Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall		Risikobewertung															
				Schadensausmaß													
Risiko-Quelle	**Bedrohung/ Risiko**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
	Unbefugte oder unrechtmäßige Verarbeitung durch CWA																	
R1-CWA-Nutzer	Datenverarbeitungen ohne/ nach widerrufener Einwilligung (Deinstallation der 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)			akzeptabel
R1-CWA-Nutzer	Unwirksame Einwilligung durch fehlende Freiwilligkeit ("erzwungene Einwilligung")	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	Unwirksame Einwilligung aufgrund fehlender / fehlerhalfter 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 Infomationen (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 dur unter 16 Jahre alt bis, dann besprich bitte die Nutzung der App mit deinen Eltern."	Gemeinsame Entwicklung der Lösung im Workstream	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)			akezptabel, mit Evaluation
R4- Betreiber Server (T)	Abhängigkeiten von Dienstleistern/ Software Herstellern (Ausfall externer Dienstleister) - SAP / T	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- 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 mgl.), siehe Dokument "Designentscheidungen D-5.1-1			akezptfeel, mit Evaluation
R4- Betreiber Server (T)	Fehlende unzureichende vertragliche Regelungen mit Dienstleistern (Auftragsverarbeitung/ Vertrag zur gemeinsamen Verantwortung) - mit T/SAP	Ja	1	3	3	3	3	0	2	2	3	3	3	ZB, TR	AVV (inkl. TOM) T/ SAP, siehe Designetscheidungen 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, Verification-, 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.	bedingt akezptabel,
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 Designetscheidungen 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 Designetscheidungen D-11-1			akzeptabel
	Verarbeitung wider Treu und Glauben																	
	Alarmmüdigkeit (mehrmalige Alarmierung inkl. Quarantäne-Emplehlung innerhalb kurzer Zeit) - Nachjustizierung	Ja	2	1	1	1	0	0	0	3	1	4	8	ZB	siehe Designentscheidungen (D-1.2-1)			akzeptabel mit Evaluation
	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-2-5)		Die Grundsatzentscheidung für das Framework von Apple / Google nebst BLE-Technik führt zu bekannten Ungenauigkeiten. Die Betrtreiber arbeiten an Optimierungen, wie auch in den Designentscheidungen beschrieben (D-2-7).	bedingt akzeptabel,
R1-CWA-Nutzer	Vortäuschen poitiver Testergebnisse (im "Standard-Verfahren", ohne teleTAN)	Ja	1	0	0	0	0	4	0	4	4	4	4	TR, IV, ZB	automatisiertes Verfahren zur Abfrage Tan beim VerificationServer erschwert Einflussnahme/ Designentscheidungen B-1-3			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	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
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

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall		Risikobewertung															
				Schadensausmaß													
Risiko-Quelle	**Bedrohung/ Risiko**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**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	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentschedungen D-11-1)			akzeptabel
	Mangelnde Funktionalität durch fehlende länderübergreifende Interopalität der App	Ja	3	0	0	0	0	0	0	0	0	3	9	ZB; DM	siehe Designentscheidungen D-2-5			akzeptabel mit Evaluation
	Für die Betroffenen intransparente Verarbeitung												0					
	Unvollständige, unverständliche Datenschutzinformationen für CWA und Backend (inkl. Funktionalitäten der CWA)	Ja	1	2	2	2	0	0	0	3	4	4	4	TR, ZB	Datenschutzinformation (siehe Z8)			akzeptabel
	Unvollständige, unverständliche Datenschutzinformationen für API / CNF	Ja	2	2	2	2	0	0	0	3	4	4	8	TR, ZB	Datenschutzinformation (siehe Z8)			akezptabel 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 Z8)			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 (+siehe Z12)			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 Handynutzung / Restrisiko beim Nutzer - Designentscheidung D-2-2			akzeptabel
R1-CWA-Nutzer	Bewusste/ Unbewusste Erteilung von nicht-notwendigen Berechigungen an CWA-Betreiber	Ja	1	4	4	4	0	0	0	2	4	4	4	DM, VT, IG, TR, ZB	Sicherheitseinstellungen Handynutzung/ Restrisiko beim Nutzer - Designentscheidung D-2-2			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	Empfehlungen Handynutzung/ Designetscheidungen (Containerisierung CWA - Designentscheidung D-2-2			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	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, ZBf	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 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: Geerschlüsselte Speicherung im Smartphone) Designentscheidung D-5.1-6)			akzeptabel
R4- Betreiber Server (T)	Zugang/ Zugriff auf Gesundheitsdaten/ Infektionsstatus durch Überwachung des WiFi-/ Internetverkehrs (Kommunikation zwischen CWA und CWA-Server) - Eavesdropping	Ja	3	1	2	2	2	0	0	0	0	3	9	ZB	Designentscheidungen/ TOM (Verschlüsselung Transportweg innerhalb der IT-Infrastruktur und zu CWA) - D-4.1-11			akzeptabel mit Evaluation
R2- Hacker	Zugang/ Zugriff auf Gesundheitsdaten/ Infektionsstatus durch Überwachung des Internetverkehrs (Kommunikation zwischen CWA und CWA-Server) nach Maßnahmen (Dummy Requests nicht in Rel.1)	Ja	3	1	2	2	2	0	0	0	0	3	9	ZB	siehe Designentscheidungen D-5.1-15			akzeptabel mit Evaluation
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)			akezptabel
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) - Designentscheiidungen B-4-1			akzeptabel mit Evaluation
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/ Korellation verhindern durch Trennung von Meta- und Nutzdaten/ Keine TAN - Speicherung auf Verification Server			akzeptabel mit Evaluation
R2- Hacker	PostgreSQL Injektion (Benutzergenerierte Nachrichten können bösartige SQL-Befehle enthalten)	Ja	1	0	3	3	3	0	0	0	0	4	4	ZB	Einschätzung Threat Modellng (Prüfung, ob Eingabe Validierung für Anwenderdaten) - Designentscheidung B-1-5			akezptabel
R2- Hacker	Code-Injektionsfehler (Injektionsfehler im Verfification-Server Backend)	Ja	1	0	3	3	3	0	0	0	0	4	4	ZB	Einschätzung Threat Modelling (siehe IT-Sicherheitskonzepte)			akzeptabel

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall		Risikobewertung															
				Schadensausmaß													
Risiko-Quelle	**Bedrohung/ Risiko**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
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 Modelling/ Einsatz von verschlüsselten Netzwerkverbindungen (siehe Z41) - TOM: Authentifizierung der Server			akzeptabel mit Evaluation
R4- Betreiber Server (T)	Unberechtigter Administratorenzugriff auf (i) TEK 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 /	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			akezptabel 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 Drittland																	
R4- Apple / Google	Beabsichtiger / unbeabsichtiger Datenexport von TEK 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	Beabsichter / unbeabsichtiger Datenexport von TEK/ TAN/ (i)TEK durch SAP/ T (Schnittstellen)	Ja	1	4	4	4	0	0	0	1	4	4	4	TR, ZB, VT, IG, DM	AVV inkl. TOM mit DL (siehe Z41) , keine Datenübermittlung in Drittland			akzeptabel
R1-CWA-Nutzer	Beabsichtiger / unbeabsichtiger Datenexport (i) TEK/ Infektionsstatus an Unberechtigte (Auslandsaufenthal 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 versursachtes Risiko)	Nein											-					
R2- Hacker	Verlust von Daten, mit der Folge dass fehlende Information des Nutzers über Kontakt mit Infizierten innerhalb Inkubationszeit (durch Dritte bei Verluust Smartphone)	Ja	2	4	4	4	0	0	0	4	4	4	8	TR, IV,VF, IG, DM, ZB	Nutzerverantwortung (Designentscheidungen D-2-2)			akezptabel 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-Techniik, Nutzung der "Radiofunktion"		Zwischenzeitlich liegt eine Stellungnahme des BSI vor, wonach keine zusätzlichen Sicherheitsriiken 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 Unterstüzung durch SAP/T)																	
R4 - Softwareentwickler / SAP	Nichtbeachtung von Auskunftsrechten (keine Verplfichtung zur Herstellung Personenbezug) - Art. 11	Ja	1	4	0	0	0	0	0	0	0	0	4	DM	esignentscheidung/ Pseudonymisierung, keine Herrstellung Personenbezug zur Erfüllung Betroffenenrechte, Designentscheidungen D-8-1			akezptabel
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 Herrstellung 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 Herrstellung Personenbezug zur Erfüllung Betroffenenrechte Designentscheidungen D-8-1			akzetpabel
R4 - Softwareentwickler / SAP	Fehlende Übertragbarkeit	Ja	1	0	0	0	0	0	0	0	0	0	0	IV	Designentscheidung/ Pseudonymisierung, keine Herrstellung 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			akzetpabel
R4- Betreiber Server (T)	Fehlende/ unzureichende Löschung der Daten im Backend (CWA-Backend, Testresult, Verification)	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) unrd AVV inkl. TOM			akzeptabel

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall		Risikobewertung															
				Schadensausmaß													
Risiko-Quelle	**Bedrohung/ Risiko**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
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			akzeptabel mit Evaluation
R4- Betreiber Server (T)	Fehlende/ unzureichende Löschung auf Servern iund 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 ("Dammbruch")	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	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	AVV inkkl. TOM mit DL, Designentscheidungen D-11-1			
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.	bedintgt 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	Die Offenlegung Quellcodes zeigte, dass die CWA-App ohne Zugang auf Standortdaten. Kein Einfluss auf Berechtigungsanforderungen durch Google/ Apple.			akzeptabel mit Evaluation
	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-Backend			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			akzeptabel mit Evaltuation
R8-staatl Behörden	De-Anonymisierung/ De-Pseudonymisierung von Nutzern anhand von Standortdaten (siehe Z 78)	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 (siehe Z 77) / Zugriff Strafvervolgungsbehörden	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		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 Strafvervolgungsbehörden 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 Ntzer durch Peilung (BLE/ WiFi) als sendende Person**	Ja	2	1	2	2	0	0	0	2	2	3	6	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	Ja	2	1	2	0	4	1	0	4	4	4	8	ZB, TR, IV	Designentscheidungen (Verschlüsselung) D-5.1-11			akzettabel 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	Designentscheidungen D-7-2			akzeptabel
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 (zugangsbeschränkungen zu staatlichen/ privaten Leistungen)	Ja	2	0	4	0	0	0	0	4	0	4	8	DM, ZB, IV	siehe Dokument Designentscheidugen 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-Identifikfaktion	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																	

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall		Risikobewertung															
				Schadensausmaß													
Risiko-Quelle	**Bedrohung/ Risiko**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
	Fälschung Parameter / Falsche Berechnungen in der App durch statische Programmierung für das Risiko der Ansteckung	Ja	2	0	0	0	0	0	0	4	4	4	8	ZB, TR, IV	Designentscheidungen D-8-1 (Paramenteranpassungen 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 Sicherheitsriiken 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-7-3)		Zwischenzeitlich liegt eine Stellungnahme des BSI vor, wonach keine zusätzlichen Sicherheitsriiken durch Nutzung der Bluetooth - Technologie gesehen werden.	bedingt 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 Niutzerverantwortung			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
R2- Hacker	Missbrauch der upload-Autorisierung	Ja	2	1	3	3	0	0	0	0	0	1	6	IG	Bewertung aus Threat Modelling(AVV mit DL, inkl. TOM Designentscheidung D-11-1			akzeptabel mit Evaluation
R2- Hacker	Manipulation der Parameter zum Abrufen und Hochladen von Tests	Ja	2	1	4	4	0	0	0	0	0	1	8	VT, IG	Designentscheidungen B-2-4/ Bewertung aus Threat Modelling			akzeptabel mit Evaluation
R2- Hacker	Manipulation von Positivschlüsseln	Ja	2	1	4	4	0	0	0	0	0	4	8	VT, IG, ZB	Designentscheidungen b-2-4/ Threat Modelling			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 von Apple/ Google (inkl. Backup/ Restore)	Ja	2	0	0	0	3	0	3	3	0	3	6	VF, R , IV, TR	Designentscheiidungen, Restriskio beschrieben im DSK CWA			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 - 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-Techniik / Empfehlung an Nutzer die empfohlenen Sicherheitspatches einzuspielen.		Zwischenzeitlich liegt eine Stellungnahme des BSI vor, wonach keine zusätzlichen Sicherheitsriiken durch Nutzung der Bluetooth - Technologie gesehen werden.	bedingt akezptabel,
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	Designentscheidungen zur Nutzung der BLE-Technik/laufende Beratung durch Forschungseinrichtung (CISPA)		Zwischenzeitlich liegt eine Stellungnahme des BSI vor, wonach keine zusätzlichen Sicherheitsriiken 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-/ Zeifaktoren gemessen wird (siehe Z 96)	Ja	2	0	0	0	0	0	0	4	4	4	8	IV, TR, ZB	Designentscheidungen (siehe Z 96)			akzeptabel mit Evaluation
R4- Apple / Google	Fehlfunktionen bei Backup & Restore führt zu Verlusten oder Inkonsistenzen von TEK oder RPI (siehe Z 109)	Ja	2	0	0	0	3	0	3	3	0	3	6	VF, R	siehe Z 109			akzeptabel mit Evaluation
R1-CWA-Nutzer	Unsachgemäße Verwendung eines Mobilfunkgerätes für Zwecke der CWA / Verlust des Gerätes (siehe Z 60)	Ja	2	4	4	4	0	0	0	4	4	4	8	ZB, T, IV	siehe Z 60			akzeptabel mit Evaluation
R1-CWA-Nutzer	Unsachgemäße/ unberechtigte Vernichtung und Löschung von Daten (Mobilgerät) (siehe Z 63)	Ja	2	0	0	4	4	0	4	4	4	4	8	ZB, T, IV	siehe Z 63 (Resrisiko beim Nuter)			akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA) VT 1: App-seitige Verarbeitung Kontaktereignisse/VT2: Kontaktfall/VT4: Infektfall		Risikobewertung															
				Schadensausmaß													
Risiko-Quelle	**Bedrohung/ Risiko**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
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 60			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) (Z 117)	Ja	2	4	4	4	0	0	0	4	4	4	8	ZB, TR, IV , VT, IG	siehe Z 117			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 funkspektrum 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 Grundsatzenscheidung 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	Designentscheidungen B-1-5ff.			bedingt 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			bedingt 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	Avv mit DL, inkl. TOM , Designentscheidungen D-11-1			beidingt 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 77)	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 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)	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 Verabeitung 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					
	Freiheitsgewinne bei Nutzung der App (Immunitätsausweis, Zugangserleichterung zu staatlichen/ kommunalen Leistungen)																	
	Freiheitsbeschränkungen bei Nicht-Nutzung der App (zugangsbeschränkungen zu staatlichen/ privaten Leistungen)																	
	Gewöhnung an Überwachung durch Staat und Markt																	
	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	Designentscheidungen D-2.2-3			