Datenschutzfolgenabschätzung (DSFA)

VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung: 08.10.2020) u Implementierung EFGS (11.10.2020)

								Risikobewertung														
										Schadensausmaß												
Prüfgegenstand/ Risikoursprung	**Risiko-Quelle**	**Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Betroffenengruppen (CWA-Nutzer, Nutzer anderer nat. Corona-Apps, Personen im Umfeld, Personen, die von Falschmeldungen Betroffen sein könnten). Soweit keine Auswahl**	**Risikoverantwortlicher**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
Allgemein		1	**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	RM		akzeptabel
	R1-CWA-Nutzer		Datenverarbeitungen ohne/ nach widerrufener Einwilligung (Deinstallation der CWA App)				Ja	1	4	4	4	4	4	0	4	0	4	RM		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	siehe Anlage 7, Ziff. 2.3.2 (3)	bedingt akzeptabel
	R1-CWA-Nutzer		Unwirksame Einwilligung durch fehlende Freiwilligkeit ("erzwungene Einwilligung")				Ja	1	4	4	4	4	4	4	4	4	4	RM		akzeptabel
	R1-CWA-Nutzer		Unwirksame Einwilligung aufgrund fehlender / fehlerhafter ausdrückliche Einwilligungserklärung (technischer Einwilligungs-Akt)				Ja	1	4	4	4	4	4	4	4	4	4	RM		akzeptabel
	R1-CWA-Nutzer		Unwirksame Einwilligung aufgrund fehlender Information über Umfang und Folgen				Ja	2	4	4	4	4	4	4	4	4	8	DM, VT, IG, IV, TR, ZB		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	8	DM, VT, IG, IV, TR, ZB		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	16	DM, VT, IG, IV, TR, ZB	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		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		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		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		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		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		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		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	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		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		akzeptabel
		2	**Verarbeitung wider Treu und Glauben**																		
	R1-CWA-Nutzer		Alarmmüdigkeit (mehrmalige Alarmierung inkl. Quarantäne-Empfehlung innerhalb kurzer Zeit) - Nachjustizierung				Ja	2	1	1	1	0	0	0	3	1	4	8	ZB		akzeptabel mit Evaluation
	R4- Apple / Google		Ungenauigkeit der Kontaktbestimmung				Ja	3	0	0	0	0	0	0	0	0	4	12	ZB	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		akzeptabel
	R2- Hacker		Vortäuschen von Kontaktereignissen durch Duplizierung von BLE-Beacons				Ja	3	o	0	0	3	0	3	0	0	0	9	VF, R		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		akzeptabel mit Evaluation
	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		akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA)

VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung: 08.10.2020) u Implementierung EFGS (11.10.2020)

								Risikobewertung													
										Schadensausmaß											
Prüfgegenstand/ Risikoursprung	**Risiko-Quelle**	**Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Betroffenengruppen (CWA-Nutzer, Nutzer anderer nat. Corona-Apps, Personen im Umfeld, Personen, die von Falschmeldungen Betroffen sein könnten). Soweit keine Auswahl**	**Risikoverantwortlicher**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
	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		akzeptabel
		3	**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		akzeptabel
	R8- Behörden		Unvollständige, unverständliche Datenschutzinformationen für API / CNF				Ja	2	2	2	2	0	0	0	3	4	4	8	TR, ZB		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		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		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		akzeptabel mit Evaluation
		4	**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		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		akzeptabel
	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		akzeptabel mit Evaluation
	R4- Apple / Google		Unbefugter Zugriff von Plattformen, die Kontaktereignisse ermitteln, auch für NutzerInnen ohne CWA				Ja	3	4	4	4	0	0	0	2	4	4	12	DM, VT, IG, TR, ZB	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	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		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		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		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 Implemetierung Dummyschlüssel) (ohne Berücksichtigung Angaben zum Symptombeginn)				Ja	2	1	3	3	2	0	0	0	0	3	6	ZB , VT, IG		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		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				Ja	1	1	3	3	2	0	0	0	0	4	4	ZB, VT, IG		akzeptabel
	R2- Hacker		Abhören des Bluetooth - Verkehrs				Ja	2	1	2	2	0	0	0	2	2	2	4	VT, ZB , TR		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		akzeptabel mit Evaluation
	R2- Hacker		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		akzeptabel
	R2- Hacker		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		akzeptabel mit Evaluation
	R2- Hacker		Unbefugte Offenlegung durch Metadaten-Korrelation				Ja	2	0	4	4	0	0	0	0	0	4	8	ZB		akzeptabel mit Evaluation
	R2- Hacker		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 welchen Mitgliedsstaates reisen in welche anderen Mitgliedsstaaten (statistische Daten)			Ja	1	3	3	0	0	0	0	3	0	3	3			akzeptabel

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung: 08.10.2020) u Implementierung EFGS (11.10.2020)							Risikobewertung													
									Schadensausmaß											
Prüfgegenstand/ Risikoursprung	**Risiko-Quelle**	**Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Betroffenengruppen (CWA-Nutzer, Nutzer anderer nat. Corona-Apps, Personen im Umfeld, Personen, die von Falschmeldungen Betroffen sein könnten). Soweit keine Auswahl**	**Risikoverantwortliche**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
	R2- Hacker		Offenbarung der Anzahl der relevanten Länder eines Daten zur Verfügung stellenden Betroffenen (Kodierlänge einer hochgeladenen Zeichenkette). (EFGS-Risiko)	Eine Kodierung des Felds "relevante Länder" als variable Zeichenkette klann 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			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 erfordern, kann bei einer			Ja	1	1	4	4	0	0	0	4	4	4	4			akzeptabel
	R2- Hacker		Nicht-autorisierter Zugriff auf personenenbezogene 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			akzeptabel
	R2- Hacker		Nicht-autorisierter Zugriff auf personenenbezogene 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 heruntezuladenden 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, dass			Ja	1	2	2	2	0	0	0	2	2	2	2			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		akzeptabel
	R2- Hacker		Code-Injektionsfehler (Injektionsfehler im Verifikation-Server Backend)				Ja	1	0	3	3	3	0	0	0	0	4	4	ZB		akzeptabel

Datenschutzfolgenabschätzung (DSFA)

VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung: 08.10.2020) u Implementierung EFGS (11.10.2020)

							Risikobewertung														
									Schadensausmaß												
Prüfgegenstand/ Risikoursprung	**Risiko-Quelle**	**Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Betroffenengruppen (CWA-Nutzer, Nutzer anderer nat. Corona-Apps, Personen im Umfeld, Personen, die von Falschmeldungen Betroffen sein könnten). Soweit keine Auswahl**	**Risikoverantwortlicher**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
Unberechtigter DL- oder Administratorenzugriff/ Zugriff auf / Veränderung von	R2- Hacker		Transaktionen Hijacking (Abfangen des laufenden Uploads von Diagnoseschlüsseln)				Ja	2	0	2	2	0	0	0	0	0	4	8	ZB		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		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		akzeptabel mit Evaluation
	R2- Hacker		Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts-, Zugangs- und Zugriffskontrolle …(TOM) auf dem Smartphone /				Ja	2	4	4	4	4	4	4	4	4	4	8	VT , IG, VF, A, R, IV, TR, ZB, DM		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		akzeptabel
		5	**Ungerechtfertigter Datentransfer in Drittland**																		
	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	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 SAP/ T (Schnittstellen)				Ja	1	4	4	4	0	0	0	1	4	4	4	TR, ZB, VT, IG, DM		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		akzeptabel
		6	**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		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		akzeptabel mit Evaluation
	R1-CWA-Nutzer		Verlust von Daten (durch Anwendung zurücksetzen) - nur die Daten der App (kein durch die App versursachtes 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		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		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	Zwischenzeitlich 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		akzeptabel
		7	**Verweigerung der Betroffenenrechte (Betrachtung der Unterstützung durch SAP/T)**																		
	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		akzeptabel
	R4 - Softwareentwickler / SAP		Nichtbeachtung von Löschungsersuchen, Berichtigungsersuchen - Art. 11				Ja	1	4	0	0	0	0	0	0	0	0	4	DM		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		akzeptabel
	R4 - Softwareentwickler / SAP		Fehlende Übertragbarkeit				Ja	1	0	0	0	0	0	0	0	0	0	0	IV		
	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		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		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		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		akzeptabel mit Evaluation
		8	**Verwendung der Daten zu inkompatiblen Zwecken**																		

Datenschutzfolgenabschätzung (DSFA)

VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung: 08.10.2020) u Implementierung EFGS (11.10.2020)

								Risikobewertung													
										Schadensausmaß											
Prüfgegenstand/ Risikoursprung	**Risiko-Quelle**	**Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Betroffenengruppen (CWA-Nutzer, Nutzer anderer nat. Corona-Apps, Personen im Umfeld, Personen, die von Falschmeldungen Betroffen sein könnten). Soweit keine Auswahl**	**Risikoverantwortlicher**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
	R8-staatl Behörden		Nachträgliche Zweckänderung/-erweiterung durch die verantwortliche Stelle ("Dammbruch")				Nein	3	4	4	4	0	0	0	4	1	4	-	ZB; IV, VT, IG, DM		
	R8-staatl Behörden		Nutzung der Daten zur Erstellung eines Immunitätsausweises				Nein	3	4	0	0	0	0	0	0	0	4	-	DM, TR		
	R8-staatl Behörden		Missbrauch der Systeme/ Daten zur Überwachung von Maßnahmen der soz. Distanzierung, Quarantänemaßnahmen (durch Anweisung an die Telekom)				Nein	3	4	4	4	0	0	0	4	4	4	-	ZB , IV, TR, DM, VT, IG		
	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										-			
	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		akzeptabel mit Evaluation
	R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)		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										-			
	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										-			
	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										-			
	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 Systemeinrichtungen ermöglicht.			Ja	1	3	3	0	0	0	0	0	0	3	3	DM, VT, TR		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	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)**				Ja	3	3	3	3	0	0	0	3	3	3	9	ZB , TR, IV, IG, VT, DM		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		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		akzeptabel mit Evaluation
	R8-staatl 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		akzeptabel mit Evaluation
	R4- Betreiber Server (T)		Re-identifizierung Nutzer durch Protokolldaten (siehe Z 86) / Zugriff Strafverfolgungsbehörden				Ja	3	4	4	4	0	0	0	4	4	4	12	ZB , TR, IV, IG, VT, DM	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		akzeptabel mit Evaluation
	R2- Hacker		De-Anonymisierung/ De-Pseudonymisierung/ Enttarnung von Nutzern durch Benachrichtigungen oder Metadaten				Ja	2	1	2	0	4	1	0	4	4	4	8	ZB, TR, IV		akzeptabel mit Evaluation
	R4- Apple / Google		Ermittlung 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		Aufbau von zentralen Bewegungs- und Kontaktprofilen (Verhaltenskontrolle, Compliance Scoring) anhand "Kontakthistorien"				Ja	1	4	4	0	0	0	0	4	4	4	4	DM, VT, ZB, TR, IV		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		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		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		akzeptabel mit Evaluation
	R5-Arbeitgeber, Versicherungen		(Freiheits-)Beschränkungen bei Nicht-Nutzung der App (Zugangs Beschränkungen zu staatlichen/ privaten Leistungen)		[Kinder / Jugendliche, Schüler, Auszubildende], [Epidemiologische Risikogruppen (60+,		Ja	2	0	4	0	0	0	0	4	0	4	8	DM, ZB, IV		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		akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA)

VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung: 08.10.2020) u Implementierung EFGS (11.10.2020)

								Risikobewertung														
										Schadensausmaß												
Prüfgegenstand/ Risikoursprung	**Risiko-Quelle**	**Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Betroffenengruppen (CWA-Nutzer, Nutzer anderer nat. Corona-Apps, Personen im Umfeld, Personen, die von Falschmeldungen Betroffen sein könnten). Soweit keine Auswahl**	**Risikoverantwortlicher**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
	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		akzeptabel mit Evaluation
			Verarbeitung nicht richtiger Daten																		
	R4 - Softwareentwickler / SAP		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 durch allein durch diese Art der Programmierung a) das			Ja	2	0	3	1	0	0	0	2	2	3	6	IG, ZB		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		akzeptabel mit Evaluation
			"falscher Negativer"				Ja	3	0	4	0	0	0	0	4	4	4	12	ZB, TR, IV	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	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-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.			Ja	1	4	2	4	0	0	0	4	4	4	4	DM, VT, IG, IV, TR, ZB		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		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		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		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		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		akzeptabel
	R2- Hacker		Manipulation von Daten auf Transportwegen (https)				Ja	2	0	3	3	0	0	0	0	0	0	6	IG, VT		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		akzeptabel mit Evaluation
	R2- Hacker		Missbrauch der upload-Autorisierung				Ja	2	1	3	3	0	0	0	0	0	1	6	IG		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		akzeptabel mit Evaluation
	R2- Hacker		Manipulation von Positivschlüsseln				Ja	2	1	4	4	0	0	0	0	0	4	8	VT, IG, ZB		akzeptabel mit Evaluation
		11	**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		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		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		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		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		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 Zeritifikaten und Autorisierungsfunktionen. (EFGS-Risiko)	Keine weitere Beschreibung erforderlich.			Ja	3	0	0	0	3	0	3	2	0	2	9	VF, RE		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 Zeritifikaten und Autorisierungsfunktionen (siehe Zeile 137) (EFGS Risiko)	Siehe Zeile 137			Ja	3	0	0	0	3	0	3	2	0	2	9	VF, RE		akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA)

VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung: 08.10.2020) u Implementierung EFGS (11.10.2020)

								Risikobewertung														
										Schadensausmaß												
Prüfgegenstand/ Risikoursprung	Risiko-Quelle	Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Betroffenengruppen (CWA-Nutzer, Nutzer anderer nat. Corona-Apps, Personen im Umfeld, Personen, die von Falschmeldungen Betroffen sein könnten). Soweit keine Auswahl	Risikoverantwortlicher	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	Bewertung, warum "rote" Risiken akzeptiert werden können	Restrisiko
	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	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 Neuübertragungen kommen				Ja	3	0	0	4	0	4	0	0	0	4	12	A, ZB	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		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		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		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		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		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		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		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…		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		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		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		akzeptabel mit Evaluation
	R2- Hacker	B-1-51-5	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	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)				Ja	2	0	0	0	4	4	4	4	4	4	8	VT, DM, ZB, T , IV		bedingt akzeptabel mit Evaluation
	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	0	2	0	2	3	VT, IG		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 Verarbeitungsverügbarkeit des			Ja	3	0	3	0	3	0	3	2	0	2	9	VT, VF, R		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		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		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		akzeptabel
		12	**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	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	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. releante 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.			Ja	3	1	1	1	0	0	0	1	1	1	3			akzeptabel
	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		akzeptabel
			Risiken durch Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt																		
			DV ohne fehlende/ hinreichende epidemiologisch signifikante Wirksamkeit				Ja	3	4	4	4	4	4	4	4	4	4	12			

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall (Stand nach Aktualisierung: 08.10.2020) u Implementierung EFGS (11.10.2020)							Risikobewertung															
									Schadensausmaß													
Prüfgegenstand/ Risikoursprung	**Risiko-Quelle**	**Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Betroffenengruppen (CWA-Nutzer, Nutzer anderer nat. Corona-Apps, Personen im Umfeld, Personen, die von Falschmeldungen Betroffen sein könnten). Soweit keine Auswahl**	**Risikoverantwortlicher**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
			Freiheitsgewinne bei Nutzung der App (Immunitätsausweis, Zugangserleichterung zu staatlichen/ kommunalen Leistungen)																		
			Freiheitsbeschränkungen bei Nicht-Nutzung der App (Zugangs Beschränkungen zu staatlichen/ privaten Leistungen)																		
			Gewöhnung an Überwachung durch Staat und Markt																		
Allgemein			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?)				Nein	4	0	0	0	0	0	0	0	0	4	-	DM, ZB, U		