizer Gateway übermittelt bekommen, die von Drittstaaten stammen. Die Schweiz könnte Daten, die von der CWA über das Schweizer Gateway übermittelt werden an Drittstaaten weiterleiten. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	2	4	4	0	0	0	0	4	4	4	8	RM	Abschluss eines (völker-)rechtlichen Vertrages mit der Schweiz erfolgt.			akzeptabel mit Evaluation
R1-CWA-Nutzer	10	Nicht rechtskonforme Verarbeitung im KTB	Für CWA-Nutzer selbst könnten sich Risiken aus seiner Verantwortlichkeit für die rechtskonforme Datenverarbeitung bei Nutzung des KTB ergeben. Die Verantwortlichkeit könnte dem Nutzer nicht transparent sein, ebenso seine Pflichten zur Wahrung der Privatsphäre Dritter. Hieraus können Schadensersatzansprüche erwachsen und - soweit die Bereichsausnahme nicht gilt - Bußgelder.	Ja	3	3	3	3	1	1	1	3	3	3	9		Designentscheidungen zur Einführung des KTB (siehe Anlage 1 zum DSFA-Bericht: D-2-2b, D-6-2c, D-5-11, D-9-8, D-7-10), DSK-Rahmenkonzept 14.27.17.			akzeptabel, mit Evaluation
R1-CWA-Nutzer	11	[Release 1.14] Unrechtmäßige DV bei Eintrag von Kontaktpersonen in KTB (inkl. falscher Eintrag)	Risiken für die Persönlichkeitsrechte derjenigen Personen, die in KTB eingetragen werden. Die Risiken erhöhen sich mit der Erweiterung der Attribute mit [Release 1.14], insbesondere auch durch die Einführung eines Freitextfeldes, indem der Nutzer genauere Informationen zur Begegnung aufzeichnen kann.	Ja	3	2	3	2	1	1	1	3	3	3	9	DM, VT, IG, T, ZB	Designentscheidungen zur Einführung des KTB (siehe Anlage 1 zum DSFA-Bericht: D-2-2b, D-6-2c, D-5-11, D-9-8, D-7-10), DSK-Rahmenkonzept 14.27.17.			akzeptabel, mit Evaluation
R1-CWA-Nutzer	12	Unwirksame Einwilligung durch fehlende Freiwilligkeit ("erzwungene Einwilligung")		Ja	1	4	4	4	4	4	4	4	4	4	4	RM	Siehe Z 5 "Unklare Verantwortlichkeiten in Bezug auf die Datenverarbeitung (EFGS-Risiko)" und Datenschutzinformationen. Abgestimmte Datenschutzinformationen liegen vor (DSK Verifikation und Testergebnis, 9.1 (mitgeltende Dokumente Datenschutzerklärung)).			akzeptabel
R1-CWA-Nutzer	13	Erzwungene Freiwilligkeit der DV von personenbezogenen Daten im KTB	Der Eintrag von Kontaktpersonen in das KTB erfolgt unabhängig vom Wissen und Wollen der Kontaktpersonen, die auch nicht CWA-Nutzer sein müssen.	Ja	2	4	4	4	4	4	4	4	4	4	8		Designentscheidungen zur Einführung des KTB (siehe Anlage 1 zum DSFA-Bericht: D-2-2b, D-6-2c, D-5-11, D-9-8, D-7-10), DSK-Rahmenkonzept 14.27.17.			akzeptabel mit Evaluation
R1-CWA-Nutzer	14	Unwirksame Einwilligung aufgrund fehlender/ fehlerhafter ausdrückliche Einwilligungserklärung (technischer Einwilligungs-Akt)		Ja	1	4	4	4	4	4	4	4	4	4	4	RM	Siehe Designentscheidungen D-2.1-2 (Install) + D-2.1-6 (Upload) + Designentscheidung D-3.1-1 + Designentscheidung D-3.1-8 (Widerruf).			akzeptabel
R1-CWA-Nutzer	15	Unwirksame Einwilligung aufgrund fehlender Information über Umfang und Folgen		Ja	2	4	4	4	4	4	4	4	4	4	8		Designentscheidungen zur Einführung des KTB (siehe Anlage 1 zum DSFA-Bericht: D-2-2b, D-6-2c, D-5-11, D-9-8, D-7-10), DSK-Rahmenkonzept 14.27.17.			akzeptabel mit Evaluation
R1-CWA-Nutzer	16	Unwirksame Einwilligung aufgrund Nichterreichbarkeit der notwendigen Informationen (sprachliche Barrieren, fehlendes Technikverständnis)		Ja	2	4	4	4	4	4	4	4	4	4	8	DM, VT, IG, IV, TR, ZB	Abgestimmte Datenschutzinformationen liegen vor (DSK Verifikation und Testergebnis, 9.1 (mitgeltende Dokumente Datenschutzerklärung)).			akzeptabel, mit Evaluation und ggf. Anpassung Datenschutzerklärung
R1-CWA-Nutzer	17	Unbefugte Nutzung der App durch Minderjährige unter 16 Jahre		Ja	4	4	4	4	4	4	4	4	4	4	16	DM, VT, IG, IV, TR, ZB	Datenschutzinformationen in leichter Sprache, Übersetzungen.			akzeptabel, mit Evaluation und ggf. Anpassung Datenschutzerklärung
R4- Apple / Google	18	Abhängigkeiten von Dienstleistern/ Software- und Firmware Hersteller (Ausfall externer Dienstleistern) - Google/ Apple		Ja	2	0	0	0	3	0	2	2	3	2	6	VF, TR	Designentscheidungen zur Nutzung API und ENF (siehe Designentscheidungen, D-6-3).			akzeptabel, mit Evaluation
R4- Betreiber Server (T)	19	Abhängigkeiten von Dienstleistern/ Software Herstellern (Ausfall externer Dienstleister) - SAP/T, DIGIT (EFGS)	Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	0	0	0	3	0	2	2	3	2	3	VF, TR	Siehe Designentscheidungen D-3-1. Die App und die Backend-Infrastruktur folgen dem Open-Source-Prinzip - lizenziert unter Apache 2.0.			akzeptabel
R4- Betreiber Server (T)	20	Abhängigkeit des Betriebs des EFGS von der Verfügbarkeit der Infrastruktur der nationalen Backends der Corona-Warn-Systeme der Mitgliedsstaaten (EFGS-Risiko)	Einschränkung oder Verlust der Verfügbarkeit der Datenverarbeitungsfunktionen (grenzüberschreitende Verteilung von Diagnoseschlüsseln). Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	3	3	0	3	0	3	3	3	3	3	DM, VF, R, IV, TR, ZB, VT	Design-Entscheidungen EFGS D-2-3, D-2-6, D-2-8, D-2-9: Die Mitgliedsstaaten sind für die Umsetzung der durch die Gesundheitsbehörden festgelegten Vorgehensweisen zuständig. Design-Entscheidungen EFGS D-2.1-3: Die Kommission unterstützt alle Funktionen des EFGS.			akzeptabel
R4- Apple / Google	21	Fehlende/ unzureichende vertragliche Regelungen mit Dienstleistern (Auftragsverarbeitung/ Vertrag zur gemeinsamen Verantwortung) - Google/ Apple - Verantwortlichkeiten des Kunden spezielle API		Ja	2	3	3	3	3	0	2	2	3	3	6	ZB , TR	AVV/ gem. Verantwortung/ Leistungsbeschreibung/ (soweit mgl.), siehe Designentscheidungen D-5.1-1.			akzeptabel, mit Evaluation
R4- Betreiber Server (T)	22	Fehlende unzureichende vertragliche Regelungen mit Dienstleistern (Auftragsverarbeitung/ Vertrag zur gemeinsamen Verantwortung) - mit T/SAP + DIGIT/ TSI (EFGS)	Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	3	3	3	3	0	2	2	3	3	3	ZB, TR	AVV (inkl. TOM) T/ SAP, siehe Designentscheidungen D-11-1.			akzeptabel
R4 - Softwareentwickler / SAP	23	Identifizierung der Nutzer (direkte Identifizierung) mittels der App		Ja	1	1	4	1	1	1	1	1	1	1	4	DM	Siehe Designentscheidungen (Pseudonymisierung) - D-2.1-2/ D-4.1-3/ D-4.2-3/ D-5-5.			akzeptabel
R4- Betreiber Server (T)	24	Identifizierung der Nutzer (direkte Identifizierung) auf dem CWA-Backend, Verifikation-, TestResult-Servern		Ja	1	1	4	1	1	1	1	1	1	1	4	DM	Siehe Designentscheidung Pseudonymisierung - D-2.1-2/ D-4.1-3/ D-4.2-3/ D-5-5 (Pseudonyme auch auf Backend).			akzeptabel
R4- Apple / Google	25	Erhebung und Speicherung nicht-notwendiger Daten, inklusive Nutzer- und Metadaten durch Apple/ Google (DM)		Ja	3	4	4	0	0	0	0	2	0	4	12	DM, IG, ZB	AVV/ gem. Verantwortung/ Leistungsbeschreibung/ (soweit mgl.), siehe Designentscheidungen D-5.1-1.		Die Grundsatzentscheidung für das Framework von Apple/ Google bedingt das Vertrauen der Nutzer in diese Plattformen, siehe DSFA-Bericht.	bedingt akzeptabel
R4- Betreiber Server (T)	26	Erhebung und Speicherung nicht-notwendiger Daten, inkl. Metadaten (TK-Daten) durch Betreiber Server (T) (DM)		Ja	2	4	4	0	0	0	0	2	0	4	8	DM, IG, ZB	AVV (inkl. TOM) T/ SAP, siehe Designentscheidungen D-11-1.			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	27	Erhebung und Speicherung nicht-notwendiger Daten, inkl. Metadaten (TK-Daten) durch Betreiber CWA (SAP) (DM)		Ja	1	4	4	0	0	0	0	2	0	4	4	DM, IG, ZB	AVV (inkl. TOM) T/ SAP, siehe Designentscheidungen D-11-1.			akzeptabel
	28	**2) Verarbeitung wider Treu und Glauben**																		
R1-CWA-Nutzer	29	Alarmmüdigkeit (mehrmalige Alarmierung inkl. Quarantäne-Empfehlung innerhalb kurzer Zeit) - Nachjustizierung		Ja	2	1	1	1	0	0	0	3	1	4	8	ZB	Siehe Designentscheidungen D-1.2-1.			akzeptabel mit Evaluation
R4- Apple / Google	30	Ungenauigkeit der Kontaktbestimmung		Ja	3	0	0	0	0	0	0	0	0	4	12	ZB	Siehe hierzu die Designentscheidung zur Nutzung der BLE-Technik D-2-5a und D-2.1-1.		Die Grundsatzentscheidung für das Framework von Apple/ Google nebst BLE-Technik führt zu bekannten Ungenauigkeiten. Die Betreiber arbeiten an Optimierungen, wie auch in den Designentscheidungen D-2-7 beschrieben.	bedingt akzeptabel

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse + VT2: Kontaktfall + VT4: Infektfall + Eventregistrierung+Stopp der Warnungen (Stand: 22.05.2023)				Risikobewertung															
						Schadensausmaß													
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R1-CWA-Nutzer	31	Fehlinterpretationen von Aufzeichnungen im Kontakttagebuch	Wenn ein CWA-Nutzer das Kontakttagebuch sehr detailliert pflegt (inklusive Dauer, Maskenstatus und möglichen weiteren Begegnungsdetails) und ihm dann im Kontakt-Tagebuch angezeigt wird, an welchem Tag eine Risikobegegnung stattgefunden hat, dann stehen im Kontakt-Tagebuch der CWA möglicherweise alle notwenigen Informationen zur Verfügung, die zu einer Re-Identifikation einer positiv auf Corona getesteten Person führen könnte. Durch die zusätzliche Anzeige der ab der CWA [Release 1.14] auf Tagesbasis aggregierten Infektionsrisiken im Kontakttagebuch könnte es gelingen, die Wahrscheinlichkeit zu erhöhen "richtige Hypothesen" bezüglich möglicher Corona-Risiken an bestimmten Orten oder bezüglich möglicher Corona-Infektionen von Einzelpersonen zu treffen. Diese verbesserten Hypothesen können dazu führen, das es dem CWA-Nutzer ermöglicht wird, in der CWA App einen anderen Nutzer einfacher bzw. präziser zu re-identifizieren. Fehlinterpretationen können aber zu Diskriminierungen der als „Infektionsherd" ausgemachten Personen führen.	Ja	3	2	2	2	1	1	1	2	2	2	6	DM, VT, IG, IV, TR, ZB	Aufklärung der CWA-Nutzer über die Grenzen der Aussagekraft der möglichen Aufzeichnungen und Rückschlüsse auf positiv getestete Personen			akzeptabel mit Evaluation
R1-CWA-Nutzer	32	[Release 2.20] Verwirrung durch Verkürzung der Anzeigezeit des erhöhten Kontaktrisikos	Mit [Release 2.20] wird die Anzeigezeit der roten Kachel für ein erhöhtes Kontaktrisiko in der CWA-App von 14 auf 10 Tage reduziert. Die Zeiträume für Kontakttagebuch und Event Check-Ins bleiben von dieser Änderung jedoch unberührt. Diese Diskrepanz könnte beim CWA-Nutzer zu Verwirrungen führen, z.B. wenn die rote Anzeige für ein in der CWA-App registriertes Kontaktrisiko bereits nach 10 Tagen verschwindet, gleichzeitig jedoch noch die dazugehörigen Einträge im Kontaktagebuch 4 Tage länger einzusehen sind.	Ja	1	2	1	1	1	1	1	1	2	2	2	DM, TR, ZB				akzeptabel
R1-CWA-Nutzer	33	Vortäuschen positiver Testergebnisse (im "Standard-Verfahren", ohne teleTAN)		Ja	1	0	0	0	0	4	0	4	4	4	4	TR, IV, ZB	Bewertung aus Threat Modelling, AVV mit DL, inkl. TOM Designentscheidung D-11-1.			akzeptabel
R2- Hacker	34	Vortäuschen von Kontaktereignissen durch Duplizierung von BLE-Beacons		Ja	3	o	0	0	3	0	3	0	0	0	9	VF, R	Designentscheidung zur Nutzung der BLE-Technik erzeugte Schwachstelle, Designentscheidungen B-2-3.			akzeptabel mit Evaluation
R6 - Krimineller	35	Vortäuschen von Kontaktereignissen durch Duplizierung von BLE-Beacons in bewusster Zusammenarbeit mit infizierter Person		Ja	2	0	0	0	3	0	3	0	0	4	8	VF, R, ZB	Designentscheidung zur Nutzung der BLE-Technik erzeugte Schwachstelle, Designentscheidungen B-2-3.			akzeptabel mit Evaluation
R6 - Krimineller	36	Herstellung mutwilliger, massenhafter Kontakte durch positiv Getestete (infolge Fehlverhalten Nichtbeachtung Quarantäne-Empfehlung) vor Upload des Testergebnisses zur Verbreitung der Kontakte (z.B. Schulschließungen provozieren)		Ja	3	0	0	0	3	0	3	3	3	3	9	ZB, IV , TR, VF, R	Designentscheidung zur Nutzung der BLE-Technik erzeugte Schwachstelle, Restrisiko.			akzeptabel mit Evaluation
R4- Betreiber Server (T)	37	Auftreten von Sicherheitslücken und Datenschutzvorfällen bei App-Betreiber und/ oder Serverbetreiber (Vertrauensverlust der Bevölkerung in Vertrauenswürdigkeit der CWA und IT-Infrastruktur)		Ja	1	0	0	0	0	0	0	0	0	4	4	ZB, DSMS/ ISMS	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen D-11-1).			akzeptabel
R4 - Softwareentwickler / SAP	38	Unzureichende Anpassung der CWA an die Änderung der Risikoermittlung im ENF (ab Version 2.0 des ENF)	Die Risikoermittlung für eine erfolgte Begegnung wird in Version 2 des ENF grundlegend umgestellt. Das Transmission-Risk wird in Zukunft nicht mehr in die dafür erforderlichen Berechnungen einfließen; stattdessen wird eine grobe Einschätzung der Infektiosität herangezogen, die auf den Days Since Onset of Symptoms (DSOS) beruht. Wenn die Prozesse und Funktionen der CWA nicht, nicht ausreichend oder nicht rechtzeitig an das geänderte ENF angepasst werden, kann es zu fehlerhaften Risikoermittlungen oder zu Funktionsausfällen der CWA-App kommen.	Ja	1	0	0	0	3	0	3	0	0	3	3	VF, R, ZB	Designentscheidung D-2-1 und DSK-Rahmenkonzept Kap. 14.20. Um die CWA auf diese Umstellung vorzubereiten, publiziert der CWA-Server die Positivschlüssel der positiv auf Corona getesteten Nutzer sowohl mit dem Transmission Risk als auch DSOS und Report_type als Attributen. Während die CWA-App in kurzer Zeit aktualisiert und an die Veränderungen im ENF angepasst werden kann, haben die Positivschlüssel auf dem CDN eine Lebensdauer von zwei Wochen. Um eine ununterbrochene Funktionsfähigkeit der CWA zu gewährleisten, war es daher erforderlich, die Attribute DSOS und Report_type im Positivschlüssel bereits vorzeitig bereit zu stellen. Umgekehrt kann auf das Attribut Transmission Risk nach erfolgter Umstellung nicht sofort verzichtet werden, weil die CWA-Nutzer auf Grund von Abhängigkeiten zur Betriebssystemversion ihres mobilen Endgerätes nicht alle unmittelbar auf das neueste Release der CWA-App bzw. die neueste Version des ENF updaten können. Es müssen daher beide Informationen für einen gewissen Übergangszeitraum, der vom Verhalten der CWA-Nutzer abhängt, vorgehalten werden. Somit wird dem Risiko einer eingeschränkten Verfügbarkeit der CWA infolge der von den Firmen Google und Apple initiierten Veränderungen im ENF durch die vorübergehende Bereitstellung des Transmission Risk in doppelten Datenstrukturen vorgebeugt.			akzeptabel
R1-CWA-Nutzer	39	Unrichtige/ falsche Warnung durch vorgetäuschte Eventregistrierung	Ein Angreifer könnte sich zu möglichst vielen Events/ Lokationen registrieren, an denen er gar nicht teilgenommen hat, um im Falle einer eigenen Infektion möglichst viele Personen zu warnen.	Ja	3	1	3	3	1	1	1	3	1	3	9	VT, IG, IV, ZB	Designentscheidungen zur Eventregistrierung (D-2-1a, D-2-2d, D-5.1-15a, D-6-2d, D-9-8a). Die datensparsame Lösung wandelt Check-Ins des Nutzers in Warungen um und kann nicht verifizieren, ob der Benutzer die entsprechende Veranstaltung eines Check-Ins tatsächlich besucht hat.			akzeptabel mit Evaluation
R1-CWA-Nutzer	40	Unrichtige Warnung durch System-Missbrauch (vorgetäuschter Event-Besuch)	Die vorgeschlagene Lösung wandelt Check-Ins des Benutzers in Warnungen um und kann nicht verifizieren, ob der Benutzer die entsprechende Veranstalter eines Check-Ins tatsächlich besucht hat. Ein Angreifer könnte bestimmte Veranstaltungen ansprechen, indem er den entsprechenden QR-Code erhält und einen Check-In vornimmt. Erhält der Angreifer auch die Berechtigung, die Check-Ins beim CWA-Server einzureichen, würden für diese Veranstaltungen falsche Warnungen ausgegeben. Das Szenario dieses Angriffs wird von der Schwierigkeit geprägt, die Genehmigung zum Einchecken zu erhalten. Dies ist derzeit nur mit einem bestätigten positiven Test für SARS-CoV-2 oder durch Erhalt einer TeleTAN von der Hotline möglich. Während ein bestätigter positiver Test schwierig zu erlangen ist, ohne sich selbst in Gefahr zu setzen, kann eine gültige Tele TAN z.B. durch Social Engineering erzielt werden.	Ja	3	1	3	3	1	1	1	3	1	3	9	VT, IG, IV, ZB	Designentscheidungen zur Eventregistrierung (D-2-1a, D-2-2d, D-5.1-15a, D-6-2d, D-9-8a). Die datensparsame Lösung wandelt Check-Ins des Nutzers in Warungen um und kann nicht verifizieren, ob der Benutzer die entsprechende Veranstaltung eines Check-Ins tatsächlich besucht hat.			akzeptabel mit Evaluation
R1-CWA-Nutzer	41	Bekanntmachung von Corona-Hotspots im Rahmen Eventregistrierung	Ein Angreifer könnte versuchen, Hotspots, an denen es häufig zu Infektionen kommt, öffentlich bekannt zu machen. Hierzu braucht ein Nutzer einerseits die Event-IDs, die über das CDN veröffentlicht werden, und zusätzlich die passenden QR-Codes, um zu der Event-ID den Titel/ Ort des Events/ Lokation zu ermitteln.	Ja	3	3	3	1	1	1	1	3	1	3	9	DM, VT, IG, IV, ZB	Designentscheidungen zur Eventregistrierung (D-2-1a, D-2-2d, D-5.1-15a, D-6-2d, D-9-8a). Eine Mitigierung dieses Risikos ist nach derzeitigem Stand nicht möglich. Um eine effektive Warnung auch über die CWA hinaus zu ermöglichen, sollte die Lokation/ Event auch nicht verschleiert werden.			akzeptabel mit Evaluation
R1-CWA-Nutzer	42	Verbreitung von Falschinformationen nach Einscannen von Event-QR-Codes und Austausch der QR-Codes / Anmeldung zum falschen Event	Beim Einscannen des Event-QR-Codes durch den CWA-Nutzer wird ihgm während des Einscan-Prozesses die Eventbeschreibung angezeigt (Grund: Feedback zum Nutzer, ob es sich zum richtigen Event anmeldet), diese Funktion könnte missbraucht werden.	Ja	3	1	3	3	3	1	3	3	3	3	9	VT, IG, VF, RE, IV, TR, ZB	Designentscheidungen zur Eventregistrierung (D-2-1a, D-2-2d, D-5.1-15a, D-6-2d, D-9-8a).			akzeptabel mit Evaluation
R1-CWA-Nutzer	43	Verbreitung der QR-Codes über das Internet	Ein QR-Code könnte fotografiert und über das Internet verbreitet werden. CWA-Nutzer, die sich zu dem Event korrekterweise eingetragen haben, könnten so von anderen Nutzer eine Warnung erhalten, die nicht an dem Event teilgenommen haben.	Ja	3	3	3	1	1	1	1	3	1	3	9	DM, VT, IV, ZB	Designentscheidungen zur Eventregistrierung (D-2-1a, D-2-2d, D-5.1-15a, D-6-2d, D-9-8a).			akzeptabel mit Evaluation
R1-CWA-Nutzer	44	[Release 2.12] Fehlinterpretationen von Sicherheitshinweis "Gerootetes Gerät" in der CWA-App	Durch die Anzeige der Warnungen mit CWA [Release 2.12] auf Android Geräten, dass ein gerootetes Gerät genutzt wird, könnten Nutzer verschreckt/ verunsichert werden und die App nicht mehr nutzen, da sie fälschlicherweise vermuten, das Problem hinge mit der CAW-App zusammen (und nicht mit dem Gerät/ Betriebssystem, welches sie nutzen). Andererseits könnten sich Nutzer fälschlicherweise in Sicherheit fühlen, kein ge-rootetes Gerät zu nutzen, obwohl das „rooten" durch die Library nur nicht erkannt wurde: https://blog.ctdefense.com/how-to-bypass-rootbeers-root-detection/	Ja	1	1	1	1	1	1	1	1	1	1	1	VF	Designentscheidungen a.) (B-6-2), Kommunikation über den Aussagegehalt des Sicherheitshinweises/ FAQ-Eintag.			akzeptabel

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse + VT2: Kontaktfall + VT4: Infektfall + Eventregistrierung+Stopp der Warnungen (Stand: 22.05.2023)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R1-CWA-Nutzer	45	[Release 2.16] Deaktivierung der CWA-Nutzer-Benachrichtigung (rooted Device)	Sofern es einem Angreifer gelingen sollte, auf dem Handy eines CWA-Nutzers eine App zu installieren, die das Smartphone des Nutzers rooted, dann kann der Angreifer das neue Feature zur Unterdrückung von Warnhinweisen (das, dass Gerät genootet wurde) bis zum nächsten Update der App dazu nutzen, den CWA-Nutzer in der Zeit zwischen dem "rooting" bis zum nächsten Update der CWA-App durch einen Vollzugriff auf das Smartphone auszuspionieren. Solch eine Angriff wäre für den CWA-Nutzer nicht erkennbar und er würde sich in „falscher Sicherheit" wiegen, weil er auf die vollständige Erkennung von gerooteten Smartphones durch die CWA vertraut. Die Dauer des Angriffs könnte vom Angreifer dadurch verlängert werden, dass er das CWA-Update für den Nutzer durchführt und die erneute Warnung vor dem Rooten durch die CWA-App ebenfalls unterdrücken lässt.	Ja	2	1	3	1	1	1	1	1	1	3	6	VT, ZB	Mitigation nicht möglich. Hinweis in den FAQ, dass Warnungen zu Root-Berechtigungen ab dem [Release 2.16] bis zum nächsten Update der CWA-App unterbunden werden können. Restrisiko bleibt somit bestehen.			akzeptabel mit Evaluation
	46	**3) Für die Betroffenen intransparente Verarbeitung**													27					
R8- Behörden	47	Unvollständige, unverständliche Datenschutzinformationen für CWA-App und Backend (inkl. Funktionalitäten der CWA)	Release 3.1: Möglicherweise könnten die DSE noch über die DV mittels EFGS informieren, obwohl das EFGS bereits abgeschalten wurde. Das Risiko für den Betroffenen beschränkt sich auf die Information. Eine intransparente Datenverarbeitung ist damit nicht betroffen.	Ja	1	2	2	2	0	0	0	3	4	4	4	TR, ZB	Abgestimmte Datenschutzinformationen liegen vor (DSK Verifikation und Testergebnis, 9.1 (mitgeltende Dokumente Datenschutzerklärung)). Eine Anpassung sollte zeitnah nach Abschaltung von Funktionalitäten erfolgen. Ausgeschlossen sein sollte der Fall, dass die Information über eine DV in B			akzeptabel
R1-CWA-Nutzer	48	Unvollständige, unverständliche DSI für Kontaktpersonen bei Nutzung des KTB	Verantwortlicher CWA-Nutzer stellt seinen Kontakten nicht die hinreichenden Informationen nach Art. 13 DSGVO zur Verfügung, hinsichtlich der DV im KTB und auch bzgl. der Weiterleitung an GA im Infektionsfall. Das Schadensausmaß für Kontaktpersonen könnte sich durch die mit der CWA [Release 1.14] erfolgten Erweiterung der Attribute inkl. Freitextfeld erhöhen; eine vollständige Information wird komplexer.	Ja	3	3	3	3	0	0	0	3	3	3	6	TR, ZB	Designentscheidungen zur Einführung des KTB (siehe Anlage 1 zum DSFA-Bericht: D-2-2b, D-6-2c, D-5-11, D-9-8, D-7-10), DSK-Rahmenkonzept 14.27.17.			akzeptabel mit Evaluation
R8- Behörden	49	Unvollständige, unverständliche Datenschutzinformationen für API/ ENF		Ja	2	2	2	2	0	0	0	3	4	4	8	TR, ZB	Abgestimmte Datenschutzinformationen liegen vor (DSK Verifikation und Testergebnis, 9.1 (mitgeltende Dokumente Datenschutzerklärung)).			akzeptabel mit Evaluation
R4- Betreiber Server (T)	50	Gefahr der Intransparenz und fehlenden Prüfbarkeit der verarbeiteten Daten mittels der Server und Komponenten in der OTC		Ja	3	0	0	0	0	0	0	2	3	1	9	TR, ZB	Abgestimmte Datenschutzinformationen liegen vor (DSK Verifikation und Testergebnis, 9.1 (mitgeltende Dokumente Datenschutzerklärung)).			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	51	Gefahr der Intransparenz und fehlenden Prüfbarkeit der verarbeiteten Daten und Funktionsweise der CWA		Ja	2	0	0	0	0	0	0	2	3	1	6	T R	Datenschutzinformationen und Informationen auf GitHub			akzeptabel mit Evaluation
R4- Apple / Google	52	Gefahr der Intransparenz und fehlenden Prüfbarkeit der verarbeiteten Daten und Funktionsweise der ENF		Ja	3	1	1	1	1	1	1	3	3	1	9	T R, IV	Designentscheidungen D-11-2.			akzeptabel mit Evaluation
R8- Behörden	53	[Release 3.2]: Intransparente Datenverarbeitung im Zusammenhang mit der Einstellungen von Warnungen	Für den CWA-Nutzer ist nicht erkennbar, dass die Warnungen mittels PoC und Labor (PCR-Tests) ab dem 20.4. nicht mehr in der CWA angezeigt werden können und ab diesem Zeitpunkt auch keine Test DCC mehr in die CWA übertragen werden können.	Ja	3	2	0	0	0	2	0	0	2	0	6	DM, TR, VF, ZB		Datenschutzrechtlich relevante Information werden in der DSE ausgeführt.		akzeptabel mit Evaluation
	54	**4) Unbefugte Offenlegung von und Zugang zu Daten**																		
R1-CWA-Nutzer	55	(Bewusste/ unbewusste) Erteilung von Berechtigungen an Google/ Apple/ andere App-Anbieter auf Smartphone		Ja	1	4	4	4	0	0	0	2	4	4	4	DM, VT, IG, TR, ZB	Sicherheitseinstellungen im Rahmen der Handynutzung/ Restrisiko beim Nutzer - Designentscheidung D-2-2.			akzeptabel
R1-CWA-Nutzer	56	Bewusste/ unbewusste Erteilung von nicht-notwendigen Berechtigungen an CWA-Betreiber		Ja	1	4	4	4	0	0	0	2	4	4	4	DM, VT, IG, TR, ZB	Sicherheitseinstellungen im Rahmen der Handynutzung/ Restrisiko beim Nutzer - Designentscheidung D-2-2.			akzeptabel
R1-CWA-Nutzer	57	Unbewusste Offenlegung von Kontakteinträgen in KTB (Shoulder Surfing)	Unbefugte Dritte könnten durch einen Blick über die Schulter des CWA-Nutzers während des Eintragens Kenntnis von personenbezogenen Daten der Kontakte erhalten. Ab [Release 1.12]: Zufällig könnte eine Risikobegegnung einer bestimmten Person zugeordnet werden. Das Risiko erhöht sich mit CWA [Release 1.14] sowie CWA [Release 2.4], da weitere Attribute hinzugefügt werden können.	Ja	3	3	3	3	1	1	1	3	3	3	9	VT, IG, ZB	Designentscheidungen zur Einführung des KTB (siehe Anlage 1 zum DSFA-Bericht: D-2-2b, D-6-2c, D-5-11, D-9-8, D-7-10), DSK-Rahmenkonzept 14.27.17.			akzeptabel
R1-CWA-Nutzer	58	Bewusste Offenlegung von KTB an (unbefugte) Dritte (Nutzung der Exportfunktion)	CWA-Nutzer könnten ohne Wissen der Betroffenen die Exportfunktion nutzen, um Daten zu Kontakten unbefugt und unrechtmäßig an Dritte zu übermitteln. Der empfangende Dritte könnte die Daten auf rechtswidrige Weise/ unbefugte Weise (z.B. unzureichende TOM auf Seiten des Empfängers, unzulässige Verarbeitungszwecke wie bspw. Veröffentlichen der Daten durch Privatpersonen über soziale Netzwerke usw.) erlangen. Ebenso könnte der CWA-Nutzer die Exportfunktion (E-Mail) nutzen, ohne diese nach Stand der Technik gegen unbefugten Zugriff zu schützen (Verschlüsselung). Ab [Release 1.12]: Durch Einführung der Begegnungshistorie ist präzisere Info mgl. (nicht mehr lediglich 14 Tage Zeitraum (+heutigem Tag), sondern Risiko wird bestimmten Tagen zuordenbar übertragen). Ab [Release 1.14] können weitere Daten übertragen werden, ggf. ohne dass die Kontaktperson davon Kenntnis hat [(E-Mail, Tel.Nr. der Kontaktperson + die Begegnungsdauer, die Begleitumstände (Freitextfeld), sowie weiterführende Informationen, die für die Beurteilung eines möglichen Infektionsrisikos relevant sind (drinnen/draußen; mit/ohne Maske; Dauer der Begegnung)].	Ja	3	3	4	3	1	1	1	3	3	4	12	VT, IG, T, ZB	Designentscheidungen zur Einführung des KTB (siehe Anlage 1 zum DSFA-Bericht: D-2-2b, D-6-2c, D-5-11, D-9-8, D-7-10), DSK-Rahmenkonzept 14.27.17.	Möglicherweise prüfen: Beschränkung der Exportfunktion auf Fälle, in denen positives Testergebnis vorliegt.		bedingt akzeptabel; Informationskampagne
R2- Hacker	59	Zugang/ Zugriff trotz fehlender und unzureichender Berechtigungen zu Smartphone/ CWA/ ENF/ inkl. Elevation of Privilege (Ausweiten der Rechte)		Ja	2	4	4	4	0	0	0	2	4	4	8	DM, VT, IG, TR, ZB	Empfehlungen im Rahmen der Handynutzung/ Designentscheidungen (Containerisierung CWA - Designentscheidung D-2-2).			akzeptabel mit Evaluation
R4- Apple / Google	60	Unbefugter Zugriff von Plattformen, die Kontaktereignisse ermitteln, auch für Nutzer ohne CWA		Ja	3	4	4	4	0	0	0	2	4	4	12	DM, VT, IG, TR, ZB	Dokument Designentscheidungen - Designentscheidungen zur Nutzung API und ENF (siehe Designentscheidungen, D-6-3) - für Phase 2 angekündigt.		Von Google/ Apple ist dies für die Phase 2 des ENF angekündigt. Wie dies implementiert wird, ist daher unklar. Es ist aber davon auszugehen, dass sich an dem Einwilligungserfordernis nichts ändern wird.	bedingt akzeptabel,
R4- Apple / Google	61	Zugang/ Zugriff zu Gesundheitsdaten (Infektionsstatus) trotz fehlender Berechtigungen zu CWA durch Google/ Apple (über API/ ENF) (Datenabfluss an Google/ Apple)		Ja	3	4	4	4	0	0	0	2	4	4	12	DM, VT, IG, TR, ZB	Dokument Designentscheidungen - Designentscheidungen zur Nutzung API und ENF (siehe Designentscheidungen, D-6-3) und Datenabfluss (Designentscheidungen D-5-3-1).		Die Grundsatzentscheidung für das Framework von Apple/ Google bedingt das Vertrauen der Nutzer in diese Plattformen.	bedingt akzeptabel,
R2- Hacker	62	Zugang/ Zugriff auf (Gesundheits-) Daten in CWA-Backend (z.B. Infolge der Nutzung einfacher Passwörter, fehlender IT-Sicherheit)		Ja	2	1	2	2	2	0	0	0	0	3	6	ZB	Vereinbarung AVV mit DL und TOM OTC (Designentscheidungen D-11-1).			akzeptabel mit Evaluation
R2- Hacker	63	Datenzugang durch Reverse Engineering (Angreifer führt R.E. auf die CWA durch und ermittelt dadurch ungeschützte Datenstrukturen)		Ja	1	0	3	3	0	0	0	0	0	0	3	VT, IG	Risikobewertung nach Threat Modelling (Gegenmaßnahme: Verschlüsselte Speicherung im Smartphone); Designentscheidung D-5.1-6.			akzeptabel
R2- Hacker	64	Zugang/ Zugriff auf Gesundheitsdaten/ Infektionsstatus durch Überwachung des WiFi-/ Internetverkehrs (Kommunikation zwischen CWA und CWA-Server) - Eavesdropping (ohne Dummyrequests)		Ja	3	1	3	3	2	0	0	0	0	3	9	ZB , VT, IG	Designentscheidungen/ TOM (Verschlüsselung Transportweg innerhalb der IT-Infrastruktur und zu CWA) - D-4.1-11 (ohne Dummyrequests).			akzeptabel mit Evaluation
R2- Hacker	65	Zugang/ Zugriff auf Gesundheitsdaten/ Infektionsstatus durch Re-Identifizierung von infizierten Nutzern durch Analyse der publizierten Positivschlüssel und Zusatzinformationen außerhalb der CWA (nach Implementierung Dummyschlüssel) (ohne Berücksichtigung Angaben zum Symptombeginn)		Ja	2	1	3	3	2	0	0	0	0	3	6	ZB , VT, IG	Siehe Designentscheidungen D-5.1-11c/ D-5.1-15 und 16. Auffüllen der zum Download bereitgestellten Schlüsselpakete mit Dummy-Schlüsseln, wenn nicht genügend Positivschlüssel von Nutzern zur Verfügung stehen, Designentscheidung D-5.1-5a, DSK, Rahmenkonzept Kap. 14.8.			akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse + VT2: Kontaktfall + VT4: Infektfall + Eventregistrierung+Stopp der Warnungen (Stand: 22.05.2023)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R2- Hacker	66	Zugang/ Zugriff auf Gesundheitsdaten/ Infektionsstatus durch Re-Identifizierung von infizierten Nutzern durch Analyse der publizierten Positivschlüssel und Zusatzinformationen außerhalb der CWA (ohne Verwendung von Dummyschlüsseln, bei Implementierung einer strikten Mindestgröße) (ohne Berücksichtigung Angaben zum Symptombeginn)		Ja	1	1	3	3	2	0	0	0	0	3	3	ZB, VT, IG		Mit der Zunahme an verfügbaren Metadaten der Positivschlüssel im Zuge der Weiterentwicklung der CWA erscheint es angeraten, die oben beschriebene Mindestpaketgröße für Positivschlüssel in Zukunft (durch das RKI) konfigurierbar zu gestalten.		akzeptabel
R2- Hacker	67	Zugang/ Zugriff auf Gesundheitsdaten/ Infektionsstatus durch Re-Identifizierung von infizierten Nutzern durch Analyse der publizierten Positivschlüssel und Zusatzinformationen außerhalb der CWA (ohne Verwendung von Dummyschlüsseln, bei Implementierung einer strikten Mindestgröße) (unter Berücksichtigung Angaben zum Symptombeginn) infolge der Änderung der Risikoermittlung im ENF (ab Version 2.0 des ENF)	Die Risikoermittlung für eine erfolgte Begegnung wird in Version 2 des ENF grundlegend umgestellt. Das Transmission Risk wird in Zukunft nicht mehr in die dafür erforderlichen Berechnungen einfließen; stattdessen wird eine grobe Einschätzung der Infektiosität herangezogen, die auf den Days Since Onset of Symptoms (DSOS) sowie dem Report Type beruht. Um die gewohnte Genauigkeit der Risikoermittlung auch in Version 2 des ENF aufrechtzuerhalten, führt die CWA-App basierend auf den Vorarbeiten des ENF eine eigene Risikoberechnung durch und greift nicht auf vom Betriebssystem errechnete Risikowerte zurück. Um der CWA-App den Zugang auf das einem Positivschlüssel zugewiesene Transmission-Risk zu ermöglichen, wird dieses mit Hilfe der Datenfelder Days Since Onset of Symptoms (DSOS) und Report Type dargestellt. Diese Zusatzinformationen werden ab der Umstellung der Risikoermittlung teilweise veröffentlicht, so dass diese Zusatzinformationen zur Re-Identifizierung eines Nutzers herangezogen werden könnten.	Ja	1	1	4	3	2	0	0	0	0	4	4	ZB, VT, IG		DSK_Rahmendokument Kap. 14.8: Die auf den CWA-Server geladenen Positivschlüssel enthalten Informationen über das Ansteckungsrisiko des infizierten Nutzers an dem Tag, für den der jeweilige Schlüssel Gültigkeit hat. Dieses sogenannte Transmission-Risk wurde von Epidemiologen auf Grund mathematischer Modelle sorgfältig errechnet. Wie im Datenschutzkonzept der CWA-App beschrieben wird es in Abhängigkeit vom durch den Nutzer angegebenen Symptombeginn oder - bei Fehlen einer solchen Angabe - in Abhängigkeit vom Tag des Ladens auf den CWA-Server bestimmt. Beim Symptombeginn handelt es sich um ein Datum oder den Zeitraum des Einsetzens von Krankheitssymptomen. Durch diese Berechnung ergeben sich für die Positivschlüssel eines Nutzers verschiedene Muster von Transmissio-Risks, die von Außenstehenden zur Gruppierung der durch den CWA-Server veröffentlichten Positivschlüssel herangezogen werden können. Deshalb ist es für einige der Positivschlüssel möglich, aus dem Tag der Gültigkeit des Schlüssels und dem Transmission-Risk auf die Angaben des dahinterstehenden Nutzers zu seinem Symptombeginn zu schließen. Außerdem kann so eine Schätzung für die Anzahl der positiv getesteten Personen abgeleitet werden, die ihre Positivschlüssel auf den CWA-Server geladen haben. Weitergehende Schlüsse können jedoch nicht getroffen werden.	Mit der Zunahme an verfügbaren Metadaten der Positivschlüssel im Zuge der Weiterentwicklung der CWA erscheint es angeraten, die oben beschriebene Mindestpaketgröße für Positivschlüssel in Zukunft (durch das RKI) konfigurierbar zu gestalten.		akzeptabel
R2- Hacker	68	Abhören des Bluetooth-Verkehrs		Ja	2	1	2	2	0	0	0	2	2	2	4	VT, ZB , TR	Siehe Designentscheidungen zur Nutzung der BLE-Technik, Risiken werden weiter betrachtet, mit dem Ziel, die Technik onangreifbarer zu machen, Schwachstellen zu minimieren (B-4-2).			akzeptabel
R2- Hacker	69	Zugriff auf Positiv-Schlüssel; TEK beim CWA-Server, Rückrechnung RPI und Vortäuschen von Kontakten mit Infizierten (mit Vorwissen) (Vortäuschen falscher Kontakte)		Ja	2	1	1	1	1	1	1	1	1	4	8	ZB	TOM/ Zugangssicherung + Designentscheidungen (Verschlüsselung auf Transportwegen) - Designentscheidungen B-4-1.			akzeptabel mit Evaluation
R2- Hacker	70	Zugriff auf Positiv-Schlüssel, Rückrechnung RPI und Nachbau ENF mit z.B. Ortungsdaten angereichert, um Kontakte mit infizierten Personen zu tracken (Re-Identifizierung und Tracking als Missbrauch der Daten durch Dritte) Mashed App		Ja	1	3	1	0	0	0	0	0	0	3	3	VT, ZB, IG	TOM/ Zugangssicherung + Designentscheidungen (Verschlüsselung auf Transportwegen) - Designentscheidungen B-4-1.			akzeptabel
R2- Hacker	71	Zugriff auf Positiv-Schlüssel, Rückrechnung RPI und Nachbau ENF mit z.B. Ortungsdaten angereichert, um Kontakte mit infizierten Personen zu tracken (Re-Identifizierung und Tracking als Missbrauch der Daten durch Dritte) Einzel App		Ja	3	3	1	0	0	0	0	0	0	3	9	DM, VT, ZB, IG	TOM/ Zugangssicherung + Designentscheidungen (Verschlüsselung auf Transportwegen) - Designentscheidungen B-4-1.			akzeptabel mit Evaluation
R2- Hacker	72	Unbefugte Offenlegung durch Metadaten-Korrelation		Ja	2	0	4	4	0	0	0	0	0	4	8	ZB	Designentscheidungen/ TOM/ Threat Modeling/ Korrelation verhindern durch Trennung von Meta- und Nutzdaten/ Keine TAN - Speicherung auf Verifikation Server .			akzeptabel mit Evaluation
R2- Hacker	73	Verknüpfung von Metadaten (speziell EFGS) (EFGS-Risiko)	Nicht-autorisierte Reidentifikation eines Betroffen durch die Kombination verfügbarer Metadaten. Durch die Auswertung von Mustern der Daten des relevanten-Länder-Feldes kann es möglich sein, folgende Informationen zu ermitteln: 1. relevante Länder, die einen Bezug zu einem Schlüssel aufweisen, 2. Ursprungsland des Schlüssels, 3. Heatmap: Die Bürger welches Mitgliedsstaates reisen in welche anderen Mitgliedsstaaten (statistische Daten). Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	3	3	0	0	0	0	3	0	3	3	DM, VT, IV, ZB	Risiko hat keine Relevanz für CWA: Siehe Designentscheidungen D-6-2b: Liste von Ländern, mit denen die Tagesschlüssel über das EFGS verteilt werden, entspricht ab [Release 1.5] immer allen Ländern, die über die Konfiguration als „Unterstützte Länder" bereitgestellt werden. Eine Auswahl durch den CWA-Nutzer, mit welchen Ländern Schlüssel geteilt werden, erfolgt ebenso wenig, wie eine Angabe von Ländern, für die sich der CWA-Nutzer interessiert.			akzeptabel
R2- Hacker	74	Verknüpfung von Metadaten im Zusammenhang mit Schweizer Gateway	Analog der Risikobeschreibung in Z 66, könnte die Re-Identifikation durch Länderauswahl auf Seiten der Schweiz ermöglicht werden. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	3	3	0	0	0	0	3	0	3	3	DM, VT, IV, ZB	Risiko hat aktuell keine Relevanz für CWA. Schweizer Gateway "kopiert" EFGS. Konfiguration durch die Schweiz bleibt jedoch möglich.			akzeptabel
R2- Hacker	75	Offenbarung der Anzahl der relevanten Länder eines Betroffenen, der Daten zur Verfügung stellt (Kodierlänge einer hochgeladenen Zeichenkette); (EFGS-Risiko).	Eine Kodierung des Felds "relevante Länder" als variable Zeichenkette kann zur Offenbarung von Informationen führen, z.B. bezüglich des Reiseverhaltens des Betroffenen auf Grund der Erkennbarkeit der Anzahl der Länder, die der Betroffene als relevant angibt. Betrachtung beschränkt für die CWA. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	1	4	4	0	0	0	4	4	4	4	VT, IG, IV, TR, ZB	Risiko hat keine Relevanz für CWA: Siehe Designentscheidungen D-6-2b: Liste von Ländern, mit denen die Tagesschlüssel über das EFGS verteilt werden, entspricht ab [Release 1.5] immer allen Ländern, die über die Konfiguration als „Unterstützte Länder" bereitgestellt werden. Eine Auswahl durch den CWA-Nutzer, mit welchen Ländern Schlüssel geteilt werden, erfolgt ebenso wenig, wie eine Angabe von Ländern, für die sich der CWA-Nutzer interessiert.			akzeptabel
R2- Hacker	76	Offenbarung der Anzahl der relevanten Länder (Kodierlänge einer hochgeladenen Zeichenkette) im Zusammenhang mit Schweizer Gateway	Analog der Risikobeschreibung in Z 74, könnte die Re-Identifikation durch Offenbarung auf Seiten der Schweiz ermöglicht werden. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	1	4	4	0	0	0	4	4	4	4	VT, IG, IV, TR, ZB	Risiko hat aktuell keine Relevanz für CWA. Schweizer Gateway "kopiert" EFGS. Konfiguration durch die Schweiz bleibt jedoch möglich.			akzeptabel
R2- Hacker	77	Re-Identifikation eines Betroffenen durch die Verknüpfung von Angaben zu relevanten Ländern mit externen Informationen über das Reiseverhalten (EFGS-Risiko).	Das Datenfeld "relevante Länder" kann zur Reidentifikation eines Betroffenen verwendet werden, wenn die Kombination der relevanten Länder hinreichend einmalig ist. Wird diese Information mit weiteren Informationen kombiniert, die außerhalb des Anwendungsbereichs des EFGS gewonnen werden, z.B. durch Fluggesellschaften oder Reisebüros oder statistische Informationen bezüglich der möglichen Ethnie des Betroffenen, können weitere personenbezogene Informationen erschlossen werden. Wenn das Feld Informationen über Länder enthält, die Visa erfordern, kann bei einer hinreichend kleinen Anzahl von Reisenden in diese Länder die Identität des Betroffenen hinter einem Schlüssel diesen Ländern offenbart werden. Betrachtung beschränkt für die CWA. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	1	4	4	0	0	0	4	4	4	4		Risiko hat keine Relevanz für CWA: Siehe Designentscheidungen D-6-2b: Liste von Ländern, mit denen die Tagesschlüssel über das EFGS verteilt werden, entspricht ab [Release 1.5] immer allen Ländern, die über die Konfiguration als „Unterstützte Länder" bereitgestellt werden. Eine Auswahl durch den CWA-Nutzer, mit welchen Ländern Schlüssel geteilt werden, erfolgt ebenso wenig, wie eine Angabe von Ländern, für die sich der CWA-Nutzer interessiert.			akzeptabel
R2- Hacker	78	Nicht-autorisierter Zugriff auf personenbezogene Daten (hier: relevante Länder) durch das Überwachen von Internetverkehr beim Download (EFGS-Risiko).	Das Datenfeld "relevante Länder" kann als URL-Bestandteil eventuell für Dritte beim Download von Daten mittels der App erkennbar sein, wenn die Dritten den Datenverkehr der App geeignet abhören. Betrachtung beschränkt für CWA. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	2	2	2	0	0	0	2	0	2	2		Risiko hat keine Relevanz für CWA: Siehe Designentscheidungen D-6-2b: Liste von Ländern, mit denen die Tagesschlüssel über das EFGS verteilt werden, entspricht ab [Release 1.5] immer allen Ländern, die über die Konfiguration als „Unterstützte Länder" bereitgestellt werden. Eine Auswahl durch den CWA-Nutzer, mit welchen Ländern Schlüssel geteilt werden, erfolgt ebenso wenig, wie eine Angabe von Ländern, für die sich der CWA-Nutzer interessiert.			akzeptabel
R2- Hacker	79	Nicht-autorisierter Zugriff auf personenbezogene Daten (hier: relevante Länder) durch das Überwachen von Internetverkehr beim Download (EFGS-Risiko).	Das Vorliegen von Reisetätigkeit eines Betroffenen an sich kann durch das Herunterladen von Schlüsseln erschlossen werden, wenn die herunterzuladenden Daten aufgeteilt werden, um nicht die Mobiltelefone im Allgemeinen mit dem Download aller Daten vom EFGS zu überlasten. Genauer: Wenn ein Benutzer kürzlich beispielsweise Italien besucht hat, ist es sehr wahrscheinlich, dass sie die mobile Applikation so einstellen, dass die italienischen Schlüssel heruntergeladen werden. Die Größe der heruntergeladenen Datenpakete könnte für die einzelnen Länder unterschiedlich genug sein, so dass aus der Größe der Downloads geschlossen werden kann, welche Datenpakete der Benutzer heruntergeladen hat, z.B. das italienische Datenpaket. Betrachtung beschränkt für CWA. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	2	2	2	0	0	0	2	2	2	2		Risiko hat keine Relevanz für CWA: Siehe Designentscheidungen D-6-2b: Liste von Ländern, mit denen die Tagesschlüssel über das EFGS verteilt werden, entspricht ab [Release 1.5] immer allen Ländern, die über die Konfiguration als „Unterstützte Länder" bereitgestellt werden. Eine Auswahl durch den CWA-Nutzer, mit welchen Ländern Schlüssel geteilt werden, erfolgt ebenso wenig, wie eine Angabe von Ländern, für die sich der CWA-Nutzer interessiert.			akzeptabel
R2- Hacker	80	SQL Injektion (Benutzergenerierte Nachrichten können bösartige SQL-Befehle enthalten)		Ja	1	0	3	3	3	0	0	0	0	4	4	ZB	Einschätzung Threat Modeling (Prüfung, ob Eingabe Validierung für Anwenderdaten) - Designentscheidung B-1-5.			akzeptabel
R1-CWA-Nutzer	81	SQL Injektion wissentlich/ unwissentlich über Tastatur	Mit dem KTB können erstmals Daten über die Tastatur eingegeben werden. Eine SQL-Injektion könnte zum einen zum Verlust der eigenen Daten führen, jedoch könnte auch versucht werden, die Berechtigungen der App zu erweitern.	Ja	1	2	2	2	2	1	2	2	2	2	2	DM, VT, ZB	Als Gegenmaßnahme erfolgt die Inputvalidierung nach dem Stand der Technik.			akzeptabel

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse + VT2: Kontaktfall + VT4: Infektfall + Eventregistrierung+Stopp der Warnungen (Stand: 22.05.2023)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R2- Hacker	82	Code-Injektionsfehler (Injektionsfehler im Verifikation-Server Backend)		Ja	1	0	3	3	3	0	0	0	0	4	4	ZB	Einschätzung Threat Modelling (siehe IT-Sicherheitskonzepte).			akzeptabel
R2- Hacker	83	Transaktionen Hijacking (Abfangen des laufenden Uploads von Diagnoseschlüsseln)		Ja	2	0	2	2	0	0	0	0	0	4	8	ZB	Designentscheidungen/ Threat Modelling/ Einsatz von verschlüsselten Netzwerkverbindungen (siehe Z 61) - TOM: Authentifizierung der Server			akzeptabel mit Evaluation
R4- Betreiber Server (T)	84	Unberechtigter Administratorenzugriff auf Positiv-Schlüssel beim CWA-Backend, Magenta CDN (inkl. Veränderung von Protokolldaten)		Ja	1	0	4	0	0	0	0	4	4	4	4	VT, IV, TR, ZB	AVV, inkl. TOM OTC (Berechtigungskonzept, Zugriffskontrolle, Protokollierung).			akzeptabel
R8-staatl Behörden	85	Unberechtigter Zugriff auf TEK/ Daten der CWA über Crashlogs		Ja	2	4	4	2	0	0	0	4	4	4	8	VT, ZB, T R	siehe Designentscheidungen D-5-3-1 und 2.			akzeptabel mit Evaluation
R2- Hacker	86	Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts- und Zugriffskontrolle ...(TOM) auf dem Smartphone	Update 1.9: Nachdem der CWA Nutzer seine Einwilligung zum Teilen seiner Positivschlüssel auch dem Betriebssystem gegenüber bestätigt hat nimmt die CWA-App die Positivschlüssel des CWA-Nutzers vom ENF entgegen und speichert sie auf dem mobilen Endgerät, bis der CWA-Nutzer seine Eingaben zum Symptombeginn beendet hat und die Positivschlüssel auf den CWA-Server geladen werden können. Durch die vorübergehende, kurzzeitige Zwischenspeicherung der Positivschlüssel auf dem mobilen Endgerät besteht in dieser Zeitspanne grundsätzlich die Möglichkeit, dass ein Angreifer, dem physisch oder über eine Netzwerkverbindung der Zugriff auf das mobile Endgerät des CWA-Nutzer gelingt, in den Besitz der Positivschlüssel des CWA-Nutzers zu gelangen, solange ein Personenbezug noch herstellbar ist. [Release 1.8]: Anfangs hat die CWA-App ihre personenbezogenen Daten auf allen unterstützen Betriebssystemen über die bereits betriebssystemseitig vorhandene Verschlüsselung der Sandbox hinaus mit einem zusätzlichen Mechanismus unter Zuhilfenahme einer betriebssystemnahen Bibliothek verschlüsselt. Dafür wird auf das Schlüsselmanagement des jeweiligen Betriebssystems zurückgegriffen. Allerdings treten bei Android-basierten Endgeräten immer wieder Probleme mit diesem Schlüsselmanagement auf, insbesondere bei konkurrierenden Zugriffen. Dies kann dazu führen, dass betroffene Daten nicht mehr entschlüsselt werden können und die CWA-App in den Ausgangszustand zurückgesetzt werden muss. Dabei gehen die bisher gesammelten Daten der CWA-App verloren (wie z.B. Registration Token, bereits ermittelte Risiken, Konfigurationen), jedoch nicht die des ENF (z.B. Tagesschlüssel oder eigene wie auch fremde PRIs). KTB Diskussion um PIAB, weil Klartext von	Ja	2	4	4	4	4	4	4	4	4	4	8	VT , IG, VF, A, R, IV, TR, ZB, DM	Sicherheitseinstellungen Smartphone/ Verantwortung Nutzer mitigieren auch das Risiko welches in Spalte E [Release 1.9] beschrieben wurde. Zu [Release 1.8]: DSK-Rahmenkonzept v1.8 "pers. Daten auf mob.Endgerät", 14.23 : Die Sicherheitseinstellung (zusätzliche Verschlüsselung) führt bei Android-Geräten mgl.weise zu Datenverlusten. Deshalb wird ab Release 1.8 mit gebotener Sorgfalt schrittweise darauf verzichtet, bis der Hersteller (Google) die Problem behoben hat. Ein Angriff der diese Sicherheitslücke ausnutzt, wird als gering eingeschätzt (schwer realisierbar, hohe technische Kenntnisse und Aufwand erforderlich)".			akzeptabel mit Evaluation
R4- Betreiber Server (T)	87	Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts- und Zugriffskontrolle ...(TOM) für den CWA-Server		Ja	1	4	4	4	4	4	4	4	4	4	4	VT, IG, VF, A, R, IV, TR, ZB, DM	AVV, inkl. TOM OTC.			akzeptabel
R1-CWA-Nutzer	88	Eventregistrierung: Re-Identifikation von CWA-Nutzern/ positiv Getesteten bei kleinen Events IVm KTB	Durch das Hinzufügen von weiteren Informationen zum Kontakt-Tagebuch erhöht sich generell das Re-Identifikationsrisiko. Mit der Einführung der Event-Registrierung wird dem CWA-Nutzer im KTB zudem angezeigt, ob das Event ein niedriges oder ein erhöhtes Infektionsrisiko hat. Diese Information zusammen mit den Informationen aus dem Kontakt-Tagebuch/Gedächtnis des CWA-Nutzers ermöglichen es, bessere Hypothesen bezüglich einer auf Corona positiv getesteten Person aufzustellen.	Ja	4	1	3	1	1	1	1	3	3	3	12	VT, IV, TR, ZB	Designentscheidungen zur Eventregistrierung (D-2-1a, D-2-2d, D-5.1-15a, D-6-2d, D-9-8a).		Datensparsames Design bedingt Vertrauen in die rechtskonforme, angemessene und eventspezifische Nutzung durch CWA-Nutzer + Schutz KTB vor Angriffen von Außen.	bedingt akzeptabel
R1-CWA-Nutzer	89	Eventregistrierung: Re-Identifikation von CWA-Nutzern/ positiv Getesteten durch personalisierten QR-Code	Ein Event-Organisator könnte für jeden Teilnehmer einen individuellen QR-Code erstellen, der jeweiligen Person bei seinem Event vorzeigen und sie bitten, diesen QR-Code in der CWA-App als vermeidliches Gruppen-Event einzuscannen. Der Organisator fügt sich anschließend selbst zu allen erstellten Events hinzu und wartet auf die Ergebnisse. Wenn jetzt ein CWA-Nutzer positiv getestet wird und seine Schlüssel und Check-Ins teilt, kann der Event-Organisator innerhalb der CWA-App direkt sagen, wer positiv auf Corona getestet wurde.	Ja	4	1	3	1	1	1	1	3	3	3	12	VT, IV, TR, ZB	Siehe Designentscheidung D-2-2d und DSK Rahmenkonzept 2.0 (Ob die CWA-App wie geplant vor möglichen Infektionsrisiken im Rahmen von Veranstaltungsbesuchen warnen kann, hängt davon ab, dass die erzeugten QR-Codes eventspezifisch eingesetzt und korrekt erzeugt werden).		Datensparsames Design bedingt Vertrauen in die rechtskonforme, angemessene und eventspezifische Nutzung durch CWA-Nutzer	bedingt akzeptabel
R2- Hacker	90	Eventregistrierung: Re-Identifikation/ User-Tracking mittels Erzeugung einer Geo-Location Datenbank	Ein Angreifer könnte eine Geo-Location Datenbank aufsetzten, die bestimmte Events auf eine Geo-Lokation mappt. Durch sehr niedrige Fallzahlen in einem Gebiet könnte es so zu einem Tracking der CWA-Nutzer kommen. Es könnten vielleicht sogar Bewegungsprofile erzeugt werden.	Ja	1	3	3	1	1	1	1	3	3	3	3	DM, VT, IV, TR, ZB	Designentscheidung D-5.1-15a.			akzeptabel
R2- Hacker	91	Eventregistrierung: Re-Identifikation eines Nutzers durch das Hochladen seiner Positivschlüssel mit den Event-Check-Ins in einem Paket (Überwachung des Netzverkehrs)	Beim Hochladen der Positivschlüssel zum CWA-Server werden mit [Release 2.0] auch die Event-CheckIn-IDs (keine UserIDs) hochgeladen. Damit besteht das Paket aus den Positivschlüsseln, den CheckIn-IDs und Metadaten. Es besteht die Möglichkeit, dass ein Angreifer durch Überwachung des Netzverkehrs anhand der Paketgröße darauf schließt, dass ein CWA-Nutzer gerade seine Positivschlüssel geteilt hat. Somit könnte der Angreifer einen CWA-Nutzer als positiv getestet identifizieren. [Release 2.8]: Sofern ein CWA-Nutzer eine ältere CWA App Version (<=2.7) nutzt und seine Event-IDs teilt, ist es möglich, anhand der versendeten Netzwerk-Pakete festzuzustellen, ob ein CWA-Nutzer seine Event-IDs in der ursprünglichen Form der Event Registrierung geteilt hat oder nicht. Weil vermutlich viele Nutzer auf die neue Version der CWA App (>2.7) wechseln werden, kann angenommen werden, dass es nur wenige CWA App's mit einer Version (<= 2.7) geben wird. Wegen der vermutlich geringen Nutzungszahlen der alten CWA-App Versionen könnte sich das individuelle Re-Identifikationsrisiko für CWA-Nutzer älterer App Versionen (<= 2.7) erhöhen.	Ja	1	3	3	1	1	1	1	3	3	3	3	DM, VT, IV, TR, ZB	Designentscheidung D-5.1-15a (Bis zur CWA v1.15 finden Fake-Requests von der CWA-App zum CWA-Server statt, diese Fake-Requests verhindern eine direkte Re-Identifikation des CWA-Nutzers. Mit der Einführung eines weiteren Parameters mit einer sehr hohen Varianz (betrachtet auf die Anzahl der teilgenommen Events) wäre eine Re-Identifikation von Nutzem möglicherweise möglich. Deshalb werden die Fake Requests angepasst).			akzeptabel
R1-CWA-Nutzer	92	Offenlegung von Daten gegenüber Dritten (Apple/ Google) (bei Scan QR-Code ohne Installation der CWA-App)	GUID vom Event könnte an Apple/ Google übertragen werden, wenn die CWA veraltet oder nicht installiert ist. Die Betriebssystemhersteller könnten diese Informationen mit anderen verknüpfen und Rückschlüsse auf die Person ziehen, die den QR-Code hochgeladen hat.	Ja	2	1	2	1	1	1	1	2	2	2	4	VT, IV, TR, ZB	Verantwortung der Nutzer			akzeptabel
R2- Hacker	93	[Release 3.2]: Fehlende (Sicherheits-)updates im Ruhemodus	Wenn die Sandbox der Betriebssysteme nicht mehr gepflegt wird, können sich Sicherheitslücken auftun, wodurch Angreifer potenziell Zugriff auf die dort gehaltenen Daten erlangen	Ja	1	4	4	4	1	1	1	4	4	4	4	DM, VT, TR, ZB	Verantwortung der Nutzer für die IT-Sicherheit ihrer devices zu sorgen.			akzeptabel
	94	**5) Ungerechtfertigter Datentransfer in Drittland**																		
R4- Apple / Google	95	Beabsichtigter/ unbeabsichtigter Datenexport von Positiv-Schlüsseln, RPI durch Apple/ Crash-Logs		Ja	3	4	4	4	0	0	0	1	4	4	12	T, ZB; DM, VT, IG	Siehe Designentscheidung 5-3-1 und 5-3-2.		Die Grundsatzentscheidung für das Framework von Apple/ Google bedingt das Vertrauen der Nutzer in diese Plattformen.	bedingt akzeptabel
R4 - Softwareentwickler / SAP	96	Beabsichtigter/ unbeabsichtigter Datenexport von TEK/ TAN/ (i)TEK durch SAP/T (Schnittstellen)		Ja	1	4	4	4	0	0	0	1	4	4	4	TR, ZB, VT, IG, DM	AVV inkl. TOM mit DL, keine Datenübermittlung in Drittland.			akzeptabel
R1-CWA-Nutzer	97	Beabsichtigter/ unbeabsichtigter Datenexport von Positiv-Schlüssel/ Infektionsstatus an Unberechtigte (Auslandsaufenthalt des CWA-Nutzers)		Ja	1	4	4	4	0	0	0	1	4	4	4	TR, ZB, IG, VT, DM	Verantwortung der Nutzer (Designentscheidungen, Siehe D-2-2).			akzeptabel
	98	**6) Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten**																		
R1-CWA-Nutzer	99	Verlust des Smartphones (siehe oben - abhängig von Einstellung des Nutzers)		Ja	2	4	4	4	0	0	0	4	4	4	8	TR, ZB, VT, IG, DM	Nutzerverantwortung (Designentscheidungen D-2-2).			akzeptabel mit Evaluation
R1-CWA-Nutzer	100	Verlust von Daten, mit der Folge dass fehlende Information des Nutzers über Kontakt mit Infizierten innerhalb der Inkubationszeit erfolgt (beim Telefon zurücksetzen) - inkl. Schlüssel (Abhängigkeit)		Ja	3	0	0	0	0	0	0	0	2	2	6	TR , ZB	Nutzerverantwortung (Designentscheidungen D-2-2).			akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA)
VT 1: App-seitige Verarbeitung Kontaktereignisse + VT2: Kontaktfall + VT4: Infektfall + Eventregistrierung+Stopp der Warnungen
(Stand: 22.05.2023)

				Risikobewertung															
						Schadensausmaß													
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können**	**Restrisiko**
R1-CWA-Nutzer	101	Verlust von Daten (durch Anwendung zurücksetzen) - nur die Daten der App (kein durch die App versursachtes Risiko)		Nein											-					
R4- Betreiber Server (T)	102	Verlust/ Beschädigung von Diagnoseschlüsseln im Zusammenhang mit EFGS (EFGS-Risiko)	Unerwarteter Verlust oder unerwartete Löschung personenbezogener Daten im EFGS mit in Folge auftretender Nicht-Verfügbarkeit der Daten für die nationalen Backends. Die Speicherung und Bereitstellung der Daten kann gestört werden, hochgeladene Daten werden dann nicht richtig gespeichert oder die Daten werden nicht korrekt bereitgestellt. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	2	1	3	3	3	0	3	3	3	3	6	VT, IG, VF, R, TR, IV, ZB	EFGS-Betrieb mit redundanten Datenbanken. Zusätzlich müssen Schnittstellen Status- und Fehlermeldungen vorsehen, um festzustellen, ob emeute Uploads oder ähnliche Maßnahmen erforderlich sind. Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: ST_operational_mgt.doc, Backup security standard.pdf			akzeptabel mit Evaluation
R4- Betreiber Server (T)	103	Verlust/ Beschädigung von Diagnoseschlüsseln im Schweizer Gateway	Unerwarteter Verlust oder unerwartete Löschung personenbezogener Daten im Schweizer Gateway mit in Folge auftretender Nicht-Verfügbarkeit der Daten für die nationalen Backends (Dt. und Schweiz). Die Speicherung und Bereitstellung der Daten kann gestört werden, hochgeladene Daten werden dann nicht richtig gespeichert oder die Daten werden nicht korrekt bereitgestellt. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	2	1	3	3	3	0	3	3	3	3	6	VT, IG, VF, R, TR, IV, ZB	Abschluss eines (völker-)rechtlichen Vertrages mit der Schweiz ist erfolgt.			akzeptabel mit Evaluation
R2- Hacker	104	Verlust von Daten, mit der Folge fehlender Information des Nutzers über Kontakt mit Infizierten innerhalb Ider nkubationszeit (durch Dritte bei Verlust Smartphone)		Ja	2	4	4	4	0	0	0	4	4	4	8	TR, IV,VF, IG, DM, ZB	Nutzerverantwortung (Designentscheidungen D-2-2).			akzeptabel mit Evaluation
R1-CWA-Nutzer	105	Beeinträchtigung der Funktionalität durch fehlerhafte Einstellungen (Bluetooth an/ aus) und Nutzung (Gerät von Person phys. getrennt)		Ja	3	2	4	2	0	0	0	0	0	4	12	ZB, VT	Designentscheidung zur Nutzung der BLE-Technik, Nutzung der "Radiofunktion", siehe DSK_Rahmenkonzept, Kap. 14.6 (der Nutzer der CWA-App wird darüber in Kenntnis gehalten, wenn aktuelle Einstellungen der CWA-App deren Funktionalität beeinträchtigen. Auf diese Weise kann der Nutzer überprüfen, ob die entsprechenden Einstellungen tatsächlich von ihm selbst vorgenommen wurden).		Zwischenzeitlich liegt eine Stellungnahme des BSI vor, wonach keine zusätzlichen Sicherheitsrisiken durch Nutzung der Bluetooth-Technologie gesehen werden.	bedingt akzeptabel,
R1-CWA-Nutzer	106	Gleichzeitige Verbindungen zu mehreren Bluetooth-Geräten		Ja	1	0	0	0	0	0	0	0	2	0	2	TR	Designentscheidungen D-2-6.			akzeptabel
R6 - Krimineller	107	Eventregistrierung: Vorsätzliche Zerstörung des QR-Codes im Rahmen der Eventregistrierung		Ja	1	1	1	1	2	1	2	2	1	1	2	VF, RE, IV	Verantwortung der Nutzer			akzeptabel
	108	**7) Verweigerung der Betroffenenrechte (Betrachtung der Unterstützung durch SAP/T)**																		
R1-CWA-Nutzer	109	CWA-Nutzer ist sich seiner Pflichten aus der DSGVO nicht oder nicht ausreichend bewusst	Der CWA-Nutzer als für die DV-Verantwortlicher unterlässt es, seine Kontakte zu informieren, wenn er sie eintragen möchte oder ihnen ggf. Berichtigungs-, Löschungsrechte zu gewähren (Transparenzrisiko, Verweigerung der Betroffenenrechte). Risikoerhöhung durch Freitextfeld.	Ja	3	4	4	4	1	1	1	4	4	4	12	IV, T, ZB	Designentscheidungen zur Einführung des KTB (siehe Anlage 1 zum DSFA-Bericht: D-2-2b, D-6-2c, D-5-11, D-9-8, D-7-10), DSK-Rahmenkonzept 14.27.17.			bedingt akzeptabel, Informationskampagne
R4 - Softwareentwickler / SAP	110	Nichtbeachtung von Auskunftsrechten (keine Verpflichtung zur Herstellung Personenbezug) - Art. 11		Ja	1	4	0	0	0	0	0	0	0	0	4	DM	Designentscheidung/ Pseudonymisierung, keine Herstellung des Personenbezugs zur Erfüllung Betroffenenrechte, Designentscheidungen D-8-1.			akzeptabel
R4 - Softwareentwickler / SAP	111	Nichtbeachtung von Löschungsersuchen, Berichtigungsersuchen - Art. 11		Ja	1	4	0	0	0	0	0	0	0	0	4	DM	Designentscheidung/ Pseudonymisierung, keine Herstellung des Personenbezugs zur Erfüllung Betroffenenrechte, Designentscheidungen D-8-1.			akzeptabel
R4 - Softwareentwickler / SAP	112	Fehlende Anfechtbarkeit der automatisiert erfolgenden Empfehlungen (Prüfung und Bestätigung der Empfehlungen durch eine fachkundige Person) - da Empfehlungen ohne Rechtsfolgen		Ja	1	0	0	0	0	0	0	4	0	0	4	IV	Designentscheidung/ Pseudonymisierung, keine Herstellung des Personenbezugs zur Erfüllung Betroffenenrechte, Designentscheidungen D-8-1.			akzeptabel
R4 - Softwareentwickler / SAP	113	Fehlende Übertragbarkeit		Ja	1	0	0	0	0	0	0	0	0	0	0	IV	Designentscheidung/ Pseudonymisierung, keine Herstellung des Personenbezugs zur Erfüllung Betroffenenrecht, Designentscheidungen D-8-1.			akzeptabel
R4 - Softwareentwickler / SAP	114	Fehlende/ unzureichende Löschung der Daten bei De-Installation der App/ Zurücksetzen der App (Frontend)		Ja	1	4	0	0	0	0	0	0	0	0	4	DM	Siehe Ausführungen zur Löschung in dem DSK CWA.			akzeptabel
R4- Betreiber Server (T)	115	Fehlende/ unzureichende Löschung der Daten im Backend (CWA-Backend, Testresult, Verifikation)		Ja	1	4	0	0	0	0	0	0	0	0	4	DM	Siehe Aufführungen zur Löschung in den Teil-DKS, Designentscheidungen (D-8-1ff.) und AVV inkl. TOM.			akzeptabel
R4- Apple / Google	116	Fehlende/ unzureichende Löschung der Daten im ENF bei Löschersuchen		Ja	2	4	0	0	0	0	0	0	0	0	8	DM	Designentscheidungen D-11-2; fehlende Einflussmöglichkeit auf Löschung im ENF (Designentscheidung D-9-2).			akzeptabel mit Evaluation
R4- Betreiber Server (T)	117	Fehlende/ unzureichende Löschung auf Servern und Übertragungsmittel zum CDN bei Löschersuchen (unzureichende Löschung/ internes System)		Ja	2	4	0	0	0	0	0	0	0	0	8	DM	Designentscheidungen D-9-1ff.			akzeptabel mit Evaluation
	118	**8) Verwendung der Daten zu inkompatiblen Zwecken**																		
R8-staatl Behörden	119	Nachträgliche Zweckänderung/ -erweiterung durch die verantwortliche Stelle ("Dammbruch")		Nein	3	4	4	4	0	0	0	4	1	4	-	ZB; IV, VT, IG, DM	Designentscheidungen D-1-1.			
R8-staatl Behörden	120	Nutzung der Daten zur Erstellung eines Immunitätsausweises		Nein	3	4	0	0	0	0	0	0	0	4	-	DM, TR	Designentscheidungen D-1-1.			
R8-staatl Behörden	121	Nutzung zur Überwachung von Maßnahmen der soz. Distanzierung, Quarantänemaßnahmen (z.B. Strafverfolgung, mittels Anweisung an die Telekom)		Ja	3	4	4	4	0	0	0	4	4	4	12	ZB , IV, TR, DM, VT, IG				bedingt akzeptabel
R1-CWA-Nutzer	122	Nutzung des KTB-Einträge durch staatliche/private Stellen zur Überwachung von Maßnahmen der soz. Distanzierung, von Quarantänemaßnahmen oder weiteren Zwecken, die über die Zwecke der CWA hinausgehen	Private könnten den CWA-Nutzer bitten, ihm KTB-Einträge zur Verfügung zu stellen (z.B. Unterstützung bei Suche nach Vermissten). Strafverfolgungs- oder Polizeibehörden könnten den CWA-Nutzer anweisen, KTB-Daten zur Strafverfolgung oder Gefahrenabwehr herauszugeben. Das Risiko erhöht sich, wenn immer mehr Details im Kontakttagebuch gespeichert werden.	Ja	3	3	4	4	1	1	1	4	4	4	12	VT, IG, IV, TR, ZB	Designentscheidungen zur Einführung des KTB (siehe Anlage 1 zum DSFA-Bericht: D-2-2b, D-6-2c, D-5-11, D-9-8, D-7-10), DSK-Rahmenkonzept 14.27.17.	Zusätzlicher Zugangsschutz durch CWA-Nutzer für besondere Bereiche (PIN).		bedingt akzeptabel
R8- Behörden	123	Modifikation oder Wechsel des Zwecks der Verarbeitung im Rahmen der nachfolgenden Verarbeitung durch die Mitgliedsstaaten oder Missachtung des ursprünglichen Zwecks.	Durch das Einführen von Analysemöglichkeiten in nationale mobile Applikationen wird ein Risiko begründet, dass Daten außerhalb des mittels des EFGS verfolgten Zwecks verarbeitet werden. Dieses Risiko ist nicht unmittelbar auf den EFGS bezogen. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Nein											-		Design-Entscheidungen EFGS D-1-1 (Die nationalen Gesundheitsbehörden bestimmen die Schranken des Verarbeitungszwecks), Designentscheidungen EFGS D-1-2, D-1-3.			
R8- Behörden	124	Modifikation oder Wechsel des Zwecks der Verarbeitung mittels des Schweizer Gateways oder Missachtung des ursprünglichen Zwecks	Durch das Einführen von Analysemöglichkeiten in nationale (hier: schweizerische) mobile Applikationen wird ein Risiko begründet, dass Daten außerhalb des mittels des Anschlusses des Schweizer Gateways an die CWA verfolgten Zwecks verarbeitet werden. Dieses Risiko kann nur durch den Verantwortlichen für das Schweizer Gateway zugerechnet werden. Es handelt sich nicht um eine Schwachstelle der CWA. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Nein											-					
R8- Behörden	125	Anfänglicher oder späterer Missbrauch des Parameters "Transmission Risk Level".	Dieser Parameter kann von den Mitgliedsstaaten unterschiedlich verwendet werden. Auf Grund der erwarteten Ablösung des Datenfelds kann es zur Übertragung beliebiger Daten verwendet werden.	Ja	3	0	0	0	0	0	0	3	3	3	9	IV, TR, ZB	Weiterzuverteilende Diagnoseschlüssel werden in den nationalen Backends vor der Verteilung an die Apps normalisiert.			akzeptabel mit Evaluation
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	126	Missbrauch der über das EFGS geteilten personenbezogenen Daten zur Durchsetzung und Sanktionierung von Maßnahmen zur sozialen Distanzierung, der Quarantänesicherung und/ oder Einschränkungen der Bewegungsfreiheit.	Dieses Risiko wird durch die nationale mobile Applikation begründet und bestimmt. Es kann nicht unmittelbar dem EFGS zugerechnet werden. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Nein											-		Design-Entscheidungen EFGS D-1-5 (Keine Verwendung für die Überwachung von Quarantäne-Maßnahmen) + Designentscheidungen CWA national D-1-1.			

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse + VT2: Kontaktfall + VT4: Infektfall + Eventregistrierung+Stopp der Warnungen (Stand: 22.05.2023)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	127	Missbrauch der über das Schweizer-Gateway geteilten personenbezogenen Daten zur Durchführung und Sanktionierung von Maßnahmen zur sozialen Distanzierung, der Quarantänesicherung und/ oder Einschränkungen der Bewegungsfreiheit	Dieses Risiko wird durch die nationale mobile Applikation begründet und bestimmt. Es kann nur durch den Verantwortlichen für das Schweizer Gateway zugerechnet werden. Es handelt sich nicht um eine Schwachstelle der CWA. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Nein											-					
R3-kommerzielle Datensammler	128	Missbrauch der über das EFGS geteilten personenbezogenen Daten für andere kommerzielle oder interne Zwecke von Dritten.	Dieses Risiko wird durch die nationale mobile Applikation begründet und bestimmt. Es kann nicht unmittelbar dem EFGS zugerechnet werden. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Nein											-		Die Mitgliedsstaaten überwachen die Einhaltung der Freiwilligkeitsbedingungen abhängig vom nationalen Gesetzesrecht.			
R3-kommerzielle Datensammler	129	Missbrauch der über das Schweizer Gateway geteilten personenbezogenen Daten für andere kommerzielle oder interne Zwecke von Dritten	Dieses Risiko wird durch die nationale mobile Applikation begründet und bestimmt. Es kann nur durch den Verantwortlichen für das Schweizer Gateway zugerechnet werden. Es handelt sich nicht um eine Schwachstelle der CWA. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Nein											-					
R4- Apple / Google	130	Missbrauch der über das EFGS geteilten Daten durch Kombination mit Standortdaten und weitergehende Verwendung zu kommerziellen Zwecken.	Dieses Risiko wird durch die nationale mobile Applikation begründet und bestimmt. Es kann nicht unmittelbar dem EFGS zugerechnet werden. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Nein											-		Design-Entscheidungen EFGS D-1-7 (Keine Bestimmung des Standorts des Betroffenen).			
R4- Apple / Google	131	Missbrauch der über das schweizer Gateway geteilten Daten durch Kombination mit Standortdaten und weitergehende Verwendung zu kommerziellen Zwecken	Dieses Risiko wird durch die nationale mobile Applikation begründet und bestimmt. Es kann nur durch den Verantwortlichen für das Schweizer Gateway zugerechnet werden. Es handelt sich nicht um eine Schwachstelle der CWA. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Nein											-					
R4- Betreiber Server (T)	132	Re-Identifikation von Betroffenen auf Grund bei der Benutzung von Telekommunikationseinrichtung anfallender Daten (z.B. Übertragungsprotokolle, Typisierung von Datenverkehr etc.).	Aufgrund nicht bestehender oder fehlender Isolierung von Komponenten des EFGS untereinander wird einem Angreifer der Zugriff auf weitergehende Systemeinrichtungen ermöglicht. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	3	3	0	0	0	0	0	0	3	3	DM, VT, TR	Trennung von System-Komponenten - DIGIT-Standard.			akzeptabel
R3-kommerzielle Datensammler	133	Missbrauch der Daten durch Apple/ Google, Hersteller, Betreiber und andere Interessierte für eigene Zwecke		Ja	3	4	4	4	0	0	0	4	4	4	12	ZB , TR, IV, IG, VT, DM	Designentscheidungen D-5.3-1.		Die Grundsatzentscheidung für das Framework von Apple/ Google bedingt das Vertrauen der Nutzer in diese Plattformen.	bedingt akzeptabel
R4- Apple / Google	134	Missbrauch der Systeme, um Schlüsse auf den Standort der Nutzer, konkrete Kontaktpersonen und/ oder andere Kriterien zu ziehen (aktuell nur Google, weil technische Notwendigkeit zur Nutzung von BLE bis Betriebssystemversion 10)		Ja	3	3	3	3	0	0	0	3	3	3	9	ZB , TR, IV, IG, VT, DM	Die Offenlegung Quellcodes zeigte, dass die CWA-App ohne Zugang auf Standortdaten funktionier. Kein Einfluss auf Berechtigungsanforderungen durch Google/ Apple.DSK, Rahmenkonzept, Kap. 14.20.5: " Auf Android-basierten mobilen Endgeräten ist das Aktivieren des ENF mit der gleichzeitigen Aktivierung der Lokalisierungsfunktion verbunden. Letztere wird weder von der CWA-App noch – nach den insoweit nachvollziehbaren Angaben von Google – dem ENF verwendet. Jedoch werden mit dieser Aktivierung zwangsläufig Standortdaten des mobilen Endgeräts an Google übertragen, und der Nutzer kann sein mobiles Endgerät über den Google Service Find My Device orten. Anders ist mit dem Betriebssystem Android eine Nutzung vom ENF und damit der CWA-App nicht möglich."			akzeptabel mit Evaluation
R2- Hacker	135	De-Anonymisierung/ De-Pseudonymisierung durch Verbindung von Gerät und GUID auf CWA - Server (technisch unmöglich)		Nein											-					
R3-kommerzielle Datensammler	136	De-Anonymisierung / De-Pseudonymisierung durch Verbindung mit Daten, die über andere Geräte/ Apps gesammelt werden		Ja	2	1	2	0	4	1	4	4	4	4	8	DM, ZB, TR, IV, VF, R	Restrisiko ist beschrieben im DSK CWA-Server.			akzeptabel mit Evaluation
R3-kommerzielle Datensammler	137	De-Anonymisierung/ De-Pseudonymisierung durch Mitnutzung des Partner-QR-Codes für die Eventregistrierung mittels CWA-App	Durch die Schaffung der Interoperabilität von QR-Codes besteht die Möglichkeit, dass die Daten aus beiden Systemen (Partner + CWA) dazu genutzt werden könnten, Bewegungsprofile zu erstellen. Die Mitnutzung des Partner-QR-Codes soll sich auf den Zweck der Aufnahme des entsprechenden LINKs in den QR-Code zur Eventregistrierung beschränken.	Ja	2	1	3	0	1	1	1	1	1	1	6	VT	Ohne eine Anmeldung des CWA-Nutzers im Partnersystem kommt es zu keinen Datenflüssen aufgrund der Aufnahme des LINKs in den Eventregistrierungs-QR-Code. Es wurde mit dem Partner ein Threat-Modelling durchgeführt. Des weiteren wird durch eine Vereinbarung zwischen dem Partner und dem Verantwortlichen der CWA abgesichert, dass die erforderlichen Maßnahmen zur Einhaltung von Datenschutz- und Sicherheitsanforderungen eingehalten werden.			akzeptabel mit Evaluation
R6 - Krimineller	138	Re-Identifizierung durch Protokollierung	Ein potentieller Angreifer kann die CWA-App auf mehreren Mobilfunkgeräten für jeweils kurze Zeit am Tag einsetzen und sich dabei zu jedem Gerät notieren, mit welchen Personen er zu dieser Zeit Kontakt hatte. Der Angreifer kontrolliert in regelmäßigen Abständen, auf welchen mobilen Endgeräten er über potentielle Kontakte mit positiv getesteten Personen informiert wurde. Über seine Notizen kann er gegebenenfalls im Ausschlussverfahren ermitteln, bei welchem seiner Kontakte ein positives Testergebnis vorliegen muss. Bei Personen mit generell wenigen Kontakten kann es bereits mit einem einzigen Gerät ohne Zuhilfenahme zusätzlicher Informationen möglich sein, eine positiv getestete Person allein auf Grund des Gedächtnisses zu identifizieren.	Ja	1	1	2	0	o	1	o	4	4	4	4	ZB, TR, IV	Auf Grund der bewussten Entscheidung, auf Personenbezug zu verzichten, kann die Mehrfachnutzung der CWA-App durch einen einzigen Anwender nicht ausgeschlossen werden. Restrisiko ist beschrieben im DSK Rahmendokument .			akzeptabel
R1-CWA-Nutzer	139	Re-Identifizierung durch Protokollierung (durch Integration KTB)	(ohne Kontakthistorie)	Ja	2	2	2	2	1	1	1	2	2	3	6	ZB, VT, IG	Designentscheidungen zur Integration KTB (D-2-2b, D-6-2c, D-5-1-11, D-9-8, D-7-10).			akzeptabel mit Evaluation
R1-CWA-Nutzer	140	Re-Identifizierung durch Begegnungshistorie in KTB und Ergänzung Attribute mit CWA [Release 1.14]	Das KTB wird mit [Release 1.12] um das Feature der "Risiko-Historie" erweitert. Das Kontakt-Tagebuch zeigt nun neben den eingetragenen Einträgen vom Nutzer auch das Gesamtrisiko des jeweiligen Tages an. Mit den angezeigten Informationen kann der CWA-Nutzer möglicherweise Rückschlüsse ziehen, welcher seiner Kontakte möglicherweise positiv auf Corona getestet wurde. Die CWA-App ermöglicht es nun neben der Protokollierung von Begegnungen auch festzustellen, ob eine getroffene Person möglicherweise positiv auf Corona getestet wurde. Auch wird Clustenung bei Zugriff auf mehrere CWA-Apps erleichtert (z.B. Schnittmenge innerhalb Familie). Je stärker staatliche Restriktionen verhängt (Ausgangssperren, Kontaktbeschränkungen, Homeoffice Ausweitungen, Schul- und Kita-Schließungen) und Selbst-Isolation wirkt, um so geringer sind die Kontaktbegegnungen und umso höher wird das Re-Identifizierungsrisiko. Durch die Möglichkeit, mit [Release 1.14] weitere Attribute hinzuzufügen, erhöht sich das Risiko weiter.	Ja	3	3	3	1	1	1	1	3	3	3	9	DM, VT,, IV, TR, ZB	Informationen der Nutzer über Funktionalität und Risiken der Falschbewertung und falschen Verdächtigung (siehe Designentscheidungen D-2-4a).	Zusätzlicher Zugangsschutz durch CWA-Nutzer für besondere Bereiche (PIN).	Die Begegnungshistorie ist grundsätzlich nur eine übersichtlichere Darstellung bereits vorhandener Informationen, die vom Nutzer auch manuell zusammengestellt werden kann.	akzeptabel mit Evaluation
R1-CWA-Nutzer	141	Falsche Verdächtigung infolge einer Re-Identifizierung durch Begegnungs-Historie KTB und Ergänzung um Attribute mit CWA [Release 1.14]	Folge-Risiko zu Z 136. Es drohen Diskriminierungen der Kontaktpersonen; Freiheitsbeschränkungen, Rufschädigungen und ggf. finanzielle Verluste durch Quarantäneanordnung und Beschränkung Berufsausübungsfreiheit.	Ja	3	3	3	3	1	1	1	3	3	3	9	DM, VT, IG, IV, TR, ZB	Informationen der Nutzer über Funktionalität und Risiken der Falschbewertung und falschen Verdächtigung (siehe Designentscheidungen D-2-4a).	Zusätzlicher Zugangsschutz durch CWA-Nutzer für besondere Bereiche (PIN).	Die Begegnungshistorie ist grundsätzlich nur eine übersichtlichere Darstellung bereits vorhandener Informationen, die vom Nutzer auch manuell zusammengestellt werden kann.	akzeptabel mit Evaluation
R4- Betreiber Server (T)	142	De-Anonymisierung/ De-Pseudonymisierung von Nutzem anhand von Verbindungsdaten (beim Hochladen der Diagnoseschlüssel auf CWA-Server, Abfrage Testergebnis, Registration Token, TAN, teleTAN)		Ja	2	1	2	0	4	1	4	4	4	4	8	DM, ZB , TR, IV, VF, R	AVV mit DL, inkl. TOM Designentscheidung D-11-1. Die Auswertung der IP-Adressen auf Infrastukturebene der OTC ist zeitlich stark begrenzt und durch die etablierten Sicherheitsprozesse zur Angriffserkennung in den DDoS Systemen definiert; die Verarbeitung wird nur dort systemintern vorgenommen, siehe Risikobeschreibung für die einzelnen Komponenten, inkl. CDN in DSK-Rahmenkonzept (v1.8) , Kap. 14.8.			akzeptabel mit Evaluation
R8-staatl Behörden	143	De-Anonymisierung/ De-Pseudonymisierung von Nutzem anhand von Standortdaten		Ja	3	3	3	3	0	0	0	3	3	3	9	ZB, TR, IV, VT, IG, DM	AVV mit DL inkl. TOM Designentscheidungen D-11-1.			akzeptabel mit Evaluation
R4- Betreiber Server (T)	144	Re-Identifizierung der Nutzer durch Protokolldaten/ Zugriff durch Strafverfolgungsbehörden		Ja	3	4	4	4	0	0	0	4	4	4	12	ZB , TR, IV, IG, VT, DM	AVV mit DL inkl. TOM Designentscheidungen D-11-1, DSK_Rahmenkonzept, Kap. 14.20.2 (Staatliche Organe wie Geheimdienste oder Strafverfolgungsbehörden können sich Zugriff auf die einzelnen Komponenten der Anwendungsarchitektur verschaffen, deren Datenbestände beschlagnahmen und durch Kombination, der ihnen zur Verfügung stehenden Informationen den Personenbezug herstellen. Gesetzlich ist diese Möglichkeit wegen Betroffenheit des Kernbereichs des Allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) jedenfalls stark eingeschränkt ausgeschlossen).		Die Nutzung der IT-Infrastruktur der OTC bedarf des Vertrauens der Nutzer, dass sich Betreiber rechtskonform verhält und nur bei Vorliegen der gesetzlichen Voraussetzung Daten an Strafverfolgungsbehörden herausgibt. Es ist ein Prozess etabliert, wonach das Vorliegen einer Rechtsgrundlage für die Herausgabe von Daten explizit juristisch geprüft wird.	bedingt akzeptabel,

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse + VT2: Kontaktfall + VT4: Infektfall + Eventregistrierung+Stopp der Warnungen (Stand: 22.05.2023)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R2- Hacker	145	Re-Identifizierung Nutzer durch Peilung (BLE/ WiFi) als sendende Person		Ja	3	1	2	2	0	0	0	2	2	3	9	DM, ZB	Designentscheidungen zur Nutzung der BLE-Technik D-5.1-14.			akzeptabel mit Evaluation
R2- Hacker	146	De-Anonymisierung/ De-Pseudonymisierung/ Enttarnung von Nutzern durch Benachrichtigungen oder Metadaten	Falls ein CWA-Nutzer durch eine visuelle, textuelle oder auch akustische Benachrichtigung von der CWA-App über einen möglichen Kontakt mit einem positiv getesteten Nutzer oder das Vorliegen eines Testergebnisses informiert oder mittels des Erinnerungs-Pop-Ups an den Upload des Testergebnisses erinnert wird - insbesondere durch die Anzeige der Erinnerung an das upload des positiven Testergebnisses, die auch auf dem Sperrbildschirm des Smartphones erscheinen kann - ist es einem unbestimmten Personenkreis ohne weiteres durch den Blick auf das Smartphone möglich, den Besitzer des Smartphones als eindeutig infizierten zu identifizieren. Diese Offenlegung des Gesundheitsstatus an Unbefugte kann zur Verletzung der Vertraulichkeit und Diskriminierungen des Betroffenen führen.	Ja	2	1	4	1	1	0	0	2	2	4	8	VT, ZB	Designentscheidungen (Verschlüsselung) D-5.1-11 und datenschutzfreundliche Voreinstellungen D-3.1-4. DSK_Rahmenkonzept Kap. 14.5. Benachrichtigungen sind per Voreinstellung ausgeschaltet, müssen also vom CWA-Nutzer aktiviert werden. Die Erinnerung dient allein dem CWA-Nutzer, es erfolgt nur eine lokalen Datenverarbeitung auf dem Smartphone. Die erste Erinnerung erfolgt darüber hinaus nach 2 Stunden, eine Zeitspanne in der sich der CWA-Nutzer in der überwiegenden Zahl der Fälle bereits in Quarantäne begeben haben wird, was den Personenkreis, die eine solche Nachricht zur Kenntnis nehmen könnten, auf den Nahbereich beschränkt.			akzeptabel mit Evaluation
R4- Apple / Google	147	Emittlung von Kontaktereignissen, auch für Nutzer ohne CWA (keine Schwachstelle der CWA) - siehe oben		Nein	0	0	0	0	0	0	0	0	0	0	-					
R4 - Softwareentwickler / SAP	148	Aufbau von zentralen Bewegungs- und Kontaktprofilen (Verhaltenskontrolle, Compliance Scoring) anhand von "Kontakthistorien"	In Version 1 des ENF erhält die CWA-App im Rahmen der Kontaktermittlung und Risikoberechnung durch das Betriebssystem des mobilen Endgeräts eine sogenannte Exposure-Info, die statische Informationen wie Dauer, Alter und Signaldämpfung einer Begegnung mit einem positiv auf Corona getesteten Nutzer umfasst. In Version 2 des ENF hingegen übergibt das Betriebssystem der CWA-App jeweils eine als Exposure-Window bezeichnete Datenstruktur, die eine dynamische Darstellung des Verlaufs einer Risikobegegnung in Form mehrerer, sich über bis zu 30 Minuten hinweg erstreckender Messpunkte (Scan-Windows) enthält (s. 14.1 sowie den Abschnitt XXX des Datenschutzkonzepts der CWA App). Gegenwärtig verwendet die CWA App die vom Betriebssystem zur Verfügung gestellten Informationen als Eingangsgrößen für die Risikoberechnung eines Kontaktes nach einer festgelegten mathematischen Formel. Grundsätzlich wäre es jedoch mit Version 2 des ENF denkbar, die Struktur des Verlaufs einer Begegnung mit Methoden der Künstlichen Intelligenz wie z.B. Machine Learning zu analysieren, um die infektiologische Situation, in der eine Begegnung stattgefunden hat, zu erschließen und in die Bewertung des damit verbundenen Risikos einfließen zu lassen – also beispielsweise, ob ein Kontakt in einem Innenraum oder im Freien stattgefunden hat.	Ja	1	4	4	0	0	0	0	4	4	4	4	DM, VT, ZB, TR, IV	Designentscheidungen D-7-2, D-2-1 (Exposure Window).	Sollte in Zukunft eine solche Technologie/ KI zum Einsatz kommen, ist intensiv darauf zu achten, dass die Erfassung der infektiologischen Situationen nicht in einer Granularität erfolgt, welche die Analyse, Bewertung oder Überwachung von Benutzerverhalten ermöglicht (z.B. Besuch einer Bar, eines Kinos, einer Cocktailparty).		akzeptabel
R8- Behörden	149	Re-Identifikation von Betroffenen auf Grund der Abfrage der relevanten Länder: Erzeugung einer Reisehistorie; Re-Identifikation auf Grund der Einmaligkeit der Reisehistorie oder weiterer Daten, die staatlichen Einrichtungen zur Verfügung stehen (EFGS - Risiko)	Siehe Zeilen 72, 74, 76-78. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	2	2	0	0	0	0	2	0	2	2	DM; VT, IT, ZB	Siehe Zeilen 70, 72, 74-76.		Siehe Zeilen 70, 72, 74-76.	akzeptabel
R8- Behörden	150	Re-Identifikation von Betroffenen auf Grund der Abfrage der relevanten Länder durch Schweizer Gateway: Erzeugung einer Reisehistorie; Re-Identifikation auf Grund der Einmaligkeit der Reisehistorie oder weiterer Daten, die staatlichen Einrichtungen zur Verfügung stehen (siehe Zeilen 73, 75)	Siehe Zeilen 73, 75. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	2	2	0	0	0	0	2	0	2	2	DM, VT, IT, ZB	Siehe Zeilen 71, 73.		Siehe Zeilen 71, 73.	akzeptabel
R2- Hacker	151	Herstellung eines "Ausländerscanners" (EFGS - Risiko)	Re-Identifikation von Nutzern von mobilen Applikationen aus Drittstaaten auf Grund der Kennzeichnung der Herkunft der Diagnoseschlüssel: Ein Angreifer kann die RPI nach einem Kontakt ableiten und auf Grund der Herkunftsinformation der Diagnoseschlüssel Informationen bezüglich der Nationalität eines Kontakts ableiten. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	3	2	2	0	0	0	0	2	0	2	6	DM, VT, IT, ZB	Design-Entscheidungen EFGS (Normalisierung).			akzeptabel mit Evaluation
R5-Arbeitgeber, Versicherungen	152	(Freiheits-)Beschränkungen bei Teilung der Anzeige "Status Tracing"		Ja	2	0	4	0	0	0	0	4	0	4	8	IG, ZB, IV	Designentscheidung D-2.2-1.			akzeptabel mit Evaluation
R2- Hacker	153	Eventregistrierung: CWA-Nutzer Profiling (+ Zusatzinfos außerhalb der CWA)	Die vorgeschlagene Lösung veröffentlicht Warnungen im CDN stündlich in Paketen. Ein Paket enthält mehrere Warnungen. Eine Warnung besteht aus der GUID eines Veranstaltungsortes und einem Zeitintervall. Alle Warnungen, die beim Einchecken eines einzelnen Benutzers erstellt wurden, sind in einem Paket enthalten. Ein Berichtspaket kann Warnungen mehrerer Benutzer enthalten. Ein Angreifer kann die Check-Ins eines einzelnen Pakets analysieren und versuchen, ein Profil der Benutzer zu erstellen, deren Check-Ins enthalten sind. Dies zeigt nur begrenzte Informationen, wenn die GUIDs der Veranstaltungen nicht mit einer konkreten Veranstaltungen verknüpft werden können (vgl. [Profiling von Veranstaltungen]), kann aber signifikante Informationen über den Nutzer aufzeigen, je mehr GUIDs von Veranstaltungen identifiziert werden können.	Ja	1	2	2	1	1	1	1	2	2	2	2	DM, VT, IV, TR, ZB	Designentscheidungen zur Eventregistrierung (D-2-1a, D-2-2d, D-5.1-15a, D-6-2d, D-9-8a) + Verantwortung der Nutzer.			akzeptabel
R2- Hacker	154	Erstellung von Nutzerprofilen	In Orten mit niedrigen Fallzahlen könnte ein Angreifer die QR-Codes aus allen Veranstaltungsorten durch seine eigenen QR-Codes austauschen. Anhand der hochgeladenen Check-Ins könnte der Angreifer nun Bewegung-Profile von CWA-Nutzer anlegen.	Ja	1	3	3	1	1	1	1	3	3	3	3	DM, VT, IV, TR, ZB	Designentscheidungen zur Eventregistrierung (D-2-1a, D-2-2d, D-5.1-15a, D-6-2d, D-9-8a).			akzeptabel
R5-Arbeitgeber, Versicherungen	155	(Freiheits-)Beschränkungen bei Nicht-Nutzung der App (Zugangs Beschränkungen zu staatlichen/ privaten Leistungen)		Ja	2	0	4	0	0	0	0	4	0	4	8	DM, ZB, IV	siehe Dokument Designentscheidungen D-3.2-1.			akzeptabel mit Evaluation
	156	**9) Verarbeitung nicht vorhergesehener Daten**																		
R4- Betreiber Server (T)	157	Speicherung/ Verarbeitung von (Meta-)Daten, die für die Zweckerfüllung nicht erforderlich sind		Ja	2	3	0	0	0	0	0	0	0	4	8	ZB	AVV mit DL, inkl. TOM Designentscheidung D-11-1. Die Auswertung der IP-Adressen auf Infrastrukturebene der OTC ist zeitlich stark begrenzt und durch die etablierten Sicherheitsprozesse zur Angriffserkennung in den DDoS			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	158	Speicherung von App-Crash-Report Daten zur Re-Identifikation		Ja	2	3	0	0	0	0	0	0	0	4	8	ZB	AVV mit DL, inkl. TOM Designentscheidung D-11-1. Die Auswertung der IP-Adressen auf Infrastrukturebene der OTC ist zeitlich stark begrenzt und durch die etablierten Sicherheitsprozesse zur Angriffserkennung in den DDoS Systems definiert			akzeptabel mit Evaluation
	159	**10) Verarbeitung nicht richtiger Daten**																		
R4 - Softwareentwickler / SAP	160	Ungenauigkeit bei der Zuordnung des Ansteckungsrisikos an CWA-Nutzer (Transmission Risk zu Tagesschlüsseln)	Infolge der bisherigen Programmierung bei der Zuordnung von Transmission Risk zu Tagesschlüsseln des CWA-Nutzers, kann es zu Ungenauigkeiten in der Zuordnung des Ansteckungsrisikos für den CWA-Nutzer kommen, wenn a.) eine Lücke bei den zur Verfügung stehenden Tagesschlüsseln entsteht (z.B. durch Ausschalten des Smartphones) oder b.) mehrere Tagesschlüssel für den selben Tag kreiert wurden (z.B. in neueren Versionen oder durch die Nutzung verschiedener Tracing-Apps). In der Folge könnte allein durch diese Art der Programmierung a) das Ansteckungsrisiko als etwas zu hoch, b) etwas zu niedrig eingeschätzt werden.	Ja	2	0	3	1	0	0	0	2	2	3	6	IG, ZB	Es handelte sich bei dem Risiko um eine fehlerhafte Programmierung (Bug). Dieser Fehler wurde zwischenzeitlich behoben und tritt ab [Release 1.5] nicht mehr auf.			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	161	Fälschung Parameter/ falsche Berechnungen in der App durch statische Programmierung für das Risiko der Ansteckung (über vorhergehende Fehler hinaus)		Ja	2	0	0	0	0	0	0	4	4	4	8	ZB, TR, IV	Designentscheidungen D-8-1 (Parameteranpassungen nur durch Einspielen von Updates).			akzeptabel mit Evaluation
	162	"Falscher Negativer"		Ja	3	0	4	0	0	0	0	4	4	4	12	ZB, TR, IV	Designentscheidungen (D-7-3).		Zwischenzeitlich liegt eine Stellungnahme des BSI vor, wonach keine zusätzlichen Sicherheitsrisiken durch Nutzung der Bluetooth-Technologie gesehen werden.	bedingt akzeptabel,

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse + VT2: Kontaktfall + VT4: Infektfall + Eventregistrierung+Stopp der Warnungen (Stand: 22.05.2023)				Risikobewertung															
						Schadensausmaß													
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
	163	Alarmierung "falscher Positiver" (Grenzen der BLE-Technik - Vortäuschen falscher Kontakte trotz Wand) - "Fehldiagnostik"		Ja	3	0	0	3	0	3	0	0	0	4	12	IG, ZB	Designentscheidungen (D-8-3).		Zwischenzeitlich liegt eine Stellungnahme des BSI vor, wonach keine zusätzlichen Sicherheitsrisiken durch Nutzung der Bluetooth-Technologie gesehen werden.	bedingt akzeptabel,
R1-CWA-Nutzer	164	Upload von falsch-positiven Ergebnissen auf Grund unzureichender Zuverlässigkeit der Prüfmechanismen des Bestehens einer Infektion (Missbräuchlicher Upload nicht-infektiöser Diagnoseschlüssel, Injektion unzutreffender Testresultate); (EFGS-Risiko)	Länder mit schwächeren Mechanismen zur Überprüfung einer Infektion mit SARS-CoV-2 können eine große Anzahl unzutreffend als infiziert bezeichneter Schlüssel an das EFGS übertragen. Schwächere Mechanismen können z.B. in der Verwendung eines einzigen bekannten Codes zur Infektionsmeldung für eine Testeinrichtung bestehen. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	4	2	4	0	0	0	4	4	4	4	DM, VT, IG, IV, TR, ZB	Design-Entscheidungen EFGS D-2.3-4 (Überprüfung eines positiven Testergebnisses durch Gesundheitsbehörde).	Design-Entscheidungen EFGS D-2.3-4 (Überprüfung eines positiven Testergebnisses durch Gesundheitsbehörde). Designentscheidung CWA National D-5.1-8a: Mithilfe des EFGS können alle Nutzer der Nationalen Corona-Apps bei einer Risikobegegnung mit einem positiv auf Corona getesteten Nutzer nicht nur der eigenen, sondern auch einer anderen Nationalen Corona-Apps gewarnt werden. Deshalb lädt der CWA-Server die von CWA-Nutzern geteilten Positivschlüssel auf den EFGS, der sie an die Backends der Nationalen Corona-Apps weiterleitet. Umgekehrt empfängt der CWA-Server vom EFGS die Positivschlüssel der Nutzer anderer nationalen Corona-Apps und stellt sie der CWA-App auf den mobilen Endgeräten der CWA-Nutzer über das CDN zusammen mit den Positivschlüsseln der CWA-Nutzer zur Verfügung. Die Kriterien, nach denen ein Nutzer seine Positivschlüssel mittels der jeweiligen Nationalen Corona-App teilen kann, sind in den einzelnen Ländern verschieden. Während in Deutschland ein positiver Corona-Test von einem Labor oder einer Testeinrichtung attestiert werden muss, genügt andernorts die Selbstdiagnose eines Nutzers. Die Art und Weise, wie eine Infektion mit Corona bestätigt wurde, wird im Rahmen des EFGS als Metadatum zusammen mit dem jeweiligen Positivschlüssel übertragen. Um zu gewährleisten, dass nur eine hinreichend gesicherte Corona-Infektion zu einer Warnung von CWA-Nutzern und den sich daraus möglicherweise ergebenden Beeinträchtigungen für die betroffenen führt, verteilt der CWA-Server nur Positivschlüssel an die CWA-Apps, denen eine Attestierung durch ein Labor oder eine Testeinrichtung		akzeptabel
R1-CWA-Nutzer	165	Upload von falsch-positiven Ergebnissen auf Grund unzureichender Zuverlässigkeit der Prüfmechanismen des Bestehens einer Infektion über das Schweizer-Gateway	Soweit die Schweiz schwächeren Mechanismen zur Überprüfung einer Infektion mit SARS-CoV-2 etabliert hat bzw. einführt, können eine große Anzahl unzutreffend als infiziert bezeichneter Schlüssel an die CWA übertragen werden. Schwächere Mechanismen können z.B. in der Verwendung eines einzigen bekannten Codes zur Infektionsmeldung für eine Testeinrichtung bestehen. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	4	2	4	0	0	0	4	4	4	4	DM, VT, IG, IV, TR, ZB	Die Kriterien, nach denen ein Nutzer seine Positivschlüssel mittels des Schweizer Gateways teilen kann, kann sich unterscheiden. Die Art und Weise, wie eine Infektion mit Corona bestätigt wurde, wird auch im Rahmen des Schweizer Gateways als Metadatum zusammen mit dem jeweiligen Positivschlüssel übertragen. Um zu gewährleisten, dass nur eine hinreichend gesicherte Corona-Infektion zu einer Warnung von CWA-Nutzern und den sich daraus möglicherweise ergebenden Beeinträchtigungen für die betroffenen führt, verteilt der CWA-Server nur Positivschlüssel an die CWA-Apps, denen eine Attestierung durch ein Labor oder eine Testeinrichtung zugrunde liegt.	Die Kriterien, nach denen ein Nutzer seine Positivschlüssel mittels des Schweizer Gateways teilen kann, kann sich unterscheiden. Die Art und Weise, wie eine Infektion mit Corona bestätigt wurde, wird auch im Rahmen des Schweizer Gateways als Metadatum zusammen mit dem jeweiligen Positivschlüssel übertragen. Um zu gewährleisten, dass nur eine hinreichend gesicherte Corona-Infektion zu einer Warnung von CWA-Nutzern und den sich daraus möglicherweise ergebenden Beeinträchtigungen für die betroffenen führt, verteilt der CWA-Server nur Positivschlüssel an die CWA-Apps, denen eine Attestierung durch ein Labor oder eine Testeinrichtung zugrunde liegt.		akzeptabel
R4- Betreiber Server (T)	166	Mutwilliger Upload von falsch-positiven Schlüsseln durch eine staatliche Einrichtung, die berechtigter Weise an den EFGS angeschlossen war (EFGS-Risiko).	Ein Angreifer, der Zugang zu einem nationalen Backend erlangt, kann dieses nutzen, um über den EFGS durch den Angreifer generierte Diagnoseschlüssel zu verteilen. Der EFGS ist nicht in der Lage, festzustellen, ob ein nationales Backend in feindlicher Absicht betrieben wird. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	4	4	4	0	0	0	4	4	4	4	DM, VT, IG, IV, TR, ZB	DoS-Maßnahmen des EFGS verhindern DoS-Angriffe. Design-Entscheidungen EFGS T-2-3 (Sicherheitsstandards, Filterung), T 2-5. Um die EFGS-Datenbank gegen den Import nicht-autorisierter Daten zu schützen, werden die hochgeladenen Daten von den nationalen Backends signiert. Der Server überprüft die Signatur des Datenpakets anhand von Zertifikaten.	DoS-Maßnahmen des EFGS verhindern DoS-Angriffe. Design-Entscheidungen EFGS T-2-3 (Sicherheitsstandards, Filterung), T 2-5. Um die EFGS-Datenbank gegen den Import nicht-autorisierter Daten zu schützen, werden die hochgeladenen Daten von den nationalen Backends signiert. Der Server überprüft die Signatur des Datenpakets anhand von Zertifikaten.		akzeptabel
R4- Betreiber Server (T)	167	Mutwilliger Upload von falsch-positiven Schlüsseln durch eine staatliche Einrichtung, die berechtigter Weise an das Schweizer Gateway angeschlossen war	Ein Angreifer, der Zugang zum Schweizer Backend erlangt, kann dieses nutzen, um über das Schweizer Gateway durch den Angreifer generierte Diagnoseschlüssel zu verteilen. Die CWA ist nicht in der Lage, festzustellen, ob das über das Gateway angeschlossene Backend in feindlicher Absicht betrieben wird. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	4	4	4	0	0	0	4	4	4	4	DM, VT, IG, IV, TR, ZB	Abschluss eines (völker-)rechtlichen Vertrages mit der Schweiz erfolgt.			akzeptabel
R4- Betreiber Server (T)	168	Verteilung fehlerhafter Daten durch das EFGS auf Grund von Uploads durch berechtigter Weise angeschlossene nationale Backends (EFGS-Risiko).	Ein Angreifer könnte die Identität eines nationalen Backends oder des EFGS annehmen, um Daten an die nationalen Backends zu verteilen. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	3	3	3	0	3	0	0	0	0	3	DM, VT, IG, AT	Design-Entscheidungen EFGS T-1-1 (Nutzung von Algorithmen zur digitalen Signatur).	Design-Entscheidungen EFGS T-1-1 (Nutzung von Algorithmen zur digitalen Signatur).		akzeptabel
R4- Betreiber Server (T)	169	Verteilung fehlerhafter Daten über das Schweizer Gateway an die CWA	Ein Angreifer könnte die Identität des Schweizer Backends oder des Schweizer Gateways annehmen, um Daten an die CWA zu verteilen. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	3	3	3	0	3	0	0	0	0	3	DM, VT, IG, AT	Abschluss eines (völker-)rechtlichen Vertrages mit der Schweiz erfolgt. Schlüssel, die nicht von der Schweiz kommen, werden gelöscht. Zertifikats-Pinning im Einsatz.			aktzeptabel
R1-CWA-Nutzer	170	Manipulation von Daten durch Missbrauch der App und seiner Funktionalitäten (Smartphones mit einem Exposure Key werden z.B. in einem öffentlichen Verkehrsmittel ausgelegt und Kontakte erzeugt, ohne selbst dort zu sein).		Ja	3	0	0	2	0	0	0	0	0	0	6	IG	Restrisiko in Niutzerverantwortung.			akzeptabel mit Evaluation
R1-CWA-Nutzer	171	Angabe falscher Begegnungen (im KTB)	Wissentlich: falsche Namen, falsche Orte werden vom CWA-Nutzer im KTB eingetragen.	Ja	3	3	3	3	1	1	1	3	3	3	9	ZB, T, IV, VT,	Designentscheidungen zur Integration KTB (D-2-2b, D-6-2c, D-5-1-11, D-9-8, D-7-10).			akzeptabel, mit Evaluation
R2- Hacker	172	Manipulation von Begegnung (im KTB)	Bewusster Missbrauch - Unbefugter an Smartphone	Ja	2	3	3	3	1	1	1	3	3	3	6	ZB, T, IV, VT	Designentscheidungen zur Integration KTB (D-2-2b, D-6-2c, D-5-1-11, D-9-8, D-7-10).	Zusätzlicher Zugangsschutz durch CWA-Nutzer für besondere Bereiche (PIN).		akzeptabel, mit Evaluation
R4- Betreiber Server (T)	173	Manipulation von Daten innerhalb der OTC		Ja	2	0	3	3	0	0	0	0	0	0	6	IG	AVV mit DL, inkl. TOM Designentscheidung D-11-1.			akzeptabel mit Evaluation
R2- Hacker	174	Manipulation von Daten innerhalb der OTC		Ja	1	0	3	3	0	0	0	0	0	0	3	IG, VT	AVV mit DL, inkl. TOM Designentscheidung D-11-1.			akzeptabel
R2- Hacker	175	Manipulation von Daten auf Transportwegen (https)		Ja	2	0	3	3	0	0	0	0	0	0	6	IG, VT	AVV mit DL,inkl TOM Designentscheidung D-11-1.			akzeptabel mit Evaluation
R2- Hacker	176	Manipulation von Konfigurationseinstellungen eines gestohlenen/ ungeschützten Mobiltelefons		Ja	2	0	0	3	4	0	4	3	4	4	8	VF, R, TR, ZB	Restrisiko in Nutzerverantwortung Designentscheidung D-2.2-2.			akzeptabel mit Evaluation
R2- Hacker	177	Missbrauch der Upload-Autorisierung		Ja	2	1	3	3	0	0	0	0	0	1	6	IG	Bewertung aus Threat Modelling (AVV mit DL, inkl. TOM Designentscheidung D-11-1).			akzeptabel mit Evaluation
R2- Hacker	178	Manipulation der Parameter zum Abrufen und Hochladen von Tests		Ja	2	1	4	4	0	0	0	0	0	1	8	VT, IG	Designentscheidungen B-2-4/ Bewertung aus Threat Modelling .			akzeptabel mit Evaluation
R2- Hacker	179	Manipulation von Positiv-Schlüsseln		Ja	2	1	4	4	0	0	0	0	0	4	8	VT, IG, ZB	Designentscheidungen b-2-4/ Threat Modelling.			akzeptabel mit Evaluation
	180	**11) Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler)**																		
R4- Betreiber Server (T)	181	Ausfall/ Störung von IT und KT (inkl. Backup)		Ja	2	0	0	0	3	0	3	3	0	3	6	VF, R, IV, ZB	AVV mit DL, inkl. TOM , Designentscheidungen D-11-1.			akzeptabel mit Evaluation
R4- Apple / Google	182	Technische Grenzen des ENF bei Tracing		Ja	2	0	0	0	3	0	3	3	0	3	6	VF, R, IV, TR	DSK_Rahmendokument Kap. 14.20.4 iVm Designentscheidung zur Nutzung BLE-Technik und Vermeidung eines Rückgriffs auf Geolokalisationsdaten.			akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse + VT2: Kontaktfall + VT4: Infektfall + Eventregistrierung+Stopp der Warnungen (Stand: 22.05.2023)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R4- Apple / Google	183	Technische Grenzen des ENF von Apple/ Google (Backup/ Restore)		Ja	1	0	0	0	3	0	3	3	0	3	3	VF, R , IV, TR	DSK_Rahmenkonzept, Kap. 14.7 (Die Funktionalität des ENF ist von den Backup & Restore-Funktionen der jeweiligen Betriebssysteme **ausgenommen.** Durch das Einspielen eines Backups (Restore) auf ein mobiles Endgerät kann es daher nicht zu Verlusten oder Inkonsistenzen von eigenen Tagesschlüsseln oder RPIs kommen. Diese Frage ist auch im Zusammenhang mit dem Neuerwerb eines (gegebenenfalls gebrauchten) mobilen Endgerätes relevant. Bei der Übernahme eines gebrauchten mobilen Endgerätes sind keine Schlüssel mehr auf dem Gerät vorhanden, sofern es zuvor auf Werkseinstellungen zurückgesetzt wurde. Beim Wechsel des mobilen Endgerätes lautet die generelle Empfehlung, das alte Gerät weitere zwei Wochen parallel in Betrieb zu behalten. Durch die geltenden Aufbewahrungs- und Löschzeiten ist ein vollständiger und konsistenter Datenbestand auf dem neuen Gerät nach zwei Wochen hergestellt.			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	184	Unsichere Programmierung		Ja	2	4	4	4	4	4	4	4	4	4	8	VT, IG, VF, A, R, IV, TR, ZB, DM	Designentscheidungen D-11-1 / AVV mit DL, inkl. TOM.			akzeptabel mit Evaluation
R4- Betreiber Server (T)	185	Fehlkonfiguration von sicherheitsbezogenen Unterstützungssystemen (EFGS-Risiko)	Unbeabsichtigte Änderung von Informationen und personenbezogenen Daten - Die Verfälschung von Diagnoseschlüsseln kann zum Verlust oder zur Beschädigung personenbezogener Daten führen. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	4	4	4	4	4	4	4	4	4	4	DM, VT, IG, VF, AT, RE, IV, TR, Z	Vertrag mit DL (Betrieb EFGS).			akzeptabel
R1-CWA-Nutzer	186	Nicht-Verfügbarkeit auf Grund Inkompatibilität des EFGS mit dem mobilen Endgerät des Nutzers (EFGS-Risiko)	Nicht-Verfügbarkeit von EFGS-Funktionen (Upload/ Download von Diagnoseschlüsseln) für Nutzer der mobilen Applikationen. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	0	0	0	4	0	4	2	0	2	4	VF, RE				akzeptabel
R1-CWA-Nutzer	187	Überlastung des mobilen Endgeräts des Nutzers auf Grund des Herunterladens zu großer Datenpakete im Zusammenhang mit dem EFGS (EFGS-Risiko)	Risiko des Überlastens der mobilen Applikation und Frustration der Nutzer kann zur Deinstallation der App führen. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	3	0	0	0	4	0	4	2	0	2	12	VF, RE	Vertrag mit DL (Betrieb EFGS), TOM.		Das Überlastungsrisiko könnte durch die Auswertung des Col-Parameters in dem nationalen Backend gelöst werden. Hier bestehen dann allerdings eventuell die bekannten Erfassungslücken. Wenn eine solche Überlastung beobachtet wird, könnte man dem mit einer Umstellung auf das Traveller Pattern oder Col begegnen. Allerdings müsste so was dann europaweit vollzogen werden.	bedingt akzeptabel
R1-CWA-Nutzer	188	Überlastung des mobilen Endgeräts des Nutzers auf Grund des Herunterladens zu großer Datenpakete im Zusammenhang mit dem Schweizer Gateway	Risiko des Überlastens der mobilen Applikation und Frustration der Nutzer kann zur Deinstallation der App führen. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	2	0	0	0	4	0	4	2	0	2	8	VF, RE	Abschluss eines (völker-)rechtlichen Vertrages erfolgt.			aktzeptabel mit Evaluation
R4- Betreiber Server (T)	189	Vorübergehende oder permanente Nicht-Verfügbarkeit der vom EFGS dem nationalen Backend bereitgestellten Daten, z.B. auf Grund von Fehlfunktionen, Problemen mit Zertifikaten und Autorisierungsfunktionen (EFGS-Risiko)	Keine weitere Beschreibung erforderlich. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	3	0	0	0	3	0	3	2	0	2	9	VF, RE	Zusätzlich müssen Schnittstellen Status- und Fehlermeldungen vorsehen, um festzustellen, ob emeute Uploads oder ähnliche Maßnahmen erforderlich sind. Zertifikate auf Ebene (1) Infrastruktur (DIGIT), (2) Betrieb EFGS (T-Systems), (3) Infrastruktur der nationalen App. Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: ST_business_continuity_management.doc, ST_incident_mgt.doc			akzeptabel mit Evaluation
R4- Betreiber Server (T)	190	Vorübergehende oder permanente Nicht-Verfügbarkeit der Upload-Funktion des EFGS, z.B. auf Grund von Fehlfunktionen, Problemen mit Zertifikaten und Autorisierungsfunktionen (EFGS Risiko)	Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	3	0	0	0	3	0	3	2	0	2	9	VF, RE	Zusätzlich müssen Schnittstellen Status- und Fehlermeldungen vorsehen, um festzustellen, ob emeute Uploads oder ähnliche Maßnahmen erforderlich sind. Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: ST_business_continuity_management.doc, ST_incident_mgt.doc			akzeptabel mit Evaluation
R4- Betreiber Server (T)	191	Vorübergehende oder permanente Nicht-Verfügbarkeit der Upload-Funktion des Schweizer Gateway Servers, z.B. auf Grund von Fehlfunktionen, Problemen mit Zertifikaten und Autorisierungsfunktionen	Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	3	0	0	0	3	0	3	2	0	2	9	VF, RE	Abschluss eines (völker-)rechtlichen Vertrages erfolgt.			aktzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	192	Nutzung von Komponenten mit bekannten Schwachstellen (BLE Technik)		Ja	3	0	0	0	0	0	0	4	4	4	12	VT, T, ZB	Designentscheidungen zur Nutzung der BLE-Technik/ Empfehlung an Nutzer, die empfohlenen Sicherheitspatches einzuspielen.		Zwischenzeitlich liegt eine Stellungnahme des BSI vor, wonach keine zusätzlichen Sicherheitsrisiken durch Nutzung der Bluetooth-Technologie gesehen werden.	bedingt akzeptabel,
R4 - Softwareentwickler / SAP	193	Kollisionen von BLE Nachrichten bei Agglomerationen (begrenzt auf 20 Kanäle); bei großen Mengen könnte es zu Kollisionen und Neuübertragungen kommen		Ja	3	0	0	4	0	4	0	0	0	4	12	A, ZB	Designentscheidungen zur Nutzung der BLE-Technik/ laufende Beratung durch Forschungseinrichtung (CISPA)		Zwischenzeitlich liegt eine Stellungnahme des BSI vor, wonach keine zusätzlichen Sicherheitsrisiken durch Nutzung der Bluetooth-Technologie gesehen werden.	bedingt akzeptabel,
R4- Betreiber Server (T)	194	Security-Fehlkonfiguration		Ja	2	4	4	4	4	4	4	4	4	4	8	VT, IG, VF, A, R, IV, ZB, TR; DM	AVV mit DL, inkl. TOM , Designentscheidungen D-11-1.			akzeptabel mit Evaluation
R1-CWA-Nutzer	195	Fehlende Verfügbarkeit durch Nutzung Smartphone ohne ENF (iOS ab Version 13.5)		Ja	2	0	0	0	2	0	2	2	0	2	4	ZB, VF, R, IV	Designentscheidung D-1-5.			akzeptabel
R1-CWA-Nutzer	196	Ignorieren von Warnungen anderer aufgrund veralteter CWA-Apps (Ablauf der Übergangszeit nach Release 2.8)	Mit [Release 2.8] der CWA-App wird die ursprüngliche Event Registrierung nach der Apple Anforderung für eine konforme Event-Registrierung angepasst. Im Vergleich zur ursprünglichen Event-Registrierung werden die Event-IDs verschlüsselt auf dem CDN-Magenta abgelegt. Ältere CWA App-Versionen (vor 2.8) werden die ursprüngliche Event Registrierung weiterhin nutzen. Die neuen Versionen der CWA-App (ab 2.8) werden die Anforderung von Apple für die Event-Registrierung erfüllen. Daher handelt es sich bei der Anpassung um eine inkompatible Änderung, die ein Update der App erforderlich macht, um die neue Kontaktverfolgung über die Event-Registrierung nutzen zu können. Es wurde abgestimmt, dass die Event-IDs für eine Übergangszeit sowohl in der ursprünglichen Form als auch in der neuen Form auf dem CWA-Backend angelegt werden. Nach dem Ablauf der Übergangszeit wird nur noch die neue Form der Event-Registrierung unterstützt. Sofern der CWA-Server nach dem Ablauf der Übergangszeit Daten zur Event-Registrierung in der ursprünglichen Form erhält, werden diese vom CWA-Server nicht prozessiert. CWA-Apps, die die ursprüngliche Form der Event-Registrierung nutzen, sind dann nicht mehr in der Lage, die Daten in der Apple konformen Variante zu verarbeiten.	Ja	3	0	0	0	3	0	0	0	0	0	9	VF	CWA-Nutzer können auf die neuere Version wechseln.			akzeptabel mit Evaluation
R4- Apple / Google	197	Fehlfunktion/ fehlende Justierbarkeit des Algorithmus, mit dem das Infektionsrisiko anhand von Abstands-/ Zeitfaktoren gemessen wird		Ja	2	0	0	0	0	0	0	4	4	4	8	IV, TR, ZB	Nutzerverantwortung (Designentscheidungen D-2-2).			akzeptabel mit Evaluation
R4- Apple / Google	198	Fehlfunktionen bei Backup & Restore führt zu Verlusten oder Inkonsistenzen von (Positiv-)Schlüsseln oder RPI		Ja	1	0	0	0	3	0	3	3	0	3	3	VF, R	siehe Z 114			akzeptabel mit Evaluation
R1-CWA-Nutzer	199	Unsachgemäße Verwendung eines Mobilfunkgerätes für Zwecke der CWA/ Verlust des Gerätes (siehe Z 95)		Ja	2	4	4	4	0	0	0	4	4	4	8	ZB, T, IV	Nutzerverantwortung (Designentscheidungen D-2-2).			akzeptabel mit Evaluation
R1-CWA-Nutzer	200	Unsachgemäße/ unberechtigte Vernichtung und Löschung von Daten (Mobilgerät)		Ja	2	0	0	4	4	0	4	4	4	4	8	ZB, T, IV	Siehe Ausführungen zur Löschung in dem DSK CWA (Restrisiko beim Nutzer).			akzeptabel mit Evaluation
R1-CWA-Nutzer	201	Unsachgemäße/ unberechtigte Vernichtung und Löschung von Daten (Server)		Ja	1	0	0	4	4	0	4	4	4	4	4	ZB, T, IV	AVV mit DL,inkl. TOM , Designentscheidungen D-11-1.			akzeptabel
R1-CWA-Nutzer	202	Fehlgebrauch/ Fehlbedienung der Anwendungen der CWA/ falsche Zuordnung von Daten (falsche Auswahl von Empfänger, falsche Eingabe, falsche Dokumentation)		Ja	2	2	2	2	2	2	2	2	2	2	4	ZB, T, IV ; DM, VT, IG…	Designentscheidungen zur Integration KTB (D-2-2b, D-6-2c, D-5-1-11, D-9-8, D-7-10).			akzeptabel
R1-CWA-Nutzer	203	Beabsichtigte/ Unbeabsichtigte unsachgemäße Verwendung eines Mobilgerätes (keine Kontrolle durch die App, dass Person ihr Gerät bei sich führt , Nutzung verschiedener Geräte und durch verschiedene Personen)		Ja	2	4	4	4	0	0	0	4	4	4	8	ZB, TR, IV , VT, IG	Auf Grund der bewussten Entscheidung, auf Personenbezug zu verzichten, kann die Mehrfachnutzung der CWA-App durch einen einzigen Anwender nicht ausgeschlossen werden. Restrisiko ist beschrieben im DSK Rahmendokument.			akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse + VT2: Kontaktfall + VT4: Infektfall + Eventregistrierung+Stopp der Warnungen (Stand: 22.05.2023)				Risikobewertung															
						Schadensausmaß													
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R4 - Softwareentwickler / SAP	204	Sekundärnutzung bei der zentralen Vergabe der ID-Token (GUID)		Ja	1	1	4	4	0	2	0	4	2	4	4	ZB; IV, VT, IG, DM	Designentscheidungen D-7-8.			akzeptabel
R2- Hacker	205	Großflächiges Bluetooth Hacking/ Bluetooth Jam (Angreifer können mit einem sehr starken Signal das gesamte Funkspektrum beeinträchtigen, so dass in ca. 20m Umfang kein Austausch von Beacons mehr möglich ist)		Ja	3	1	3	3	1	1	1	1	1	1	9	IT, VT	Siehe Designentscheidungen zur Nutzung der BLE-Technik, Risiken werden weiter betrachtet, mit dem Ziel, die Technik unangreifbarer zu machen, Schwachstellen zu minimieren.			akzeptabel mit Evaluation
R2- Hacker	206	Spoofing App (Identität verschleiern)		Ja	4	4	4	4	4	4	4	4	4	4	16	VT, DM, ZB, TR, IV, VG, A, R	Designentscheidungen B-1-1f.	Böswillige Angreifer können versuchen, Benutzer davon zu überzeugen, eine alternative Anwendung mit gleichem/ ähnlichen Namen und Icon zu nutzen, um bösartigen Inhalt und/ oder Funktionalität zu verbreiten.	Es gibt keine technischen Möglichkeiten, um dies auszuschließen. Risiko liegt in der Grundsatzentscheidung begründet, ENF und BLE zu nutzen.	Es gibt keine technischen Möglichkeiten, um dies auszuschließen. Risiko liegt in der Grundsatzentscheidung begründet, ENF und BLE zu nutzen.
R2- Hacker	207	DNS-Spoofing / Man-in-the-Middle Attacke, um statt mit legitimen Backend mit einem Server seiner Wahl zu kommunizieren (Vorgetäuschter Server)	Durch DNS Spoofing oder eine Man-in-the-Middle Attacke könnte ein Angreifer die CWA-App dazu bringen, statt mit den legitimen Servern mit einem Server seiner Wahl zu kommunizieren. Das betrifft sowohl den CWA-Server als auch den Verifikationsserver. Durch Senden unzulässiger oder gefälschter Inhalte könnte der Angreifer die Funktion der CWA-App beeinträchtigen oder gar zum Erliegen bringen. Außerdem kann er sich so Zugriff auf Informationen verschaffen, die nicht für ihn bestimmt sind, und versuchen, beispielsweise über Metadaten der Netzwerkverbindung einen Personenbezug herzustellen.	Ja	2	0	0	0	4	4	4	4	4	4	8	VT, DM, ZB, T , IV	Designentscheidungen B-1-5ff. Als Abwehrmaßnahmen werden neben einer strikten Inputvalidierung TLS-Zertifikatvalidierung und -Pinning eingesetzt. Auf Grund des etablierten Zertifikatpinnings wird ein Einsatz von DNSSEC auf Serverseite derzeit nicht für notwendig erachtet.			bedingt akzeptabel mit Evaluation
R2- Hacker	208	DNS-Spoofing/ Man-in-the-Middle Angriffe auf den EFGS (EFGS - Risiko)	Ein Angreifer könnte ein nationales Backend täuschen, mit einem Server nach seiner Wahl zu kommunizieren an Stelle mit dem dem EFGS. Hierzu können DNS-Spoofing und Man-in-the-Middle Angriffe eingesetzt werden. Diese Art von Angriff kann auch umgekehrt gegen den EFGS durch ein feindliches Backend geführt werden. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	1	0	3	3	0	0	0	2	0	2	3	VT, IG	Design-Entscheidungen EFGS T-1-2 (HTTP Public Key Pinning); Um einen Kommunikationspartner (EFGS/nationales Backend) zu authentifizieren, verwendet das System digitale Signaturen.			akzeptabel
R2- Hacker	209	Denial of Service-Angriffe auf die EFGS Server mit der Folge der beabsichtigten Überlastung (EFGS - Risiko)	Ein Angreifer kann einen Denial-of-Service Angriff zur Störung des EFGS verwenden. Sind die Funktionen des EFGS nicht verfügbar, können Diagnoseschlüssel nicht geteilt werden. Gelingt es dem Angreifer, große Mengen falscher Diagnoseschlüssel in den EFGS einzuschleusen, werden diese eventuell automatisch an die nationalen Backends verteilt. Diese werden so auch Opfer des Angriffs. Ein solcher Angriff kann zudem zu Einschränkungen des Netzwerkzugangs und der Verarbeitungsverfügbarkeit des EFGS führen. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	3	0	3	0	3	0	3	2	0	2	9	VT, VF, R	Design-Entscheidungen EFGS T-5-2, T-5-3 und T-5-4 (DoS Absicherung im Betrieb).			akzeptabel mit Evaluation
R2- Hacker	210	Denial of Service-Angriffe auf das Schweizer Gateway mit der Folge der beabsichtigten Überlastung	Ein Angreifer kann einen Denial-of-Service Angriff zur Störung des Schweizer Gateways verwenden. Sind die Funktionen des Gateways nicht verfügbar, können Diagnoseschlüssel nicht geteilt werden. Gelingt es dem Angreifer, große Mengen falscher Diagnoseschlüssel in das Schweizer Gateway einzuschleusen, werden diese eventuell automatisch an die CWA verteilt. Diese wird so auch Opfer des Angriffs. Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	3	0	3	0	3	0	3	2	0	2	9	VT, VF, R	Abschluss eines (völker-)rechtlichen Vertrages erfolgt.			akzeptabel mit Evaluation
R2- Hacker	211	Denial of Service Angriffe durch Missbrauch der CWA-App	Ein solcher Angriff kann zudem zu Einschränkungen des Netzwerkzugangs und der Verarbeitungsverfügbarkeit des EFGS führen. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	3	0	0	0	3	2	3	0	0	0	9	VF, TR	Designentscheidungen D-5.1-16.			akzeptabel mit Evaluation
R2- Hacker	212	Denial of Service (mutwillige Überlastung) Angriffe auf Server durch Laden ungültiger Daten		Ja	3	0	0	0	3	2	3	0	0	0	9	VF, R	AVV mit DL, inkl. TOM , Designentscheidungen D-11-1.			bedingt akzeptabel mit Evaluation
R4 - Google/ Apple; CWA-Entwickler, Server-/ Internet-Betreiber	213	Fehlendes oder unzureichendes Test- und Freigabeverfahren		Ja	1	4	4	4	4	4	4	4	4	4	4	VT, IG, VF, A, R, IV, T, ZB	Erfolgt im Projekt (siehe Testkonzept).			akzeptabel
	214	**12) Verarbeitung über die Speicherfrist hinaus**																	
R4- Apple / Google	215	Unbefristete Speicherung von Daten (inkl. Metadaten) auf der App und mögliche spätere Verkettung		Ja	3	4	1	1	0	0	0	3	3	4	12	DM, ZB	Designentscheidungen D-11-1/ AVV mit DL inkl. TOM.		Die Grundsatzentscheidung für das Framework von Apple/ Google bedingt das Vertrauen der Nutzer in diese Plattformen.	bedingt akzeptabel,
R4- Betreiber Server (T)	216	Unbefristete Speicherung von Daten (inkl. Metadaten) in DB und mögliche spätere Verkettung mit anderen personenbezogenen Daten		Ja	3	4	1	1	0	0	0	3	3	4	12	DM, ZB	Designentscheidungen D-11-1/ AVV mit DL inkl. TOM; DSK_Rahmenkonzept Kap. 14.20.2 (Das Löschen von Positiv-Schlüsseln auf der Datenbank des CWA-Servers sowie auf dem Objectstore, der als Übergabemedium zum CDN-Magenta dient, erfolgt mit den vom jeweiligen Speicherservice angebotenen Mitteln. Ein Ausnullen der betroffenen Speicherbereiche wird nicht vorgenommen. Diese Vorgehensweise erscheint aus mehreren Gründen vertretbar: Zum einen liegen beide Speichermedien im geschützten Bereich der OTC, zum anderen kann bei Positiv-Schlüsseln kein Personenbezug hergestellt werden. Zudem werden die Positiv-Schlüssel über CDN-Magenta publiziert und millionenfach an mobile Endgeräte verteilt, sodass die Löschung an zentraler Stelle nur von begrenzter Bedeutung ist).		Die Grundsatzentscheidung zur Nutzung der IT-Infrastruktur der OTC bedarf das Vertrauen der Nutzer in die Betreiber und deren rechtskonformes Verhalten.	bedingt akzeptabel,
R4- Betreiber Server (T)	217	Unbegrenzte Speicherung überflüssiger personenbezogener Daten (z.B. relevante Länder, vermittelt durch EFGS) (EFGS - Risiko)	Ein Teilen des Herkunftskennzeichens für Diagnoseschlüssel über die nationalen Backends hinaus kann die Herkunft von Personen hinter den Diagnoseschlüsseln offenbaren. Mit dem [Release 3.1] wird das EFGS temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	3	1	1	1	0	0	0	1	1	1	3		Löschen der Daten erfolgt im nationalen Backend.			akzeptabel
R4- Betreiber Server (T)	218	Unbegrenzte Speicherung überflüssiger personenbezogener Daten, vermittelt über Schweizer Gateway	Das CHGS wurde mit dem [Release 2.21] temporär (bis auf Weiteres) außer Betrieb genommen.	Ja	2	1	1	1	0	0	0	1	1	1	2		Löschen der Daten erfolgt im Schweizer Backend.			akzeptabel
R1-CWA-Nutzer	219	Unbefristete Speicherung der Daten des KTB	Durch Nutzung der Exportfunktion (Druck, pdf) könnten die Daten für den CWA-Nutzer über den Zeitraum von 16 Tagen zur Verfügung stehen.	Ja	3	2	3	3	1	1	1	3	3	3	9	VT, IV, TR, ZB	Designentscheidungen zur Integration KTB (D-2-2b, D-6-2c, D-5-1-11, D-9-8, D-7-10).			akzeptabel, mit Evaluation
R1-CWA-Nutzer	220	Event-Registrierung: Fehlende Löschung des QR-Codes	Retentionperiod: 15 Tage.	Ja	1	1	0	0	1	0	1	1	1	1	1	0	Designentscheidungen zur Eventregistrierung (D-2-1a, D-2-2d, D-5.1-15a, D-6-2d, D-9-8a).			akzeptabel
R4- Betreiber Server (T)	221	Unbefristete Speicherung unrichtiger/ negativer/ nicht-notwendiger Daten		Ja	1	4	4	4	0	0	4	2	4	4	4	DM, ZB	Designentscheidungen D-11-1/ AVV mit DL inkl. TOM.			akzeptabel
R4- Apple / Google	222	[Release 3.2]: Fehlende Datenlöschung durch Äpple / Google nach Einstellung der Warnungen	Warnungen sind nur noch bis zum 30.03.233 möglich. Soweit das ENF über diesen Zeitpunkt hinaus aktiv ist, könnte das Tracing weiter erfolgen.	Ja	2	2	2	0	2	0	0	2	2	2	4	DM, VT, TR, IV, ZB	Zum 01.08.2023 wird CWA serverseitig der ENF Stopp bereit für die BS Android und iOS abgesetzt. Die Betreiber setzen dies unterschiedlich um. Apple:			akzeptabel
R4- Apple / Google	223	[Release 3.2]: Nicht erforderliche Datenverarbeitung mangels De-Installation der CWA durch Nutzer	Stopp-Bereit (siehe etablierte Maßnahme für Risiko in Zeile 220) für ältere Versionen möglicherweise nicht wirksam. Deinstallation durch CWA Nutzer daher ratsam. Wenn dies nicht erfolgt, dann möglicherweise weiterhin Tracing unter Verwendung ENF, zum 30.4. sind keine Warnungen mehr möglich. Die Server /	Ja	3	3	3	0	3	0	0	1	3	3	9	DM; VT, TR, ZB, VF	Auf die Möglichkeit zur manuellen De-Aktivierung des ENF wird in den FAQ zwar hingewiesen, aber im Hinweistext des "Vielen-Dank-Screens" (Home-Screen) der CWA wird darum gebeten, die CWA App nicht zu löschen. Mithin erhöht sich die EW, dass			akzeptabel
R4- Betreiber Server (T)	224	[Release 3.2]: Nicht erforderliche Datenverarbeitung nach Einstellung der Warnungen durch TSY oder SAP	CDN sind nicht mehr erreichbar. Löschung erfolgt entsprechend Löschkonzept. In der CWA werden Funktionen (Datenspende) abgeschalten. Im KTB werden Kontaktbegegnungen automatisch nach Fristablauf gelöscht. Die Stammdaten der	Ja	2	2	1	1	1	1	1	1	2	2	4	DM, ZB, VF, TR	Löschung entsprechend Löschkonzepten.			akzeptabel
	225	**13) Risiken durch Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt**																	
	226	DV ohne fehlende/ hinreichende epidemiologisch signifikante Wirksamkeit			3	4	4	4	4	4	4	4	4	4					

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse + VT2: Kontaktfall + VT4: Infektfall + Eventregistrierung+Stopp der Warnungen (Stand: 22.05.2023)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
	227	Freiheitsgewinne bei Nutzung der App (Immunitätsausweis, Zugangserleichterung zu staatlichen/ kommunalen Leistungen)																		
	228	Freiheitsbeschränkungen bei Nicht-Nutzung der App (Zugangsbeschränkungen zu staatlichen/ privaten Leistungen)																		
	229	Gewöhnung an Überwachung durch Staat und Markt	Mit Einführung des KTB könnte sich das Risiko erhöhen, dass es normaler wird, sich nicht mehr anonym treffen zu können. Dies eröffnet das Potential, dass Personen ggf. ihr Verhalten ständig kontrollieren und anpassen.	Ja	1	1	1	1	0	0	0	1	1	1	1					akzeptabel
	230	Fehlende Akzeptanz der App/ keine freiwilliger Nutzung durch Bevölkerung/ Widerruf oder Unwirksamkeit der Einwilligungen als Risiko für Zielerreichung (Kann "Contact Tracing" dabei helfen, die Infektionszahlen signifikant zu senken?)	[Release 1.10]: Die Einführung eines KTB könnte die Akzeptanz der App senken, weil damit erstmals personenbezogene Daten eingetragen können. [Release 1.12]: Die zusätzliche Einführung der Kontakthistorie könnte zu einem weiteren Akzeptanzverlust führen, weil nicht mehr in die pseudonyme Datenverarbeitung vertraut wird; die Re-Identifikationsrisiken in Zeiten harter Restriktionen steigen.	Nein	4	0	0	0	0	0	0	0	0	4	-	DM, ZB, U	Designentscheidungen D-2.2-3, DSK_Rahmenkonzept, Kap. 14.20.3.			
R4- Betreiber Server (T)	231	Akzeptanzverlust durch Publikation falscher statistischer Daten in der CWA (in-App-Statistik - ab CWA [Release 1.11])	Keine in der DSFA zu betrachtenden Risiken für den Einzelnen. Aber Risiko für Akzeptanz und epidemiologischen Nutzen der CWA-App: Angenommen die In-App-Statistik-Kachel würde anzeigen, das 50.000 Leute neu infiziert wurden und fälschlicherweise anzeigen, dass nur 50 (wamende Personen in der In-App-Statistik-Kachel) ihre Schlüssel geteilt haben. CWA-Nutzer könnten Vertrauen in die Wirksamkeit verlieren und die CWA-App deinstallieren.													IG der statistischen Daten	DSK_Rahmenkonzept v.12, Kap. 14.27.			