

Datenschutzfolgenabschätzung (DSFA) VT 5: PPA_EDUS (10.02.2021 und 17.02.2021)			Risikobewertung																
Risiko-Quelle	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ganzheitl.)	EW	Schadensausmaß										Soll-Maßnahmen - ID	(etablierte) Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko	
					Datensammlung	Verfügbarkeit	Integrität	Verfälschtheit	Authentizität	Reliabilität	Interferenzbarkeit	Transparenz	Zweckbindung / Nichterstattung	Risikolasse					
	Unbefugte oder unrechtmäßige Verarbeitung durch CWA																		
R4: Apple / Google	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	
BS-Behörden	Fehlende Rechtsgrundlage / fehlende Garantien für Datenübermittlung in USA im Rahmen der Device-Authentifizierung		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 für d eingeholt (siehe Designentscheidungen D-2-2c)		akzeptabel mit Evaluation	
R1:CWA-Nutzer	Datenverarbeitungen ohne/ nach widerlegener PPA/ EDUS-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 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-3-1-4; CWA-Nutzer kann in den Einstellungen seine PPA/ EDUS-Einwilligung widerrufen (Designentscheidung D-2-2c)		akzeptabel	
R1:CWA-Nutzer	Unwirksame PPA/ EDUS-Einwilligung durch fehlende Freiwilligkeit ("erzwungene Einwilligung") /erzwungene Freiwilligkeit	DSFA - Team sieht für die Verarbeitungstätigkeit PPA, EDUS kein besonderes Risiko.	Nein											-					
R5:Arbeitgeber, Versicherungen	erzwungene Freiwilligkeit der DV von pD	DSFA - Team sieht für die Verarbeitungstätigkeit PPA,EDUS kein besonderes Risiko.	Nein											-					
R1:CWA-Nutzer	Unwirksame PPA/ EDUS-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	Unwirksame PPA/ EDUS-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	Unwirksame PPA/ EDUS-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	Unbefugte Nutzung der Funktionen durch Minderjährige unter 16 Jahre	Minderjährige könnten an PPA, EDUS teilnehmen, 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 Auswertmöglichkeiten 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	Abhängigkeiten von Dienstleistern/ Software- und Firmware Hersteller (Ausfall externer Dienstleistern) - Google/ Apple	PPA und EDUS 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 Designentscheidungen D-2-2c)		akzeptabel, mit Evaluation	
R4: Apple / Google	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 betriebsystemseitige Verarbeitungen bleiben Apple und Google verantwortlich		akzeptabel, mit Evaluation	
R4: Betreiber Server (T)	Fehlende unzureichende vertragliche Regelungen mit Dienstleistern (Auftragsverarbeitung/ Vertrag zur gemeinsamen Verantwortung) - mit T/SAP	Keine gesteigerten Risiken durch PPA und EDUS	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)	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 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	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.	Ja	3	4	4	0	0	0	0	2	0	4	12	DM, IG, ZB	Siehe Designentscheidung D-2-2c; Restriktion 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 entgehen, 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)	Erhebung und Speicherung nicht-notwendiger Daten, inkl. Metadaten (TK-Daten) durch Betreiber Data Donation Server	Auf dem Data Donation 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	
BS-Behörden	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	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	
	Verarbeitung wider Treu und Glauben																		
R4: Betreiber Server (T)	Auftreten von Sicherheitslücken 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	
	Für die Betroffenen intransparente Verarbeitung																		
BS-Behörden	Unvollständige, unverständliche Datenschutzinformationen für PPA / EDUS Funktionalitäten der CWA		Ja	1	2	2	2	0	0	0	3	4	4	4	TR, ZB	Datenschutzinformation		akzeptabel	
BS-Behörden	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; Restriktion 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 entgehen, 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)	Gefahr der Intransparenz und fehlenden Prüfbarkeit der verarbeiteten Daten mittels der Server und Komponenten in der OTG (inklusive Data Donation Server)		Ja	3	0	0	0	0	0	0	2	3	1	9	TR, ZB	Datenschutzinformationen und Informationen auf GitHub und AVV-Vertrag mit SAP T		akzeptabel mit Evaluation	

Datenschutzfolgenabschätzung (DSFA) VT 5: PPA_EDUS (10.02.2021 und 17.02.2021)			Risikobewertung													Risikobewertung				
Risiko-Quelle	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (jahren)	EW	Datensammlung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Reliabilität	Intervallbarkeit	Transparenz	Zweckbindung / Nichtverwertung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko		
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	8	T, R	Datenschutzinformationen und Informationen auf GitHub und AV-Vertrag mit SAP IT			akzeptabel mit Evaluation	
R4: Apple/ Google	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. Restriktion ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPAW EDUS-Ermittlung der CWA - Nutzer ist erforderlich.	Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgehen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen. Diese machen die Datenverarbeitung aber nicht vollständig transparent. Eine	bedingt akzeptabel		
	Unbefugte Offenlegung von und Zugang zu Daten	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	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)	Re-Identifizierung durch Korrelation der erhobenen Daten (+ Publikation)	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	
R8: Behörden	Re-Identifizierung durch Protokollierung / Übermittlung von IP-Adressen oder Identifizieren 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-Verschiebung)			akzeptabel mit Evaluation	
R4: Apple / Google	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. Restriktion ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPAW EDUS-Ermittlung der CWA - Nutzer ist erforderlich.	Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgehen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen. Diese machen die Datenverarbeitung aber nicht vollständig transparent. Eine	bedingt akzeptabel		
R4: Apple / Google	Zugangs/ Zugriff zu Gesundheitsdaten (Infektionsstatus)	Apple/ Google erhalten durch die Token-Abfrage Daten, die für Apple/ Google den Abfragenden identifizierbar machen. Apple/ Google können auf den Infektionsstatus schließen, weil nur die Teilnehmer mit "roter Karte" an der Nutzerumfrage teilnehmen und sich damit diese einen Token abfragen.	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	Zugangs/ Zugriff auf (Gesundheits-) Daten in auf CWA Data Donation Server (z. Infolge Nutzung einfacher Parameter, 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	Zugangs/ 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	Zugangs/ 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 überwatchen können, wären Rückschlüsse auf z.B. eine Corona-Warnung (rote Karte) eines CWA-Nutzers möglich.	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	Transaktionen Hijacking (Umfrage-Server 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)	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	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	
R8: Behörden	Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts-, Zugangs- 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)	Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts-, Zugangs- 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	
	Unberechtigter Datentransfer in Drittland	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 aktuellen Rechtsprechung (Schwimm 2 Urteil, Cloud Act) ein sehr großes Datenschutzrisiko dar. Im Rahmen des API-Auflaufs werden nicht abschließend bestimmte gerätespezifische Informationen an die	Ja	3	4	4	4	0	0	0	1	4	4	12	T, ZB, DM, VT, IG	Siehe Designentscheidung D-2-2c. Restriktion ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPAW EDUS-Ermittlung der CWA - Nutzer ist erforderlich.	Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgehen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel		
R4: Apple / Google	Mögliche Datenübertragung in Drittstaaten im Rahmen der Authentifikationsprüfung (Apple)	Da von den Betriebssystemherstellern weder die übertragenen Daten noch die Verarbeitungsort offengelegt werden, besteht das Risiko einer unkontrollierten Datensammlung und Datenverarbeitung in Drittstaaten, die über kein den 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 Datenschutzniveau geschützt sind, ist eine missbrauchliche Verwendung der Daten durch Dritte nicht auszuschließen. 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 PPAW nutzen.	Ja	3	4	4	4	0	0	0	1	4	4	12	DM, VT, IG, TR, ZB	Siehe Designentscheidung D-2-2c. Restriktion ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPAW EDUS-Ermittlung der CWA - Nutzer ist erforderlich.	Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgehen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel		
R4: Apple / Google	Mögliche Datenverarbeitung in Drittstaaten		Ja	3	4	4	4	0	0	0	1	4	4	12	TR, ZB, IG, VT, DM	Siehe Designentscheidung D-2-2c. Restriktion ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPAW EDUS-Ermittlung der CWA - Nutzer ist erforderlich.	Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgehen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel		
R4: Apple / Google	Verhaltensanalyse durch die PPAW Nutzung		Ja	3	4	4	4	0	0	0	1	4	4	12	TR, ZB, IG, VT, DM	Siehe Designentscheidung D-2-2c. Restriktion ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPAW EDUS-Ermittlung der CWA - Nutzer ist erforderlich.	Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgehen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel		
R4: Apple / Google	Hypothesenbildung Risikofaktoren	Diese Informationen könnten ermöglichen, Hypothesen bezüglich der Risikofaktoren (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. Restriktion ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPAW EDUS-Ermittlung der CWA - Nutzer ist erforderlich.	Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgehen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel		
R4: Apple / Google	Indirekte Verhaltensanalyse	Solange den Betriebssystemherstellern auch ein Zugriff auf Informationen aus dem Kontakttagbuch gelingen sollte, wären von einer möglichen Verhaltensanalyse potenziell auch alle im Kontakt-Tagbuch gespeicherten 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. Restriktion ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23. Nutzer werden informiert. Die PPAW EDUS-Ermittlung der CWA - Nutzer ist erforderlich.	Auf eine Nutzerregistrierung wird verzichtet. Um der hypothetischen Gefahr manipulierter Endgeräte zu entgehen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel		

Datenschutzfolgenabschätzung (DSFA) VT 5: PPA_EDUS (10.02.2021 und 17.02.2021)			Risikobewertung																
Risiko-Quelle	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (jahren)	EW	Schadensausmaß										Soll-Maßnahmen - ID	(etablierte) Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko	
					Datensammlung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Reliabilität	Intervallierbarkeit	Transparenz	Zuschreibung / Nichtentstörung	Risikoklasse					
	Verweigerung der Betroffenenrechte (Betrachtung der Unterstützung durch SAP/IT)																		
R4 - Softwareentwickler / SAP	Fehlende Umsetzung der Widerrufsmöglichkeit		Ja	3	2	2	2	2	1	1	1	2	2	2	6	N, T, ZB	Widerruf der PPA/ EDUS-Einwilligung per Einstellung möglich. Designentscheidung D-2-2c, auf dem Servern keine Herstellung Personenbezug zur Erfüllung Betroffenenrechte. Designentscheidung D-8-1	akzeptabel mit Evaluation	
R4 - Softwareentwickler / SAP	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 Personenbezug zur Erfüllung Betroffenenrechte. Designentscheidungen D-8-1	akzeptabel		
R4 - Softwareentwickler / SAP	Nichtbeachtung von Lösungsersuchen, Berichtigungsersuchen - Art. 11		Ja	1	0	0	1	0	4	0	4	0	0	4	DM	Designentscheidung/ Pseudonymisierung, keine Herstellung Personenbezug zur Erfüllung Betroffenenrechte. Designentscheidungen D-8-1	akzeptabel		
R4 - Softwareentwickler / SAP	Fehlende Übertragbarkeit		Ja	1	0	0	0	0	0	0	4	0	4	4	IV	Designentscheidung/ Pseudonymisierung, keine Herstellung Personenbezug zur Erfüllung Betroffenenrechte. Designentscheidungen D-8-1	akzeptabel		
R4: Apple / Google	Fehlende/ unzureichende Löschung der Daten auf den Servern von Apple/ Google bei Lösungsersuchen	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 personenbedienbaren Daten durch die BS-Hersteller ergeben.	Ja	3	4	4	0	0	0	0	4	4	4	4	12	DM, VT, IV, TR, ZB	Siehe Designentscheidung D-2-2c, Restriktion 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 entgehen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen.	bedingt akzeptabel
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	4	0	4	4	DM	siehe Ausführungen zur Löschung in dem DSK CWA und die Optimierung des End-of-Life Verhaltens der App (Designentscheidung D-9-9)		akzeptabel	
	Verwendung der Daten zu inkompatiblen Zwecken																		
R8: Behörden	De-Anonymisierung/ De-Pseudonymisierung von Nutzern anhand von optionalen Lokalisierungsdaten	Die kleinteilige Datenerhebung auf Krisenebene bzw. Stadtbezirksebene kann bei sinkenden Inzidenzzahlen zur Re-Identifizierung von Nutzern führen.	Ja	3	3	3	3	0	0	0	3	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	Temporäres CWA-Tracking	Solten den Daten die von der CWA in pseudonymisierter Form an das Backend übertragen werden und ein Identifier hinzugefügt wird, der nicht ausschließlich zu einmaligen Nutzung vorgesehen ist, könnte es möglich sein, ein temporäres 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 würden. Das Risiko für einen CWA-Nutzer ist dabei abhängig von der Gültigkeitsdauer des Identifiers und der Anzahl der übertragenen.	Ja	1	4	4	0	0	0	0	4	4	4	4	4	DM, VT, ZB, TR, IV	Restrisiko beschrieben in DSK-Rahmenkonzept Kap. 14.28.20 - 14.28.23	akzeptabel	
	Verarbeitung nicht richtiger Daten																		
R1:CWA-Nutzer	Manipulation von Daten / Evaluationen / Ergebnissen/ Nutzerbefragungen des RKI durch vorgetauschten CWA-Nutzer (ohne Maßnahmen)	Befragungsergebnisse dürfen nicht soeben bewusste/unbewusste Manipulationen verrichtet werden. Insoweit sollen technisch relativ einfach machbare, umfangreiche 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 Solten es CWA-Nutzern im Rahmen der Datenerfassung gelingt, technisch vorzuzubereiten, valide Daten zu schicken (z.B. Simulation von API Aufrufen via Script, ...) 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 Befragungswebseite einfach und schnell im Source-Code zu identifizieren. Somit wäre der Link "quasi direkt" auch von außerhalb der Server des CWA-Nutzern im Rahmen der Datenerfassung möglich. Technisch vorzuzubereiten, valide Daten zu schicken (z.B. Simulation von API Aufrufen via Script, ...) 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 Befragungswebseite einfach und schnell im Source-Code zu identifizieren. Somit wäre der Link "quasi direkt" auch	Ja	4	1	1	3	1	3	1	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 Betriebssystemshersteller gesenkt werden. Siehe die folgenden Zeilen 64 und 64	bedingt akzeptabel
R1:CWA-Nutzer	Manipulation von Daten / Evaluationen / Ergebnissen/ Nutzerbefragungen des RKI durch vorgetauschten CWA-Nutzer (Apple)		Ja	2	1	1	3	1	3	1	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	Manipulation von Daten / Evaluationen / Ergebnissen/ Nutzerbefragungen des RKI durch vorgetauschten CWA-Nutzer (Google)		Ja	1	1	1	3	1	3	1	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	Manipulation von Daten / Evaluation / Ergebnisse Nutzerbefragung des RKI durch bewusste Fälschung	Nutzer könnten sich entscheiden die Fragen des RKI bewusst falsch zu beantworten oder dies unbewusst 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. Risikohöhernd wirkt der OpenSource-Ansatz (siehe Zeile 63).	Ja	3	1	1	3	1	3	1	1	1	1	1	9	IG, AT	Restrisiko beschrieben in DSK-Rahmenkonzept Kap. 14.28.20 - 14.28.23		akzeptabel mit Evaluation
R2: Hacker	Manipulation / Störung des Authentifizierungsprozesses		Ja	3	1	1	3	1	3	1	1	1	1	1	9		Mit Nutzung der DeviceChecks von Apple/ Google technisch erschwert.		akzeptabel mit Evaluation
	Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler)																		
R2: Hacker	DNS-Spoofing / Man-in-the-Middle Attacke, um statt mit Backend mit einem Server seiner Wahl zu kommunizieren (Vorgetauschter 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 und den Survey Server des RKI. Durch Senden unzulässiger oder gefälschter Inhalte könnte der Angreifer die Funktionen 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	Ja	2	0	0	0	4	4	4	4	4	4	4	8	VT, DM, ZB, T, IV	Designentscheidungen D-1-5f. Als Abwehrmaßnahmen werden neben einer strikten Invalidation TLS Zertifikatsvalidierung und -pinning eingesetzt. Auf Grund des etablierten Zertifikatspinning wird ein Einsatz von DNSSEC auf Serverseite derzeit nicht für notwendig erachtet.		akzeptabel mit Evaluation
R2: Hacker	Denial of Service Angriffe durch Missbrauch der CWA-App	Kein gesteigertes Risiko für PPA/EDUS	Ja	3	0	0	0	3	2	3	0	0	0	0	9	VF, TR	Designentscheidungen D-5.1-16		akzeptabel mit Evaluation
R2: Hacker	Denial of Service (Mutuelle Überlastung) Angriffe auf Server durch Laden unzulässiger Daten	Kein gesteigertes Risiko für PPA/EDUS	Ja	3	0	0	0	3	2	3	0	0	0	0	9	VF, R	AV-Verträge mit DL, inkl. TOM, Designentscheidungen D-11-1		akzeptabel mit Evaluation
	Verarbeitung über die Speicherfrist hinaus																		
R4: Apple / Google	Unbefristete Speicherung von Daten (inkl. Metadaten) auf den Servern von Apple/ Google und mögliche spätere Verketzung (Verhaltensanalysen durch die ENF-Nutzung)	Da das ENF bereits als Bestandteil des Betriebssystems implementiert wurde, sind die Risiken der Hypothesenbildung Risiko/Findat und indirekte Verhaltensanalyse unabhängig von den PPAC Nutzung bereits möglich.	Ja	3	4	1	1	0	0	0	0	3	3	4	12	DM, ZB	Siehe Designentscheidung D-2-2c, Restriktion 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 entgehen, welche die erhobenen Daten verfälschen, wird auf die "Device-Checks" der BS-Hersteller zurückgegriffen. Im Übrigen ist dieses Risiko eine Folge der Einsatzentscheidungen für das	bedingt akzeptabel
R4: Betreiber Server (T)	Unbefristete Speicherung von Daten (inkl. Metadaten) auf Data-Donation Server und mögliche spätere Verketzung mit anderen personenbezogenen Daten		Ja	2	4	1	1	0	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 Protokollausgaben auf der Datenbank des CWA-Servers sowie auf dem Objectstore, der als Übergabemedium zum CDN-Master ist, erfolgt mit den vom identischen Speicherbereich		akzeptabel mit Evaluation
R8: Behörden	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 von 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	0	3	3	4	8	DM, ZB	Empfehlung an RKI, Datenschutz und Datensicherheit zu gewährleisten		akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA) VT 5: PPA_EDUS (10.02.2021 und 17.02.2021)			Risikobewertung															
Risiko-Quelle	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schadensausmaß												Soll-Maßnahmen - ID	(etablierte) Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
			Schwachstelle (gesehen)	EW	Datensammlung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Realisierz	Intervallbarkeit	Transparenz	Zuspeicherung / Nichtverteilung	Risikobewertung				
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	AV-Verträge mit DL inkl. TOM, Designentscheidungen D-11-1		akzeptabel
	Risiken durch Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt																	
R4: Apple / Google	Ausweitung der in die CWA-App integrierten Funktionen	Solern 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 (Reputationschaden für Entwickler, Betreiber, Massenhalle De-Installation ...). Dies stellt kein Risiko für die Rechte und Freiheiten der Betroffenen dar und wird daher nicht als Risiko für die Rechte und Freiheiten der Betroffenen angesehen, weil diese mit einer Device-Profiling durch Apple/ Google verbunden ist. Dies könnte dazu führen, dass so wenige Nutzer teilnehmen, dass keine Repräsentanz gegeben und damit der Zweck der Funktionen kortekariert 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	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	fehlende Akzeptanz des OTP Ansatzes Apple/ Google		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		