

Datenschutzrisikoausschätzung (DSFA)			Risikobewertung																	
VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung inkl. Kontakt-Historie: 22.01.2024)			Schadensausmaß																	
Risiko-Quelle	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datensammlung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Interventierbarkeit	Transparenz	Zuschreibung / Nichtverteilung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko	
	Unbefugte oder unrechtmäßige Verarbeitung durch CWA																			
R8- Behörden	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.	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	
	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 (Widerruf) D-3.1-8			akzeptabel	
R8- Behörden	Datenverarbeitungen ohne Rechtsgrundlage mittels EFGS: Jede Art von nochmaligem Upload durch empfangende nationale Backends 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 herunterladende nationale Backend.	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	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	siehe Anlage 7, Ziff. 2.3.2 (3)	bedingt akzeptabel	
R1-CWA-Nutzer	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 im 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	Unrechtmäßige DV bei Eintrag Kontaktpersonen in KTB (inkl. falscher Eintrag)	Risiken für die Persönlichkeitsrechte derjenigen Personen, die in KTB eingetragen werden.	Ja	3	2	2	2	1	1	1	2	2	2	6	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	Unwirksame Einwilligung durch fehlende Freiwilligkeit ("erzwungene Einwilligung") // erzwungene Freiwilligkeit		Ja	1	4	4	4	4	4	4	4	4	4	4	RM	siehe Z 5 und Datenschutzinformationen / Abgestimmte Datenschutzinformationen liegt vor (DSK-Verifikation und Testergebnis, 9.1 (mitgeltende Dokumente Datenschutzerklärung)			akzeptabel	
R1-CWA-Nutzer	erzwungene Freiwilligkeit der DV von pD 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	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 (siehe oben, Z5)			akzeptabel	
R1-CWA-Nutzer	Unwirksame Einwilligung aufgrund fehlender Information über Umfang und Folgen		Ja	2	4	4	4	4	4	4	4	4	4	8	DM, VT, IG, IV, TR, ZB	Abgestimmte Datenschutzinformationen liegt vor (DSK-Verifikation und Testergebnis, 9.1 (mitgeltende Dokumente Datenschutzerklärung)			akzeptabel, mit Evaluation und ggf. Anpassung Datenschutzerklärung	
R1-CWA-Nutzer	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	Datenschutzinformationen in leichter Sprache, Übersetzungen			akzeptabel, mit Evaluation fehlendes ggf. Anpassung Datenschutzerklärung	
R1-CWA-Nutzer	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	Siehe Designentscheidungen D-3.1-2	Für Phase 2 ist ein zusätzliches Popup-Fenster mit dem Hinweis für Jugendliche unter 16 geplant. Sinngemäß: "Wenn du unter 16 Jahre alt bist, dann besprich bitte die Nutzung der App mit deinen Eltern." (Dies kommt nicht in Version 1.2 -1.5))	Gemeinsame Entwicklung der Lösung im Workstream, siehe DSFA-Bericht	bedingt akzeptabel	
R4- Apple / Google	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)	Abhängigkeiten von Dienstleistern/ Software Herstellern (Ausfall externer Dienstleister) - SAP / T, DIGIT (EFGS)		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)	Abhängigkeit des Betriebs des EFGS von der Verfügbarkeit des Infrastruktur der nationalen Backends der Corona Warning Systeme der Mitgliedsstaaten (EFGS - Risiko)	Einschränkung oder Verlust der Verfügbarkeit der Datenverarbeitungsfunktionen (grenzüberschreitende Verteilung von Diagnoseschlüsseln).	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	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 mögl.), siehe Dokument "Designentscheidungen D-5.1-1			akzeptabel, mit Evaluation	
R4- Betreiber Server (T)	Fehlende unzureichende vertragliche Regelungen mit Dienstleistern (Auftragsverarbeitung/ Vertrag zur gemeinsamen Verantwortung) - mit T/SAP + DIGIT/ TSI (EFGS)		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	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)	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 - Z15 (Pseudonyme auch auf Backend)			akzeptabel	
R4- Apple / Google	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	siehe Z 13		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)	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	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	
	Verarbeitung wider Treu und Glauben																			
R1-CWA-Nutzer	Alarmmüdigkeit (mehrmalige Alarmierung inkl. Quarantäne-Empfehlung innerhalb kurzer Zeit) - Nachjustierung		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	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 beschrieben (D-2-7).	bedingt akzeptabel,	
R1-CWA-Nutzer	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 Modeling/ AVV mit DL, inkl. TOM Designentscheidung D-11-1			akzeptabel	
R2- Hacker	Vortäuschen von Kontaktereignissen durch Duplizierung von BLE-Beacons		Ja	3	0	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	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	

Datenschutzroignisausnatzung (DSFA)			Risikobewertung																
VT 1: App-seitige Verarbeitung Kontakttereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung inkl. Kontakt.Historia: 22.01.2024)			Schadensausmaß																
Risiko-Quelle	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datensammlung	Verarbeitheit	Integrität	Verfügbarkeit	Authenzität	Resilienz	Intervierbarkeit	Transparenz	Zuschreibung / Nichtverleitung	Risikoklasse	Soil-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R6 - Krimineller	Herstellung mutwilliger, massenhafter Kontakte durch positiv Getestete (infolge Fehlverhalten Nichtbeachtung Quarantäne-Empfehlung) vor Upload Testergebnis 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)	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	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 positiv auf Corona getesteter Nutzer sowohl mit dem Transmission Risk als auch DSOS und Report Type als Attributen. Während die			
	Für die Betroffenen intransparente Verarbeitung													0					
R8- Behörden	Unvollständige, unverständliche Datenschutzinformationen für CWA App und Backend (inkl. Funktionalitäten der CWA)		Ja	1	2	2	2	0	0	0	3	4	4	4	TR, ZB	Datenschutzinformation (siehe Z10)			akzeptabel
R1-CWA-Nutzer	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.	Ja	3	2	2	2	0	0	0	2	2	2	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	Unvollständige, unverständliche Datenschutzinformationen für API / ENF		Ja	2	2	2	2	0	0	0	3	4	4	8	TR, ZB	Datenschutzinformation (siehe Z10)			akzeptabel mit Evaluation
R4- Betreiber Server (T)	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	Datenschutzinformation (siehe Z10)			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	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	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
	Unbefugte Offenlegung von und Zugang zu Daten																		
R1-CWA-Nutzer	(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 Handnutzung/ Restrisiko beim Nutzer - Designentscheidung D-2-2			akzeptabel
R1-CWA-Nutzer	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 Handnutzung/ Restrisiko beim Nutzer - Designentscheidung D-2-2			akzeptabel
R1-CWA-Nutzer	Unbewusste Offenlegung von Kontakteinträgen in KTB (shoulder surfing)	Unbefugte Dritte könnten durch einen Blick über die Schulter des CWA-Nutzers während des Eintrages Kenntnis von id der Kontakte erhalten. Ab Release 1.12, Zufällig könnte Risikobewertung Person zugeordnet werden. 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. Veröffentlichung der Daten durch Privatpersonen über soziale Netzwerke usw.). Ebenso könnte der CWA-Nutzer die Exportfunktion (E-Mail) nutzen, ohne diese nach Stand der Technik gegen unbefugten Zugriff zu schützen	Ja	3	2	2	2	1	1	1	2	2	2	4	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	bewusste Offenlegung von KTB an (unbefugte) Dritte (Nutzung der Exportfunktion)		Ja	3	3	3	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	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 Handnutzung/ Designentscheidungen (Containerisierung CWA - Designentscheidung D-2-2			akzeptabel mit Evaluation
R4- Apple / Google	Unbefugter Zugriff von Plattformen, die Kontakttereignisse ermitteln, auch für NutzerInnen 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	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	Zugang/ Zugriff auf (Gesundheits-) Daten in CWA - Backend (z. . Infolge 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	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	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	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-5.1-11a/ 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-5.1-1a, DSK_Rahmenkonzept Kap. 14.8			akzeptabel mit Evaluation
R2- Hacker	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 verrügaren Metadaten der Positivschlüssel im Zuge der Weiterentwicklung der CWA erscheint es angeraten, die oben beschriebene Mindestpaketgröße für Positivschlüssel in Zukunft (durch das nachfolgende Dokument) zu erhöhen.		akzeptabel
R2- Hacker	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-Anpassung auf	Ja	1	1	4	3	2	0	0	0	0	4	4	ZB, VT, IG	USK_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	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	Abhören des Bluetooth - Verkehrs		Ja	2	1	2	2	0	0	0	2	2	2	4	VT, ZB, TR	siehe Dokument Designentscheidungen zur Nutzung der BLE-Technik. Risiken werden weiter betrachtet, mit dem Ziel, die Technik unangreifbarer zu machen, Schwachstellen zu minimieren (B-4-2)			akzeptabel
R2- Hacker	Zugriff auf Positiv - 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 / Zugangsicherung + Designentscheidungen (Verschlüsselung auf Transportwegen) - Designentscheidungen B-4-1			akzeptabel mit Evaluation
R2- Hacker	Zugriff auf Positiv-Schlüssel, Rückrechnung RPI und Nachbau ENF mit z.B. Ortsdaten 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 / Zugangsicherung + Designentscheidungen (Verschlüsselung auf Transportwegen) - Designentscheidungen B-4-1			akzeptabel
R2- Hacker	Zugriff auf Positiv-Schlüssel, Rückrechnung RPI und Nachbau ENF mit z.B. Ortsdaten 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 / Zugangsicherung + Designentscheidungen (Verschlüsselung auf Transportwegen) - Designentscheidungen B-4-1			akzeptabel mit Evaluation

Datenschutzrisikoprüfung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung inkl. Kontakt-Historie: 22.01.2024)			Risikobewertung																
Risiko-Quelle	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (Ja/nein)	EW	Schadensausmaß									Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
					Datensensibilisierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zerschließung / Nichtverteilung						
R2- Hacker	Unbefugte Offenlegung durch Metadaten-Korrelation		Ja	2	0	4	4	0	0	0	0	0	4	8	ZB	Designentscheidungen/ TOM (siehe Z 41)/ Threat Modeling/ Korrelation verhindern durch Trennung von Meta- und Nutzdaten/ Keine TAN - Speicherung auf Verifikation Server			akzeptabel mit Evaluation
R2- Hacker	Verknüpfung von Metadaten (speziell EFGS) (EFGS-Risiko)	Nicht-autorisierte Reidentifikation eines Betroffenen 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 welchen Mitgliedsstaates reisen in welche anderen Mitgliedsstaaten (statistische Daten)	Ja	1	3	3	0	0	0	0	3	0	3	3		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 Version 1.5 immer allen Ländern, die über die Konfiguration als „Unterstützte Länder“ bereitgestellt werden. Eine Auswahl			akzeptabel
R2- Hacker	Offenbarung der Anzahl der relevanten Länder eines Daten zur Verfügung stehenden Betroffenen (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.	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 Version 1.5 immer allen Ländern, die über die Konfiguration als „Unterstützte Länder“ bereitgestellt werden. Eine Auswahl			akzeptabel
R2- Hacker	Reidentifikation 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	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 Version 1.5 immer allen Ländern, die über die Konfiguration als „Unterstützte Länder“ bereitgestellt werden. Eine Auswahl			akzeptabel
R2- Hacker	Nicht-autorisierte 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	Ja	1	2	2	2	0	0	0	2	0	2	2		Designentscheidungen D-6-2b: Liste von Ländern, mit denen die Tagesschlüssel über das EFGS verteilt werden, entspricht ab Version 1.5 immer allen Ländern, die über die Konfiguration als „Unterstützte Länder“ bereitgestellt werden. Eine Auswahl			akzeptabel
R2- Hacker	Nicht-autorisierte 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	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 Version 1.5 immer allen Ländern, die über die Konfiguration als „Unterstützte Länder“ bereitgestellt werden. Eine Auswahl			akzeptabel
R2- Hacker	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	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
R2- Hacker	Code-Injektionsfehler (Injektionsfehler im Verifikation-Server Backend)		Ja	1	0	3	3	3	0	0	0	0	4	4	ZB	Einschätzung Threat Modeling (siehe IT-Sicherheitskonzepte)			akzeptabel
R2- Hacker	Transaktionen Hijacking (Abfangen des laufenden Uploads von Diagnoseschlüsseln)		Ja	2	0	2	2	0	0	0	0	0	4	8	ZB	Designentscheidungen / Threat Modeling/ Einsatz von verschlüsselten Netzwerkverbindungen (siehe Z41) - TOM: Authentifizierung der Server			akzeptabel mit Evaluation
R4- Betreiber Server (T)	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) - siehe Z41			akzeptabel
R8-staatl Behörden	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	Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts-, Zugangs- und Zugriffskontrolle ... (TOM) auf dem Smartphone	Update 1.8: 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	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 mitgliedern auch das Risiko welches in Spalte E update 1.9 beschrieben // zu update Release 1.8 - DSK-Rahmenkonzept V1.8 "pers. Daten auf mob.Endgerät", 14.23: Die Sicherheitseinstellung (zusätzliche Verschlüsselung) führt bei			akzeptabel mit Evaluation
R4- Betreiber Server (T)	Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts-, Zugangs- 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 (siehe Z41)			akzeptabel
	Ungerechtfertigter Datentransfer in Drittländ																		
R4- Apple / Google	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	Beabsichtigter / unbeabsichtigter Datenexport von TEK/ TAN/ (i)TEK durch SAPI/ T (Schnittstellen)		Ja	1	4	4	4	0	0	0	1	4	4	4	TR, ZB, VT, IG, DM	AVV inkl. TOM mit DL (siehe Z41) , keine Datenübermittlung in Drittländ			akzeptabel
R1-CWA-Nutzer	Beabsichtigter / unbeabsichtigter Datenexport 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
	Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten																		
R1-CWA-Nutzer	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	Verlust von Daten, mit der Folge dass fehlende Information des Nutzers über Kontakt mit Infizierten innerhalb 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
R1-CWA-Nutzer	Verlust von Daten (durch Anwendung zurücksetzen) - nur die Daten der App (kein durch die App verursachtes Risiko)		Nein											-					
R4- Betreiber Server (T)	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	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 erneute Uploads oder ähnliche Maßnahmen erforderlich sind. Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme.			akzeptabel mit Evaluation
R2- Hacker	Verlust von Daten, mit der Folge dass fehlende Information des Nutzers über Kontakt mit Infizierten innerhalb Inkubationszeit (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	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.	Zwischenszeitlich liegt eine Stellungnahme des BSI vor, wonach keine zusätzlichen Sicherheitsrisiken durch Nutzung der Bluetooth - Technologie gesehen werden.	bedingt akzeptabel,	
R1-CWA-Nutzer	Gleichzeitige Verbindungen zu mehreren Bluetooth-Geräten		Ja	1	0	0	0	0	0	0	0	2	0	2	TR	Designentscheidungen (D-2-6)			akzeptabel
	Verweigerung der Betroffenenrechte (Betrachtung der Unterstützung durch SAPI/T)																		
R1-CWA-Nutzer	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-, Lösungsrechte zu gewähren (Transparenzrisiko, Verweigerung der Betroffenenrechte).	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

Datenschutzrisikoprüfung (DSFA) VT 1: App-seitige Verarbeitung Kontakt Ereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung inkl. Kontakt-Historie: 22.01.2021)			Risikobewertung																	
Risiko-Quelle	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Schadensausmaß										Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko	
					Datensensibilisierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zerschließung / Nichtverteilung	Risikoklasse						
R4 - Softwareentwickler / SAP	Nichtbeachtung von Auskunftsrechten (keine Verpflichtung zur Herstellung Personenbezug) - Art. 11		Ja	1	4	0	0	0	0	0	0	0	0	4	DM	esignentscheidung/ Pseudonymisierung, keine Herstellung Personenbezug zur Erfüllung Betroffenenrechte, Designentscheidungen D-8-1			akzeptabel	
R4 - Softwareentwickler / SAP	Nichtbeachtung von Löschungsersuchen, Berichtigungsersuchen - Art. 11		Ja	1	4	0	0	0	0	0	0	0	0	4	DM	Designentscheidung/ Pseudonymisierung, keine Herstellung Personenbezug zur Erfüllung Betroffenenrechte Designentscheidungen D-8-1			akzeptabel	
R4 - Softwareentwickler / SAP	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 Personenbezug zur Erfüllung Betroffenenrechte Designentscheidungen D-8-1			akzeptabel	
R4 - Softwareentwickler / SAP	Fehlende Übertragbarkeit		Ja	1	0	0	0	0	0	0	0	0	0	0	IV	Designentscheidung/ Pseudonymisierung, keine Herstellung Personenbezug zur Erfüllung Betroffenenrechte Designentscheidungen D-8-1				
R4 - Softwareentwickler / SAP	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)	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	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)	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	
	Verwendung der Daten zu inkompatiblen Zwecken																			
R8-staatl Behörden	Nachträgliche Zweckänderung/-erweiterung durch die verantwortliche Stelle ("Dambruch")		Nein	3	4	4	4	0	0	0	4	1	4	-	ZB, IV, VT, IG, DM	Designentscheidungen D-1-1				
R8-staatl Behörden	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	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	Nutzung des KTB-Einträge durch staatliche Stellen/ Private 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.	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-4-2c, D-5-11, D-9-8, D-7-10), DSK-Rahmenkonzept 14.27.17			bedingt akzeptabel	
R8- Behörden	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.	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	Anfänglicher oder späterer Missbrauch des Parameters "Transmission Risk Level".	Dieser Parameter kann von den Mitgliedsstaaten unterschiedlich verwandt 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 (Berufsgeheimsträger)	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.	Nein											-		Design-Entscheidungen EFGS D-1-5 (Keine Verwendung für die Überwachung von Quarantäne-Maßnahmen) + Designentscheidungen CWA nationalD-1-1				
R3-kommerzielle Datensammler	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.	Nein											-		Die Mitgliedsstaaten überwachen die Einhaltung der Freiwilligkeitsbedingungen abhängig vom nationalen Gesetzesrecht.				
R4- Apple / Google	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.	Nein											-		Design-Entscheidungen EFGS D-1-7 (Keine Bestimmung des Standorts des Betroffenen).				
R4- Betreiber Server (T)	Reidentifikation 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 Systemeintrichtungen ermöglicht.	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	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	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. Kein Einfluss auf Berechtigungsanforderungen durch Google/ Apple DSK_Rahmenkonzept, Kap. 14.20.5: "Auf Android- basierten mobilen Endgeräten ist das Aktivieren des ENF mit			akzeptabel mit Evaluation	
R2- Hacker	De-Anonymisierung/ De-Pseudonymisierung durch Verbindung von Gerät und GUID auf CWA - Server (Technisch unmöglich)		Nein											-						
R3-kommerzielle Datensammler	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	
R6 - Krimineller	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	0	1	0	4	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.			
R1-CWA-Nutzer	Re-Identifizierung durch Protokollierung (durch Integration KTB)	(ohne Kontakt-Historie)	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	Re-Identifizierung durch Begegnungshistorie in KTB	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	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)		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	Falsche Verdächtigung infolge Re-Identifizierung durch Kontakt-Historie KTB	Folge-Risiko zu Z 113: 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)		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)	De-Anonymisierung/ De-Pseudonymisierung von Nutzern anhand 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 Infrastrukturebene der OTC ist zeitlich stark begrenzt und durch die etablierten Sicherheitsprozesse zur Angriffserkennung in den DDoS Systemen definiert, die Verarbeitung wird nur dort systemintern			akzeptabel mit Evaluation	

Datenschutzroignisausnauzung (DSFA)			Risikobewertung																
VT 1: App-seitige Verarbeitung Kontakt ereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung inkl. Kontakt.Historia: 22.01.2024)			Schadensausmaß																
Risiko-Quelle	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datensammlung	Verarbeitheit	Integrität	Verfügbarkeit	Aufendziat	Resilienz	Intervierbarkeit	Transparenz	Zerschickung / Nichtverteilung	Risiko-klasse	Soil-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R8-staaff Behörden	De-Anonymisierung/ De-Pseudonymisierung von Nutzern 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)	Re-Identifizierung Nutzer durch Protokolldaten / Zugriff 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. Grundsätzlich ist dieses Modell nicht unumstößlich.)		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,
R2- Hacker	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	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 wird, insbesondere durch die Anzeige der Erinnerung an das Upload des positiven Testergebnisses, die auch auf dem Sperbildschirm 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 Privatsphäre 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.			akzeptabel mit Evaluation
R4- Apple / Google	Ermittlung von Kontakt ereignissen, 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	Aufbau von zentralen Bewegungs- und Kontaktprofilen (Verhaltenskontrolle, Compliance Scoring) anhand "Kontakt historien"	In Version 1 des ENF erhält die CWA App im Rahmen der Kontakt ermittlung und Risikoberechnung durch das Betriebssystem des mobilen Endergäts eine sogenannte ExposureInfo, 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 ExposureWindow bezeichnete Datenstruktur, die eine dynamische Darstellung des Verlaufs einer Risikobeggnung in Form mehrerer, sich über bis	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	Reidentifikation von Betroffenen auf Grund der Abfrage der relevanten Länder: Erzeugung einer Reisehistorie, Reidentifikation auf Grund der Einmaligkeit der Reisehistorie oder weiterer Daten, die staatlichen Einrichtungen zur Verfügung stehen (siehe Zeilen 56 bis 59). (EFGS - Risiko)	Siehe Zeilen 55 - 59	Ja	1	2	2	0	0	0	0	2	0	2	2	DM, VT, IT, ZB	Siehe Zeilen 55 - 59			akzeptabel
R2- Hacker	Herstellung eines "Ausländerscanners". (EFGS - Risiko)	Reidentifikation 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.	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	(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
R5-Arbeitgeber, Versicherungen	(Freiheits-)Beschränkungen bei Nicht-Nutzung der App (Zugänge 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
	Verarbeitung nicht vorhergesehener Daten																		
R4- Betreiber Server (T)	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			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	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			akzeptabel mit Evaluation
	Verarbeitung nicht richtiger Daten																		
R4 - Softwareentwickler / SAP	Ungeauigkeit bei der Zuordnung des Ansteckungsrisikos an CWA-Nutzer (Transmission Risk zu Tageschlüsseln)	Infolge der bisherigen Programmierung bei der Zuordnung von Transmission Risk zu Tageschlüsseln 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 Tageschlüsseln entsteht (z.B. durch Ausschalten des Smartphones) oder b.) mehrere Tageschlüssel für den selben Tag kreiert wurden (z.B. in neueren Versionen oder durch die Nutzung verschiedener Tracing-Apps). In der Folge könnte durch allein durch diese Art der	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 Version 1.5 nicht mehr auf.			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	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
	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,
	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	Upload von falsch-positiven Ergebnissen auf Grund unzureichender Zuverlässigkeit der Prüfmechanismen des Bestehens einer Infektion (Missbräuchlicher Upload nicht-infektöser 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.	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). Designentscheidung CWA National D-5.1-8a: Mithilfe des EFGS können alle Nutzer der Nationalen Corona-Apps bei einer Risikobeggnung mit einem positiv auf Corona getesteten			akzeptabel
R4- Betreiber Server (T)	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.	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			akzeptabel
R4- Betreiber Server (T)	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.	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
R1-CWA-Nutzer	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 Nutzerverantwortung			akzeptabel mit Evaluation
R1-CWA-Nutzer	Angabe falscher Begegnungen (im KTB)	wissenschaftl. 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	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 Schutz durch CWA-Nutzer (PIN)		akzeptabel, mit Evaluation
R4- Betreiber Server (T)	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	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	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	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

Datenschutzrisikoprüfung (DSRA) VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung inkl. Kontakt Historie: 22.01.2024)			Risikobewertung																	
					Schadensausmaß															
Risiko-Quelle	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (Ja/nein)	EW	Dateneintragung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zwischbindung / Notwendigkeit	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko	
R2- Hacker	Misbrauch der upload-Autorisierung		Ja	2	1	3	3	0	0	0	0	0	1	6	IG	Bewertung aus Threat Modeling/ AVV mit DL, inkl. TOM Designentscheidung D-11-1			akzeptabel mit Evaluation	
R2- Hacker	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 Modeling			akzeptabel mit Evaluation	
R2- Hacker	Manipulation von Positivschlüsseln		Ja	2	1	4	4	0	0	0	0	0	4	8	VT, IG, ZB	Designentscheidungen b-2-4/ Threat Modeling			akzeptabel mit Evaluation	
	Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler)																			
R4- Betreiber Server (T)	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	Technische Grenzen des ENF bei Tracing		Ja	2	0	0	0	3	0	3	3	0	3	6	VF, R, IV, TR	DSK_Rahmendumment Kap. 14.20.4 iVm Designentscheidung zur Nutzung BLE-Technik und Vermeidung eines Rückgriffs auf Geolokalisationsdaten.			akzeptabel mit Evaluation	
R4- Apple / Google	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 Betriebsysteme ausgenommen . Durch das Einspielen eines Backups (Restore) auf ein mobiles Endgerät kann es daher nicht zu Verlusten oder Inkonsistenzen von eigenen			akzeptabel mit Evaluation	
R4 - Softwareentwickler / SAP	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)	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.	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	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.	Ja	1	0	0	0	4	0	4	2	0	2	4	VF, RE				akzeptabel	
R1-CWA-Nutzer	Überlastung des mobilen Endgeräts des Nutzers auf Grund 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.	Ja	3	0	0	0	4	0	4	2	0	2	12	VF, RE			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	bedingt akzeptabel	
R4- Betreiber Server (T)	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.	Ja	3	0	0	0	3	0	3	2	0	2	9	VF, RE	Zusätzlich müssen Schnittstellen Status- und Fehlermeldungen vorsehen, um festzustellen, ob erneute Uploads oder ähnliche Maßnahmen erforderlich sind. Zertifikate auf Ebene (1) Infrastruktur (DiGIT), (2) Betrieb EFGS (T-Systems), (3) Infrastruktur der nationalen App.			akzeptabel mit Evaluation	
R4- Betreiber Server (T)	Vorübergehende oder permanente Nicht-Verfügbarkeit der Upload-Funktion des EFGS, z.B. auf Grund von Fehlfunktionen, Problemen mit Zertifikaten und Autorisierungsfunktionen (siehe Zeile 137) (EFGS Risiko)	Siehe Zeile 137	Ja	3	0	0	0	3	0	3	2	0	2	9	VF, RE	Zusätzlich müssen Schnittstellen Status- und Fehlermeldungen vorsehen, um festzustellen, ob erneute Uploads oder ähnliche Maßnahmen erforderlich sind. Anzuwendende DiGIT Sicherheitsanweisungen für IT-Systeme: ST_business_continuity_management.doc.			akzeptabel mit Evaluation	
R4 - Softwareentwickler / SAP	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	Kollisionen von BLE Nachrichten bei Agglomerationen (begrenzt auf 20 Kanäle) bei großen Mengen könnte es zu Kollisionen und Neubeträgungen 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)	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	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	
R4- Apple / Google	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	Designentscheidungen (siehe Z 91)			akzeptabel mit Evaluation	
R4- Apple / Google	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	Unsachgemäße Verwendung eines Mobilfunkgerätes für Zwecke der CWA / Verlust des Gerätes (siehe Z 68)		Ja	2	4	4	4	0	0	0	4	4	4	8	ZB, T, IV	siehe Z 68			akzeptabel mit Evaluation	
R1-CWA-Nutzer	Unsachgemäße/ unberechtigte Vernichtung und Löschung von Daten (Mobilgerät)		Ja	2	0	0	4	4	0	4	4	4	4	8	ZB, T, IV	siehe Z 63 (Restrisiko beim Nutzer)			akzeptabel mit Evaluation	
R1-CWA-Nutzer	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	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...	siehe Z 68			akzeptabel	
R1-CWA-Nutzer	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	siehe Z 119			akzeptabel mit Evaluation	
R4 - Softwareentwickler / SAP	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	Großflächiges Bluetooth Hacking / Bluetooth Jam (Angreifer können mit einem sehr starken Signal das gesamte funk Spektrum beeinträchtigen, dass in ca. 20m Umfang kein Austausch von Beacons mehr möglich		Ja	3	1	3	3	1	1	1	1	1	1	9	IT, VT	siehe Dokument 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	Spoofing App (Identität verschleiern - 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.		Ja	4	4	4	4	4	4	4	4	4	4	16	VT, DM, ZB, TR, IV, VG, A, R	Designentscheidungen B-1-1f.		Es gibt keine technischen Möglichkeiten, um dies auszuschließen. Risiko liegt in der Grundsatzentscheidung begründet, ENF und BLE zu nutzen.	bedingt akzeptabel,	
R2- Hacker	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	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 Zertifikatpinning wird ein Einsatz von DNSSEC auf Serverseite derzeit nicht für notwendig erachtet.			bedingt akzeptabel mit Evaluation	

Datenschutzfolgenabschätzung (DSFA)			Risikobewertung																			
VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung inkl. Kontakt.Historie: 22.01.2024)																						
Risiko-Quelle	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Schadensausmaß										Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko			
					Datensammlung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Interventionsbarkeit	Transparenz	Zuschließung / Nichtverletzung	Risikoklasse								
R2- Hacker	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.	Ja	1	0	3	3	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	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	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	Denial of Service Angriffe durch Missbrauch der CWA-App		Ja	3	0	0	0	3	2	3	0	0	0	9	VF, TR	Designentscheidungen D-5.1-16			akzeptabel mit Evaluation			
R2- Hacker	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	Ave mit DL, inkl. TOM , Designentscheidungen D-11-1			bedingt akzeptabel mit Evaluation			
R4 - Google/ Apple, CWA-Entwickler, Server-/ Internet-Betreiber	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			
	Verarbeitung über die Speicherfrist hinaus		Ja										0									
R4- Apple / Google	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)	Unbefristete Speicherung von Daten (inkl. Metadaten) in DB und mögliche spätere Verkettung mit anderen personenbezogenen Daten (siehe Zeile 91)		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 Positivschlüsseln auf der Datenbank des CWA Servers sowie auf dem Objectstore, der als Übergabemedium zum CDN-Magenta dient, erfolgt mit den vom jeweiligen Speicherservice		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)	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 Diagnoseschlüssel offenbaren.	Ja	3	1	1	1	0	0	0	1	1	1	3		Löschen der Daten erfolgt im nationalen Backend.			akzeptabel			
R1-CWA-Nutzer	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			
R4- Betreiber Server (T)	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			
	Risiken durch Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt																					
	DV ohne fehlende/ hinreichende epidemiologisch signifikante Wirksamkeit			3	4	4	4	4	4	4	4	4	4									
	Freiheitsgewinne bei Nutzung der App (Immunitätsausweis, Zugangsvereinfachung zu staatlichen/ kommunalen Leistungen)																					
	Freiheitsbeschränkungen bei Nicht-Nutzung der App (Zugangs Beschränkungen zu staatlichen/ privaten Leistungen)																					
	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 legt Potential das Personen ggf. ihr Verhalten ständig kontrollieren und anpassen.	Ja	1	1	1	1	0	0	0	1	1	1	1					akzeptabel			
	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?)	CWA-Version 1.10: Die Einführung eines KTB könnte die Akzeptanz der App senken, weil damit erstmals pD eingetragen können. CWA-Version 1.12: Die zusätzliche Einführung der Kontaktstrie 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						