Datenschutzfolgenabschätzung (DSFA) VT 5: PPA_EDUS (10.02.2021 und 17.02.2021) + Fehlerbericht + Release 2.14 (11.11.2021) (Stand: 11.11.2021)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können**	**Restrisiko**
	4	**1) Unbefugte oder unrechtmäßige Verarbeitung durch CWA**																		
R4- Apple / Google	5	Unklare Verantwortlichkeiten in Bezug auf die Datenverarbeitungen	Zweck und Mittel der Datenverarbeitung werden nicht vom Verantwortlichen bestimmt. Durch die Nutzung von Apple/ Google für den Device-Check besteht das Risiko, dass durch diese Datenverarbeitungen durchgeführt werden, die über den Check hinausgehen.	Ja	2	4	4	1	1	1	1	4	4	4	8	RM, DM, VT, IG, IV, TR, ZB	Nutzung des speziellen von Apple/ Google bereitgestellten DeviceCheck-Verfahrens. Designentscheidung D-2-2c.			akzeptabel mit Evaluation
R8- Behörden	6	Fehlende Rechtsgrundlage/ fehlende Garantien für Datenübermittlung in USA im Rahmen der Device-Authentifikation.		Ja	2	4	4	4	1	1	1	4	4	4	8	RM, DM, VT, IG, IV, TR, ZB	Designentscheidung D-2.2-3 (Freiwilligkeit der Datenverarbeitung); PPA/ EDUS-Einwilligung wird eingeholt (siehe Designentscheidungen D-2-2c).			akzeptabel mit Evaluation
R1-CWA-Nutzer	7	Datenverarbeitungen ohne/ nach widerrufener PPA/ EDUS/ Fehlerberichts-Einwilligung	Ein Nutzer kann sich zu jedem Zeitpunkt dazu entscheiden die PPA/ EDUS-PPA/ EDUS-Einwilligung zum Teilen der Daten zu widerrufen. Da es nach der Datenübertragung der Daten von der CWA-App an den Donation-Server/ CWA Log-Server keine Möglichkeit gibt, eine Zuordnung zwischen dem Nutzer und den von ihm bereitgestellten Daten herzustellen, ist es technisch nicht möglich, die vom Nutzer bereitgestellten Daten selektiv zu löschen.	Ja	1	4	4	4	4	4	0	4	0	4	4	RM, DM, VT, IG, IV, TR, ZB	Siehe Designentscheidungen (D-2.1-2 (Install), D-2.1-6 (Upload) + Designentscheidung D-3.1-1 + Designentscheidung (Widerruf) D-3.1-8; CWA-Nutzer kann in den Einstellungen seine PPA/ EDUS-Einwilligung widerrufen (Designentscheidung D-2-2c).			akzeptabel
R1-CWA-Nutzer	8	Unwirksame PPA/ EDUS/ Fehlerberichts-Einwilligung durch fehlende Freiwilligkeit ("erzwungene Einwilligung") /erzwungene Freiwilligkeit	DSFA-Team sieht für die Verarbeitungstätigkeit PPA_EDUS + Senden des Fehlerberichts kein besonderes Risiko.	Nein											-					
R5-Arbeitgeber, Versicherungen	9	Erzwungene Freiwilligkeit der DV von personenbezogenen Daten (pD)	DSFA-Team sieht für Verarbeitungstätigkeite PPA_EDUS + Senden des Fehlerberichts kein besonderes Risiko.	Nein											-					
R1-CWA-Nutzer	10	Unwirksame PPA/ EDUS/ Fehlerberichts-Einwilligung aufgrund fehlender/ fehlerhafter ausdrückliche Einwilligungserklärung (technischer Einwilligungs-Akt)		Ja	1	4	4	4	4	4	4	4	4	4	4	RM	Siehe Designentscheidungen D-2-2c.			akzeptabel
R1-CWA-Nutzer	11	Unwirksame PPA/ EDUS/ Fehlerberichts-Einwilligung aufgrund fehlender Information über Umfang und Folgen	Lücken in der Information über die Datenverarbeitung durch Apple und Google könnten zur Unwirksamkeit der Einwilligungserklärung insgesamt führen.	Ja	2	4	4	4	4	4	4	4	4	4	8	DM, VT, IG, IV, TR, ZB	Abgestimmte Datenschutzinformationen liegt vor, siehe Designentscheidung D-2-2c.			akzeptabel mit Evaluation u ggf. Anpassung Datenschutzerklärung
R1-CWA-Nutzer	12	Unwirksame PPA/ EDUS/ Fehlerberichts-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 formuliert, Übersetzungen liegen vor.			akzeptabel, mit Evaluation und ggf. Anpassung Datenschutzerklärung
R1-CWA-Nutzer	13	Unbefugte Nutzung der Funktionen durch Minderjährige unter 16 Jahre	Minderjährige könnten an PPA_EDUS teilnehmen oder Fehlerberichte senden, ohne dass diese etwa die Datenübermittlung an Apple/ Google ab- und einschätzen könnten. Das RKI könnte PPA und EDUS auf Minderjährige bezogen auswerten.	Ja	4	4	4	4	4	4	4	4	4	4	16	DM, VT, IG, IV, TR, ZB	Siehe Designentscheidungen D-3.1-2, eine Altersabfrage erfolgt nicht; die Auswertemöglichkeiten des RKI und Rückschluss auf Minderjährige sind nicht möglich, da Altersgruppenabfrage bis 29 Jahre.		Verhältnismäßigkeit Restrisiko ist generell bewertet (siehe DSFA-Bericht), Folge des Verzichts auf Erhebung Altersangabe und weiterer Daten.	bedingt akzeptabel
R4- Apple / Google	14	Abhängigkeiten von Dienstleistern/ Software- und Firmware-Hersteller (Ausfall externer Dienstleistern) - Google/ Apple	PPA und EDUS, aber auch die Funktion zum Versenden der Fehlerberichte, sind ohne die Device-Prüfung von Apple/ Google nicht möglich. Bei einem Ausfall des Dienstleisters könnten kein PPA und EDUS erfolgen. Der Dienst wäre nicht verfügbar und die Nutzung wäre eingeschränkt.	Ja	2	0	0	0	2	0	2	2	3	2	6	VF, TR	Designentscheidungen zur Nutzung Device Check von Apple und Google (siehe Designentscheidung D-2-2c).			akzeptabel, mit Evaluation
R4- Apple / Google	15	Fehlende/ unzureichende vertragliche Regelungen mit Dienstleistern (Auftragsverarbeitung/ Vertrag zur gemeinsamen Verantwortung)		Ja	2	3	3	3	3	0	2	2	3	3	6	ZB , TR	AVV/ gem. Verantwortung/ Leistungsbeschreibung/ (nur soweit mgl.), siehe Dokument "Designentscheidungen D-5.1-1 / für betriebssystemseitige Verarbeitungen bleiben Apple und Google verantwortlich.			akzeptabel, mit Evaluation
R4- Betreiber Server (T)	16	Fehlende unzureichende vertragliche Regelungen mit Dienstleistern (Auftragsverarbeitung/ Vertrag zur gemeinsamen Verantwortung) - mit T/SAP	Keine gesteigerten Risiken durch PPA/ EDUS und das Senden der Fehlerberichte.	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- Betreiber Server (T)	17	Identifizierung der Nutzer (direkte Identifizierung) auf dem CWA-Data Donation Server	Durch eine Speicherung von Token und/ oder IP-Adressen auf dem Data Donation Server/ CWA Log Server könnte eine Identifizierung möglich sein.	Ja	1	1	4	1	1	1	1	1	1	1	4	DM	Siehe Designentscheidung D-2-2c und D-5.1-13a, direkte Identifizierung vom Token nicht möglich, AVV (inkl. TOM) T/ SAP, siehe Designentscheidung D-11-1.			akzeptabel
R4- Apple / Google	18	Erhebung und Speicherung nicht-notwendiger Daten, inklusive Nutzer- und Metadaten durch Apple/ Google	Durch die Token-Anfrage beim Device Check könnten Nutzer- und Metadaten gespeichert werden, die zur Identifikation von CWA-Nutzern genutzt werden könnten. Wenn die Fehlerberichts-Funktion über längere Zeit genutzt wird, sind auch längerfristige Analysen zum Nutzungsverhalten der CWA-App möglich.	Ja	3	4	4	0	0	0	0	2	0	4	12	DM, IG, ZB	Siehe Designentscheidung D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPA/ EDUS-Einwilligung der CWA-Nutzer ist erforderlich.		Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgegnen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen. Diese machen die Datenverarbeitung aber nicht vollständig transparent.	bedingt akzeptabel
R4- Betreiber Server (T)	19	Erhebung und Speicherung nicht-notwendiger Daten, inkl. Metadaten (TK-Daten) durch Betreiber Data Donation Server	Auf dem Data Donation Server/ CWA Log Server könnten IP-Adressen gespeichert werden, die eine Identifizierung der Teilnehmer erlauben.	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
R8- Behörden	20	Erhebung und Speicherung nicht-notwendiger Daten, inkl. Metadaten (TK-Daten) durch RKI	Auf dem Survey Answer Storage des RKI könnten IP-Adressen gespeichert werden, die eine Identifizierung der Teilnehmer erlauben.	Ja	3	3	3	1	1	1	1	3	3	3	9	DM, VT, IV, TR, ZB	Empfehlung an RKI, Datenschutz und Sicherheit zu gewährleisten			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	21	Erhebung und Speicherung nicht-notwendiger Daten, inkl. Metadaten (TK-Daten) durch Entwickler CWA (SAP)	In der CWA-App könnten Daten gespeichert werden, die den Entwicklern eine Identifikation der CWA-Nutzer erlauben.	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
	22	**2) Verarbeitung wider Treu und Glauben**																		
R4- Betreiber Server (T)	23	Auftreten von Sicherheitslöcken und Datenschutzvorfällen bei App-Entwickler 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
	24	**3) Für die Betroffenen intransparente Verarbeitung**																		
R8- Behörden	25	Unvollständige, unverständliche Datenschutzinformationen für PPA/ EDUS/ Fehlerberichts-Funktionalitäten der CWA		Ja	1	2	2	2	0	0	0	3	4	4	4	TR, ZB	Datenschutzinformationen.			akzeptabel
R8- Behörden	26	Unvollständige, unverständliche Datenschutzinformationen für Datenübermittlung in USA		Ja	3	2	2	2	0	0	0	3	4	4	12	TR, ZB	Siehe Designentscheidung D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPA/ EDUS-Einwilligung der CWA-Nutzer ist erforderlich.		Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgegnen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen. Diese machen die Datenverarbeitung aber nicht vollständig transparent.	bedingt akzeptabel
R4- Betreiber Server (T)	27	Gefahr der Intransparenz und fehlenden Prüfbarkeit der verarbeiteten Daten mittels der Server und Komponenten in der OTC (inklusive Data Donation Server)		Ja	3	0	0	0	0	0	0	2	3	1	9	TR, ZB	Datenschutzinformationen und Informationen auf GitHub und AV-Vertrag mit SAP/ T.			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	28	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 und AV-Vertrag mit SAP/ T.			akzeptabel mit Evaluation
R4- Apple / Google	29	Gefahr der Intransparenz und fehlenden Prüfbarkeit der verarbeiteten Daten und Funktionsweise im Rahmen der Device-Authentifikation durch Betriebssystemhersteller		Ja	3	2	2	2	0	0	0	3	4	4	12	T R, IV	Siehe Designentscheidung D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPA/ EDUS-Einwilligung der CWA-Nutzer ist erforderlich.		Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgegnen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen. Diese machen die Datenverarbeitung aber nicht vollständig transparent. Eine Prüfbarkeit ist damit auch nicht gegeben.	bedingt akzeptabel
	30	**4) Unbefugte Offenlegung von und Zugang zu Daten**																		

Datenschutzfolgenabschätzung (DSFA) VT 5: PPA_EDUS (10.02.2021 und 17.02.2021) + Fehlerbericht + Release 2.14 (11.11.2021) (Stand: 11.11.2021)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R4- Betreiber Server (T)	31	Re-Identifizierung durch Korrelation der erhobenen Daten (+ Publikation)	Auch wenn die Daten im Kontext der DPA grundsätzlich in pseudonymisierter Form übertragen werden, kann nicht ausgeschlossen werden, dass unter speziellen Bedingungen (z.B. einer sehr geringen Anzahl an CWA-Nutzern die der Nutzung des Features zugestimmt haben und diese auch aktiv nutzen) Rückschlüsse auf einzelne Nutzer und deren Verhalten (z.B. mögliche Corona-Warnungen, Dauer bis zum Teilen der Schlüssel, ...) möglich werden könnten. Die Offenbarung der CWA-Nutzer kann dazu führen, dass der CWA-Nutzer staatlichen Kontrollmaßnahmen ausgesetzt wird. In einem hypothetischen Scenario, in welchem SAP/Telekom als Angreifer fungieren, könnten diese die von CWA-Nutzern geteilten PPA-Daten nutzen, um diese auf anderen Medien öffentlich zu verbreiten. Dadurch könnte es einem Angreifer möglich sein, anhand neuer, ihm zugänglicher Datenpunkte, eine Re-Identifikation von CWA-Nutzer einfacher durchzuführen.	Ja	2	2	2	1	1	1	1	1	1	2	4	DM, VT, ZB	AV-Verträge mit DL, inkl. TOM , Designentscheidungen D-11-1.			akzeptabel
R4- Betreiber Server (T)	32	Re-Identifizierung durch optionale Parameter bei PPA und EDUS	Im Falle sehr geringer Nutzerzahlen kann auch schon die Auswahl bestimmter optionaler Parameter (z.B. (Bundesland / Kreis), Altersgruppe (bis 30, 31-59, 60 oder älter), ...) das Re-Identifikationsrisiko für einen Nutzer erhöhen.	Ja	2	2	2	1	1	1	1	1	1	2	4		AV-Verträge mit DL, inkl. TOM , Designentscheidungen D-11-1.			akzeptabel
R4 - Softwareentwickler / SAP	33	Re-Identifizierung CWA-Nutzer durch die Fehlerberichte	Mit der Einführung des Fehlerberichts wird es dem CWA-Nutzer ermöglicht, Vorgänge in seiner CWA-App zu erfassen und anschließend dem RKI zur Verfügung zu stellen. Die Funktion dient dazu, Fehler der CWA-App bei den CWA-Nutzern zu finden, um diese in einem späteren Update zu beheben. Dafür werden in der CWA-App des CWA-Nutzers verschiedene Prozesse und Ereignisse geloggt. Diese erfassten Prozesse/ Ereignisse werden dann an das RKI übermittelt und der CWA-Nutzer erhält eine eindeutige Nummer, die zu seinem Fehlerbericht gehört. Die Log-Datei wird nach erfolgreicher Übertragung von geschulten Entwicklern auf das Problem analysiert. Typischerweise wird der CWA-Nutzer diese ID beim Support bei der Schilderung des Problems mitangeben. Der Entwickler kann sich das Fehlerbericht anschauen und mit einem Nutzeraccount in Verbindung bringen, somit besteht die Gefahr, dass ein Entwickler einen positiv getesteten CWA-Nutzer re-identifizieren kann.	Ja	3	3	3	1	1	1	1	3	3	3	9	DM, VT, IV, T, ZB	Verpflichtung der Entwickler auf Vertraulichkeit			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	34	Offenlegung von personenbezogenen-/ Gesundheitsdaten	Die Fehlerberichte können (Meta-)daten zum Kontakttagebuch, Eventregistrierung, Schnelltestprofil, Testergebnisse, inkl. Name und Vorname der CWA-Nutzer enthalten. Durch die Übermittlung an SAP/ T könnten diese (un-)beabsichtigt Kenntnis von Gesundheitsdaten oder anderen sensiblen Daten zum Nutzungsverhalten erlangen und missbräuchlich Profile der CWA-Nutzer erstellen. Die CWA-App ermöglicht es dem CWA-Nutzer auch seinen Fehlerbericht lokal auf dem Gerät zu speichern, um diesen selbst einzusehen und auszuwerten. Der Fehlerbericht enthält – wie oben beschrieben – verschiedene Informationen zur Nutzung der CWA-App. Daher ist es grundsätzlich nicht auszuschließen, dass auch Informationen über ein positives Testergebnis (möglicherweise indirekt) im Fehlerbericht enthalten sein können. Sofern dieser Fehlerbericht anderen zugänglich gemacht wird, besteht die Gefahr, dass der CWA-Nutzer unabsichtlich Informationen zu einem Gesundheitszustand anderen preisgibt.	Ja	3	3	3	1	1	1	1	3	3	3	9	DM, VT, IV, T, ZB	Personenbezogene Daten werden aus dem Fehler-Bericht herausgefiltert, bevor der Fehlerbericht gespeichert/verschickt wird (DSK CWA App v2.2, Kap. 7.4.12.4).			akzeptabel mit Evaluation
R1-CWA-Nutzer	35	Offenlegung von personenbezogenen-/ Gesundheitsdaten	Der Fehlerbericht kann vom CWA-Nutzer über die CWA-App geteilt werden. Der CWA-Nutzer erhält eine eindeutige Nummer, die seinem Fehlerbericht zugeordnet ist. Der Fehlerbericht wird nach erfolgreicher Übertragung von geschulten Entwicklern analysiert. Bei einem CWA-Nutzer, der sich gesondert beim Support meldet (z.B. auf GitHub) und dort seinen Fehlerbericht-ID zusammen mit einer Fehlerbeschreibung angibt, kann ein Entwickler den Fehlerbericht einem Nutzeraccount – der dazu verwendet wurde, um das Problem zu melden – in Verbindung bringen. Abhängig von den Inhalten des Fehlerberichts sind möglicherweise Rückschlüsse auf das Nutzungsverhalten der CWA-App möglich. Sollten Probleme in der CWA-App auftreten und im Fehlerbericht dokumentiert sein, die auf ein positives Testergebnis hinweisen, besteht die Gefahr, dass ein Entwickler einen CWA-Nutzer (über den Nutzeraccount) als möglicherweise Corona identifiziert erkennen kann.	Ja	3	3	3	1	1	1	1	3	3	3	9	DM, VT, IV, T, ZB	Verantwortung des CWA-Nutzers, seine personenbezogenen Daten nicht offenzulegen und nicht über den Support den Fehlerbericht zu teilen.			akzeptabel mit Evaluation
R8- Behörden	36	Re-Identifizierung durch Protokollierung/ Übermittlung von IP-Adressen oder Identifiern zusammen mit Survey-Ergebnissen	Auf dem Survey Answer Storage des RKI könnten IP-Adressen gespeichert werden, die eine Identifizierung der Teilnehmer erlauben.	Ja	3	3	3	1	1	1	1	3	3	3	9	DM, VT, IV, TR, ZB	Empfehlung an RKI, Datenschutz und Sicherheit zu gewährleisten (Empfehlung: Einsatz Prozess für Client IP-Verschleierung).			akzeptabel mit Evaluation
R4- Apple / Google	37	Re-Identifizierung der CWA-Nutzer durch Token-Abfrage durch Betriebssystemhersteller		Ja	3	4	4	4	0	0	0	2	4	4	12	DM, VT, IG, TR, ZB	Siehe Designentscheidung D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPA/ EDUS-Einwilligung der CWA-Nutzer ist erforderlich.		Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgegnen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen. Diese machen die Datenverarbeitung aber nicht vollständig transparent.	bedingt akzeptabel
R4- Apple / Google	38	Zugang/ Zugriff zu Gesundheitsdaten (Infektionsstatus)	Apple/ Google erhalten durch die Token-Abfrage Daten, die für Apple/ Google den Abfragenden identifizierbar machen. Apple/ Google könnten auf den Infektionsstatus schließen, weil nur die Teilnehmer mit "roter Karte" an der Nutzerumfrage teilnehmen und sich damit diese einen Token abfragen. Für die Fehlerberichts-Funktion ab [Release 2.2] ergeben sich keine zusätzlichen Risiken.	Ja	1	4	4	4	0	0	0	2	4	4	4	DM, VT, IG, TR, ZB	Designentscheidung D-2-2c (Apple/ Google können von Token Anfrage im Rahmen von EDUS nicht auf "Rote Karte" schließen, da Token Anfragen auch über PPA erfolgen. Damit kein Rückschluss möglich.		Die Grundsatzentscheidung für das Framework von Apple/ Google bedingt das Vertrauen der Nutzer in diese Plattformen.	akzeptabel
R2- Hacker	39	Zugang/ Zugriff auf (Gesundheits-) Daten in auf CWA Data Donation Server/ CWA Log Server (z.B. Infolge Nutzung einfacher Passwörter, fehlender IT-Sicherheit)		Ja	2	1	2	2	2	0	0	0	0	3	6	ZB	AV-Verträge mit DL, inkl. TOM , Designentscheidungen D-11-1			akzeptabel mit Evaluation
R2- Hacker	40	Zugang/ Zugriff auf Gesundheitsdaten/ Infektionsstatus durch Überwachung des WiFi-/ Internetverkehrs (Kommunikation zwischen CWA und CWA-Data Donation Server)	Identifikation des Infektionsstatus nicht möglich.	Ja	1	1	3	3	2	0	0	0	0	3	3	ZB , VT, IG	AV-Verträge mit DL inkl. TOM (Transportverschlüsselung), Designentscheidungen D-11-1.			akzeptabel
R2- Hacker	41	Zugang/ Zugriff auf Gesundheitsdaten durch Nutzung des RKI-Links erlaubt einen Rückschluss auf bestimmte Informationen des Nutzers (EDUS)	Der Zugriff auf das RKI-Befragungstool soll für CWA-Nutzer ausschließlich unter bestimmten Bedingungen – getriggert durch spezielle Events – möglich sein. Daher sind im Falle einer Kommunikation zwischen dem Smartphone des CWA-Nutzers und dem RKI-Server Rückschlüsse auf mögliche „Events" als Auslöser der Interaktion möglich. Sollte ein Angreifer also den Netzwerkverkehr zwischen dem Smartphone und RKI überwachen können, wären Rückschlüsse auf z.B. eine Corona-Warnung (rote Kachel) eines CWA-Nutzers möglich. Für die Fehlerberichts-Funktion ab [Release 2.2] ergeben sich keine zusätzlichen Risiken.	Ja	3	3	3	1	1	1	1	3	3	3	9	DM, VT, IG, IV, TR, ZB	DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23.			akzeptabel mit Evaluation
R2- Hacker	42	Transaktionen Hijacking (Umfrageserver des RKI)		Ja	2	0	2	2	0	0	0	0	0	4	8	ZB	Empfehlung an RKI, Datenschutz und Sicherheit zu gewährleisten.			akzeptabel mit Evaluation
R4- Betreiber Server (T)	43	Unberechtigter Administratorenzugriff auf Daten auf Data Donation Server		Ja	1	0	4	1	1	1	1	4	4	4	4	VT, IV, TR, ZB	AV-Verträge mit DL inkl. TOM (Berechtigungskonzept, Zugriffskontrolle, Protokollierung) und Designentscheidung D-11-1.			akzeptabel
R8- Behörden	44	Unberechtigter Administratorenzugriff auf Daten auf Umfrage-Server des RKI (Survey Answer Storage des RKI)		Ja	1	0	4	1	1	1	1	4	4	4	4	VT, IV, TR, ZB	Empfehlung an RKI, Datenschutz und Datensicherheit zu gewährleisten.			akzeptabel

Datenschutzfolgenabschätzung (DSFA) VT 5: PPA_EDUS (10.02.2021 und 17.02.2021) + Fehlerbericht + Release 2.14 (11.11.2021) (Stand: 11.11.2021)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R8- Behörden	45	Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts- und Zugriffskontrolle ... (TOM) für den Umfrage-Server des RKI (Survey Answer Storage des RKI).		Ja	1	0	4	1	1	1	1	4	4	4	4	VT, IV, TR, ZB	Empfehlung an RKI, Datenschutz und Datensicherheit zu gewährleisten.			akzeptabel
R4- Betreiber Server (T)	46	Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts- und Zugriffskontrolle ...(TOM) für den CWA-Data-Donation Service		Ja	1	4	4	4	4	4	4	4	4	4	4	VT, IG, VF, A, R, IV, TR, ZB, DM	AV-Verträge mit DL inkl. TOM (Berechtigungskonzept, Zugriffskontrolle, Protokollierung).			akzeptabel
	47	**5) Ungerechtfertigter Datentransfer in Drittland**																		
R4- Apple / Google	48	Mögliche Datenübertragung in Drittstaaten im Rahmen der Authentifikationsprüfung (Apple)	Von den Betriebssystemherstellern wurde nicht verbindlich ausgeschlossen, dass die im Rahmen der API-Nutzung erhobenen und verarbeiteten Daten nicht in Drittstaaten mit möglicherweise geringerem Datenschutzniveau übermittelt werden. Daher stellt die mögliche Datenübermittlung in Drittstaaten (z.B. USA) insbesondere vor dem Hintergrund der aktuelle Rechtsprechung (Schrems 2 Urteil, Cloud Act) ein sehr großes Datenschutzrisiko dar. Im Rahmen des API-Aufrufs werden nicht abschließend bestimmte gerätespezifische Informationen an die Betriebssystemhersteller (Google/ Apple) geschickt. Der genaue Umfang und die Details zu den übermittelten Daten wurden bisher noch nicht offiziell offengelegt. Durch die Nutzung dieser API's könnten also potenziell personenbezogene Daten des Nutzers oder sensitive Daten der CWA-App an die Betriebssystemhersteller übertragen werden. Da die Nutzung der API unverzichtbar erscheint und die übertragenen Daten nicht vollständig offengelegt werden, besteht das Risiko einer von Nutzer unbeabsichtigten Datenweitergabe an die Betriebssystemhersteller.	Ja	3	4	4	4	0	0	0	1	4	4	12	T, ZB; DM, VT, IG	Siehe Designentscheidung D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPA/ EDUS-Einwilligung der CWA-Nutzer ist erforderlich.		Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgegnen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel,
R4- Apple / Google	49	Mögliche Datenübertragung in Drittstaaten im Rahmen der Authentifikationsprüfung (Google)	Von den Betriebssystemherstellern wurde nicht verbindlich ausgeschlossen, dass die im Rahmen der API-Nutzung erhobenen und verarbeiteten Daten nicht in Drittstaaten mit möglicherweise geringerem Datenschutzniveau übermittelt werden. Daher stellt die mögliche Datenübermittlung in Drittstaaten (z.B. USA) insbesondere vor dem Hintergrund der aktuelle Rechtsprechung (Schrems 2 Urteil, Cloud Act) ein sehr großes Datenschutzrisiko dar. Im Rahmen des API-Aufrufs werden nicht abschließend bestimmte gerätespezifische Informationen an die Betriebssystemhersteller (Google/ Apple) geschickt. Der genaue Umfang und die Details zu den übermittelten Daten wurden bisher noch nicht offiziell offengelegt. Durch die Nutzung dieser API's könnten also potenziell personenbezogene Daten des Nutzers oder sensitive Daten der CWA-App an die Betriebssystemhersteller übertragen werden. Da die Nutzung der API unverzichtbar erscheint und die übertragenen Daten nicht vollständig offengelegt werden, besteht das Risiko einer von Nutzer unbeabsichtigten Datenweitergabe an die Betriebssystemhersteller.	Ja	3	4	4	4	0	0	0	1	4	4	12	DM, VT, IG, TR, ZB	Siehe Designentscheidung D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPA/ EDUS-Einwilligung der CWA-Nutzer ist erforderlich.		Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgegnen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel
R4- Apple / Google	50	Mögliche Datenverarbeitung in Drittstaaten	Da von den Betriebssystemherstellern weder die übertragenen Daten noch der Verarbeitungsort offengelegt werden, besteht das Risiko einer unkontrollierbaren Datensammlung und Datenverarbeitung in Drittstaaten, die über kein dem EWR entsprechendes Datenschutzniveau verfügen. Sofern keine Offenlegung des Verarbeitungsorts und der übertragenen Daten erfolgt und solange nicht sichergestellt werden kann, dass die Daten durch ein dem EWR entsprechendes Datenschutzregelwerk vor einer missbräuchlichen Nutzung geschützt sind, ist eine missbräuchliche Nutzung (für andere Zwecke) der Geräte-/ Nutzerdaten nicht auszuschließen. Das stellt für die Nutzer der CWA ein unkalkulierbares Risiko dar.	Ja	3	4	4	4	0	0	0	1	4	4	12	TR, ZB, IG, VT, DM	Siehe Designentscheidung D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPA/ EDUS-Einwilligung der CWA-Nutzer ist erforderlich.		Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgegnen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel
R4- Apple / Google	51	Verhaltensanalyse durch die PPAC Nutzung	Da weder Google noch Apple bisher vollständig offengelegt haben welche Daten (und insbesondere welche Metadaten) im Rahmen der Device-Verifikation erhoben, genutzt und verarbeitet werden, kann nicht ausgeschlossen werden, dass Google/ Apple diese Daten (Metadaten) nutzen könnten, um eine Verhaltensanalyse derjenigen CWA-Nutzer durchzuführen, die PPAC nutzen. Die PPAC-Nutzungsdaten könnten insbesondere in Verbindung mit den Daten, die im Rahmen der Device-Registrierung und der App-Store Nutzung ohnehin schon bei den Betriebssystemherstellern vorhanden sind, Rückschlüsse auf die CWA-Nutzung ermöglichen. Es könnte möglicherweise gelingen, zu analysieren und auszuwerten, ob und wie die CWA-App genutzt wird. Sollte es den Betriebssystemherstellern gelingen diese Informationen noch mit den im ENF gespeicherten Informationen zu verknüpfen, so können auch Analysen bezüglich der Warnhäufigkeiten und damit der verbundenen Risikoexposition der CWA Nutzer nicht ausgeschlossen werden.	Ja	3	4	4	4	0	0	0	1	4	4	12	TR, ZB, IG, VT, DM	Siehe Designentscheidung D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPA/ EDUS-Einwilligung der CWA-Nutzer ist erforderlich.		Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgegnen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel
R4- Apple / Google	52	Hypothesenbildung Risikoaffinität	Diese Informationen könnten ermöglichen, Hypothesen bezüglich der Risikoaffinität (in Hinblick auf Corona-Infektionen) der CWA-Nutzer sowie deren Umgang mit Corona-Risiken zu bilden.	Ja	3	4	4	4	0	0	0	1	4	4	12	TR, ZB, IG, VT, DM	Siehe Designentscheidung D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPA/ EDUS-Einwilligung der CWA-Nutzer ist erforderlich.		Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgegnen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel
R4- Apple / Google	53	Indirekte Verhaltensanalyse	Sofern den Betriebssystemherstellern auch eine Zugriff auf Informationen aus dem Kontakttagebuch gelingen sollte, wären von einer möglichen Verhaltensanalyse potenziell auch alle im Kontakt-Tagebuch gepflegten Begegnungen (Personen/Orte) betroffen.	Ja	3	4	4	4	0	0	0	1	4	4	12	TR, ZB, IG, VT, DM	Siehe Designentscheidung D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPA/ EDUS-Einwilligung der CWA-Nutzer ist erforderlich.		Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgegnen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel
	54	**6) Verweigerung der Betroffenenrechte (Betrachtung der Unterstützung durch SAP/T)**																		
R4 - Softwareentwickler / SAP	55	Fehlende Umsetzung der Widerrufsmöglichkeit		Ja	3	2	2	2	1	1	1	2	2	2	6	IV, T, ZB	Widerruf der PPA/ EDUS-Einwilligung per Einstellung möglich, Designentscheidung D-2-2c, auf dem Servern keine Herstellung des Personenbezugs zur Erfüllung Betroffenenrechte, Designentscheidung D-8-1.			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	56	Nichtbeachtung von Auskunftsrechten (keine Verpflichtung zur Herstellung Personenbezug) - Art. 11		Ja	1	4	0	0	0	0	0	0	4	0	4	DM	Designentscheidung/ Pseudonymisierung, keine Herstellung des Personenbezugs zur Erfüllung Betroffenenrechte, Designentscheidungen D-8-1.			akzeptabel
R4 - Softwareentwickler / SAP	57	Nichtbeachtung von Löschungsersuchen, Berichtigungsersuchen - Art. 11		Ja	1	0	0	1	0	4	0	4	0	0	4	DM	Designentscheidung/ Pseudonymisierung, keine Herstellung des Personenbezugs zur Erfüllung Betroffenenrechte Designentscheidungen D-8-1.			akzeptabel
R4 - Softwareentwickler / SAP	58	Fehlende Übertragbarkeit		Ja	1	0	0	0	0	0	0	4	0	4	4	IV	Designentscheidung/ Pseudonymisierung, keine Herstellung des Personenbezusg zur Erfüllung Betroffenenrechte Designentscheidungen D-8-1.			akzeptabel
R4- Apple / Google	59	Fehlende/ unzureichende Löschung der Daten auf den Servern von Apple/ Google bei Löschersuchen	Die Datenerhebung und Verarbeitung durch die BS-Hersteller ist nicht vollständig offengelegt. Es ergeben sich daher Datenschutzrisiken für die CWA-Nutzer, die sich durch den Verzicht auf oder unzureichende Löschung von personenbeziehbaren Daten durch die BS-Hersteller ergeben.	Ja	3	4	4	0	0	0	0	4	4	4	12	DM, VT, IV, TR, ZB	Siehe Designentscheidung D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPA/ EDUS-Einwilligung der CWA-Nutzer ist erforderlich.		Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgegnen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel
R4 - Softwareentwickler / SAP	60	Fehlende/ unzureichende Löschung der Daten bei De-Installation der App/ Zurücksetzen der App (Frontend)		Ja	1	4	0	0	0	0	0	4	0	4	4	DM	Siehe Ausführungen zur Löschung in dem DSK CWA und die Optimierung des End-of-Live Verhaltens der App (Designentscheidung D-9-9).			akzeptabel

Datenschutzfolgenabschätzung (DSFA) VT 5: PPA_EDUS (10.02.2021 und 17.02.2021) + Fehlerbericht + Release 2.14 (11.11.2021) (Stand: 11.11.2021)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können**	**Restrisiko**
	61	**7) Verwendung der Daten zu inkompatiblen Zwecken**																		
R8- Behörden	62	De-Anonymisierung/ De-Pseudonymisierung von Nutzern anhand von optionalen Lokalisierungsdaten	Die kleinteilige Datenerhebung auf Kreisebene bzw. Stadtbezirksebene kann bei sinkenden Inzidenzzahlen zur Re-Identifizierung von Nutzern führen.	Ja	3	3	3	3	0	0	0	3	3	3	9	ZB, TR, IV, VT, IG, DM	Empfehlung RKI zur Einhaltung Datenschutz und Datensicherheit (keine Aufhebung der Pseudonymisierung).			akzeptabel mit Evaluation
R2- Hacker	63	Temporäres CWA-Tracking	Sofern den Daten, die von der CWA in pseudonymisiert Form an das Backend übertragen werden, ein Identifier hinzugefügt wird, der nicht ausschließlich zu einmaligen Nutzung vorgesehen ist, könnte es möglich sein, ein temporares Tracking der CWA-Nutzer zu implementieren, sofern der Identifier eine längere Gültigkeitsdauer hat und somit möglicherweise mehrere Datensätze mit einem identischen Identifier im Backend angelegt werden würden. Das Risiko für einen CWA-Nutzer ist dabei abhängig von der Gültigkeitsdauer des Identifiers und der Anzahl der übertragenen Datenpakete. In Verbindung mit dem in Zeile 63 benannten Risiko - im Falle geringer Nutzerzahlen - könnte solch ein Tracking das Re-Identifikationsrisiko deutlich erhöhen. Dieser Angriff müsste jedoch für jeden User einzeln durchgeführt werden; es müsste sich um einen gezielten Angriff handeln.	Ja	1	4	4	0	0	0	0	4	4	4	4	DM, VT, ZB, TR, IV	Restrisiko beschrieben in DSK-Rahmenkonzept Kap. 14.28.20 - 14.28.23.			akzeptabel
R8- Behörden	64	Nutzungs-Profilbildung des CWA-Nutzers	Wenn die Fehlerberichts-Funktion über längere Zeit genutzt wird, sind auch längerfristigen Analysen zum Nutzungsverralten der CWA-App durch den CWA-Nutzer möglich. Dadurch könnte ein Nutzungsprofil erstellt werden, sofern der CWA-Nutzer dieses anderen, etwa auch dem RKI, zu Verfügung stellt.	Ja	2	3	3	1	1	1	1	3	3	3	6	DM, VT, IV, T, ZB				akzeptabel mit Evaluation
	65	**8) Verarbeitung nicht richtiger Daten**																		
R1-CWA-Nutzer	66	Manipulation von Daten/ Evaluationen/ Ergebnissen/ Nutzerbefragungen des RKI durch vorgetäuschten CWA-Nutzer (ohne Maßnahmen)	Befragungsergebnisse dürfen nicht durch bewusste/ unbewusste Manipulation verfälscht werden. Insofern sollten technisch relativ einfach machbare, umfängliche Manipulationen minimiert werden. Im Falle einer offen durchgeführten (frei im Internet zugänglichen) Studie muss die Richtigkeit der übermittelten Daten durch Prozesse und Analysen in Hinblick auf Korrektheit und Plausibilität geprüft werden. Ohne entsprechende Vorkehrungen ist die fachlich erforderliche Richtigkeit und Qualität der Daten nicht zu gewährleisten.	Ja	4	1	1	3	1	3	1	1	1	1	12	IG, AT	OTP-Alternativen wurden geprüft und dokumentiert; Designentscheidung D-2-2c.		Dieses Risiko mangelnder Datenqualität kann technisch durch Maßnahmen des "Device Checks" der Betriebssystemhersteller gesenkt werden.	bedingt akzeptabel
R1-CWA-Nutzer	67	Manipulation von Daten/ Evaluationen/ Ergebnisse/ Nutzerbefragungen des RKI durch vorgetäuschten CWA-Nutzer (Apple)	Sofern es CWA-Nutzern im Rahmen der Datenerfassung gelingt, technisch vorzutäuschen, valide Daten zu schicken (z.B. Simulation von API Aufrufen via Skript, …) wäre es möglich, die Daten der Evaluation zu verfälschen, unrichtige Daten zuzusteuern und die Datenbasis so zu verfälschen, dass sie fachlich nicht mehr nutzbar wäre. Aufgrund des OpenSource-Ansatzes wäre ein im Quellcode der CWA enthaltener "statischer" Link zu einer Befragungswebsite einfach und schnell im Source-Code zu identifizieren. Somit wäre der Link "quasi direkt" auch von außerhalb der CWA aufrufbar. In der Folge könnte nicht sichergestellt werden, dass die Evaluationsgrundlagen und Befragungsergebnisse nicht durch bewusste Manipulation verfälscht werden. In einem solchen Fall wäre die fachlich erforderliche Richtigkeit und Qualität der Daten nicht gewährleistet.	Ja	2	1	1	3	1	3	1	1	1	1	6	IG, AT	Sicherung der Datenqualität durch DeviceCheck Apple, Designentscheidung D-2-2c ; Durch Apple erfolgt eine Verifikation, dass es sich um ein Apple-Gerät handelt - die Software selbst wird nicht verifiziert.			akzeptabel
R1-CWA-Nutzer	68	Manipulation von Daten/ Evaluationen/ Ergebnissen/ Nutzerbefragungen des RKI durch vorgetäuschten CWA Nutzer (Google)	Sofern es CWA-Nutzern im Rahmen der Datenerfassung gelingt, technisch vorzutäuschen, valide Daten zu schicken (z.B. Simulation von API Aufrufen via Skript, …), wäre es möglich, die Daten der Evaluation zu verfälschen, unrichtige Daten zuzusteuern und die Datenbasis so zu verfälschen, dass sie fachlich nicht mehr nutzbar wäre. Aufgrund des OpenSource-Ansatzes wäre ein im Quellcode der CWA enthaltener "statischer" Link zu einer Befragungswebsite einfach und schnell im Source-Code zu identifizieren. Somit wäre der Link "quasi direkt" auch von außerhalb der CWA aufrufbar. In der Folge könnte nicht sichergestellt werden, dass die Evaluationsgrundlagen und Befragungsergebnisse nicht durch bewusste Manipulation verfälscht werden. In einem solchen Fall wäre die fachlich erforderliche Richtigkeit und Qualität der Daten nicht gewährleistet.	Ja	1	1	1	3	1	3	1	1	1	1	3	IG, AT	Sicherung der Datenqualität durch DeviceCheck Google, Designentscheidung D-2-2c. Durch Google erfolgt die Verifikation, dass die Software/ App über den Play Store (trusted source) heruntergeladen wurde.			akzeptabel mit Evaluation
R1-CWA-Nutzer	69	Manipulation von Daten/ Evaluation/ Ergebnisse Nutzerbefragung des RKI durch bewusste Falscheingabe	Nutzer könnten sich entscheiden, die Fragen des RKI bewusst falsch zu beantworten oder dies unbewusst zu tun. Sollte sich eine signifikante Menge an Nutzern dafür entscheiden, einzelne Fragen oder den Gesamtfragebogen falsch auszufüllen, wären die Auswertungsergebnisse nicht belastbar. Verlässliche Rückschlüsse könnten daraus nicht gezogen werden. Risikoerhöhend wirkt der OpenSource-Ansatz (siehe Zeile 67).	Ja	3	1	1	3	1	3	1	1	1	1	9	IG, AT	Restrisiko beschrieben in DSK-Rahmenkonzept Kap. 14.28.20 - 14.28.23.			akzeptabel mit Evaluation
R2- Hacker	70	Manipulation/ Störung des Authentifizierungsprozesses		Ja	3	1	1	3	1	3	1	1	1	1	9		Mit Nutzung der DeviceChecks von Apple/ Google technisch erschwert.			akzeptabel mit Evaluation
	71	**9) Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler)**																		
R2- Hacker	72	DNS-Spoofing / Man-in-the-Middle Attacke, um statt mit dem Backend mit einem Server eigener 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 auch den Data Donation Server/ CWA Log Server und den Survey Server des RKI. Durch Senden unzulässiger oder gefälschter Inhalte könnte der Angreifer die Funktion der CWA-App beeinträchtigen oder gar zum Erliegen bringen. Außerdem kann er sich so Zugriff auf Informationen verschaffen, die nicht für ihn bestimmt sind, und versuchen, beispielsweise über Metadaten der Netzwerkverbindung einen Personenbezug herzustellen.	Ja	2	0	0	0	4	4	4	4	4	4	8	VT, DM, ZB, T , IV	Designentscheidungen B-1-5ff. Als Abwehrmaßnahmen werden neben einer strikten Inputvalidierung TLS-Zertifikatvalidierung und -pinning eingesetzt. Auf Grund des etablierten Zertifikatpinnings wird ein Einsatz von DNSSEC auf Serverseite derzeit nicht für notwendig erachtet.			akzeptabel mit Evaluation
R2- Hacker	73	Denial of Service Angriffe durch Missbrauch der CWA-App	Kein gesteigertes Risiko für PPA EDUS + Fehlerberichtsfunktion.	Ja	3	0	0	0	3	2	3	0	0	0	9	VF, TR	Designentscheidungen D-5.1-16.			akzeptabel mit Evaluation
R2- Hacker	74	Denial of Service (Mutwillige Überlastung) Angriffe auf Server durch Laden ungültiger Daten	Kein gesteigertes Risiko für PPA EDUS + Fehlerberichtsfunktion	Ja	3	0	0	0	3	2	3	0	0	0	9	VF, R	AV-Verträge mit DL, inkl. TOM , Designentscheidungen D-11-1.			akzeptabel mit Evaluation
	75	**10) Verarbeitung über die Speicherfrist hinaus**																		
R4- Apple / Google	76	Unbefristete Speicherung von Daten (inkl. Metadaten) auf den Servern von Apple/ Google und mögliche spätere Verkettung (Verhaltensanalysen durch die ENF-Nutzung)	Da das ENF bereits als Bestandteil des Betriebssystems implementiert wurde, sind die Risiken der „Hypothesenbildung Risikoaffinität" und „indirekte Verhaltensanalyse" unabhängig von den PPAC-Nutzung bereits möglich.	Ja	3	4	1	1	0	0	0	3	3	4	12	DM, ZB	Siehe Designentscheidung D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept vt.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPA/ EDUS-Einwilligung der CWA-Nutzer ist erforderlich.		Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgegnen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen. Im Übrigen ist dieses Risiko eine Folge der Grundsatzentscheidung für das ENF auf Apple/ Google zurückzugreifen.	bedingt akzeptabel

Datenschutzfolgenabschätzung (DSFA) VT 5: PPA_EDUS (10.02.2021 und 17.02.2021) + Fehlerbericht + Release 2.14 (11.11.2021) (Stand: 11.11.2021)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können**	**Restrisiko**
R4- Betreiber Server (T)	77	Unbefristete Speicherung von Daten (inkl. Metadaten) auf Data-Donation Server/ CWA Log Server und mögliche spätere Verkettung mit anderen personenbezogenen Daten	Im Rahmen von [Release 2.2] auch für die Löschung der Fehlerberichte und Historie geprüft.	Ja	2	4	1	1	0	0	0	3	3	4	8	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 angebotenen Mitteln. Ein Ausnullen der betroffenen Speicherbereiche wird nicht vorgenommen). Siehe Aufführungen zur Löschung in den Teil-DKS, Designentscheidungen (D-8-1ff) und AVV inkl. TOM.	Anpassung der Löschfristen, DSK Server v1.13, Kap. 7.3.1.		akzeptabel mit Evaluation
R8- Behörden	78	Unbefristete Speicherung von Daten (inkl. Metadaten) auf dem Survey Server des RKI	In einem hypothetischen Szenario, in dem z.B. das RKI als ein möglicher Angreifer fungiert, könnte das RKI versuchen, die vom CWA-Nutzer bereitgestellten Daten nach deren Analyse/ Auswertung weiterzuverarbeiten und diese nicht zu löschen. Die Daten wären somit über den ursprünglichen Zweck weiterhin verfügbar. Zudem könnte das RKI die Daten dazu verwenden, um eine Datenverarbeitung über den ursprünglichen Zweck hinaus zu betreiben.	Ja	2	4	1	1	0	0	0	3	3	4	8	DM, ZB	Empfehlung an RKI, Datenschutz und Datensicherheit zu gewährleisten.			akzeptabel mit Evaluation
R4- Betreiber Server (T)	79	Unbefristete Speicherung unrichtiger/ negativer/ nicht-notwendiger Daten		Ja	1	4	4	4	0	0	4	2	4	4	4	DM, ZB	AV-Verträge mit DL inkl. TOM , Designentscheidungen D-11-1.			akzeptabel
	80	**11) Risiken durch Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt**																		
R4- Apple / Google	81	Ausweitung der in die CWA-App integrierten Funktionen	Sofern von den Betriebssystemhersteller nicht ausgeschlossen wird, dass Daten auch in Drittstaaten außerhalb des EWR (z.B. USA) übertragen werden, könnten CWA-Nutzer an dem hohen Datenschutzniveau der CWA zweifeln. Da nicht offengelegt werden kann, welche Daten genau an die Betriebssystemhersteller übermittelt werden, ist ein starker Vertrauensverlust der CWA-Nutzer zu erwarten (Reputationsschaden für Entwickler, Betreiber, Massenhafte De-Installation…). Dies stellt kein Risiko für die Rechte und Freiheiten der Betroffenen dar und wird daher nicht als Schwachstelle im Rahmen dieser DSFA betrachtet.	Nein	3	4	0	0	0	0	0	0	0	0	-	DM	Designentscheidungen D-2.2-3 (Freiwilligkeit), DSK_Rahmenkonzept, Kap. 14.20.3 und Folge der Grundsatz-Entscheidung für Apple /Google.			
R4- Apple / Google	82	Fehlende Akzeptanz des OTP Ansatzes Apple/ Google	Nutzer könnten schon allein deshalb nicht an PPA , EDUS + Fehlerberichtsfunktion teilnehmen, weil diese mit einer Device Prüfung durch Apple/ Google verbunden ist. Dies könnte dazu führen, dass so wenige Nutzer teilnehmen, dass keine Repräsentanz gegeben und damit der Zweck der Funktionen konterkariert wird. Fehlende Akzeptanz stellt kein Risiko für die Rechte und Freiheiten der Betroffenen dar und wird daher nicht als Schwachstelle im Rahmen dieser DSFA betrachtet.	Nein	4	4	0	0	0	0	0	0	0	0	-	DM	Designentscheidungen D-2.2-3 (Freiwilligkeit), DSK_Rahmenkonzept, Kap. 14.20.3 und Folge der Grundsatz-Entscheidung für Apple /Google.			