Datenschutzfolgenabschätzung (DSFA)

VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für

					Risikobewertung												
					Schadensausmaß												
Risiko-Quelle	**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**	**Restrisiko**
	Unbefugte oder unrechtmäßige Verarbeitung durch CWA																
R4- Testcenter	Unklare Verantwortlichkeiten in Bezug auf die Datenverarbeitungen	Zweck und Mittel der Datenverarbeitung werden nicht vom Verantwortlichen bestimmt. Durch die Datenverarbeitung in den Testcentren/ PoC (eigene Verantwortliche) besteht das Risiko, dass durch diese Datenverarbeitungen durchgeführt werden, die über deren Verantwortung hinausgehen bzw. Datenübermittlungen in die CWA-Infrastruktur erfolgen, für die die PoCs verantwortlich.	Ja	2	4	4	1	1	1	1	4	4	4	8	RM, DM, VT, IG, IV, TR, ZB	Vertragliche Regelungen mit PoC, Leistungsbeschreibungen für Portal-Anbindung und Antigen-Schnelltest-Schnittstelle	akzeptabel mit Evaluation
R8- Behörden	Fehlende Rechtsgrundlage für Datenübermittlung von den Testcentren in die CWA-Infrastruktur		Ja	2	4	4	4	1	1	1	4	4	4	8	RM, DM, VT, IG, IV, TR, ZB	Einwilligung wird für diese Funktionen / Verarbeitungstätigkeiten durch die PoC eingeholt (siehe Designentscheidungen c. D-2-2c)	akzeptael mit Evaluation
R1-CWA-Nutzer	Datenverarbeitungen nach widerrufener Einwilligung in die Datenübermittlung von den Testcentren in die CWA-Infrastruktur	Ein Nutzer kann sich zu jedem Zeitpunkt dazu entscheiden die Einwilligung zum Teilen der Daten zu widerrufen. Da es nach der Datenübertragung der Daten von den Poc an die CWA (Test Result 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 a.) (D-2.1-2 (Install), D-2.1-6 (Upload) + Designentscheidung D-3.1-1 + Designentscheidung a.) (Widerruf) D-3.1-8	akzeptabel
R4- Testcenter	Unwirksame Einwilligung durch fehlende Freiwilligkeit ("erzwungene Einwilligung") /erzwungene Freiwilligkeit		Ja	1	4	4	1	1	1	1	4	1	4	4	DM, VT, IV, ZB	Vertragliche Regelungen mit PoC, Vorsehen einer Einwilligungslösung (Check-Box) für Portallösung, Muster für Drittanbieter (Antigen-Schnelltest-Schnittstelle), Hinweis auf Freiwilligkeit im Rahmen von Datenschutzinfomationen PoC und in der CWA-App	akzeptabel
R1-CWA-Nutzer	Unwirksame Einwilligung aufgrund fehlender / fehlerhafter ausdrückliche Einwilligungserklärung (technischer Einwilligungs-Akt)	Die Einholung der Einwilligung erfolgt durch die PoC, daher mittels eines Portals oder durch Schnelltest-Drittanbieter, mittels deren Testcenter-Software bzw. auf anderem Wege.	Ja	1	4	4	1	1	1	1	4	4	4	4	DM, VT, IV, TR, ZB	siehe Designentscheidungen D-2-2c	akzeptabel
R1-CWA-Nutzer	Unwirksame Einwilligung aufgrund fehlender Information über Umfang und Folgen der Schnelltest-Anbindung und Nachweisfunktion + Schnelltest-Profil (CWA-Version 2.2)	Lücken in der Information über die Datenverarbeitung könnten zur Unwirksamkeit der Einwilligungserklärung insgesamt führen. Nutzer könnten durch fehlende Informationen die Schnelltestanzeigen gegenüber Dritten offenbaren, weil ihnen nicht bewusst ist, dass sie dazu nicht verpflichtet sind. Vertraulichkeit und Transparenz sind vor allem gefährdet.	Ja	2	4	4	1	1	1	1	4	4	4	8	DM, VT, IV, TR, ZB	Datenschutzinformationen liegt vor, siehe Designentscheidung c. D-4-4	akzeptabel mit Evaluation u ggf. Anpassung Datenschutzerklärung
R1-CWA-Nutzer	Unwirksame Einwilligung aufgrund Nichterreichbarkeit der notwendigen Informationen (sprachliche Barrieren, fehlendes Technikverständnis)	Risiko umfasst auch die unwirksame Einwilligung in Erstellung des Schnelltest-Profils (CWA Version 2.2)	Ja	2	4	4	1	1	1	1	4	4	4	8	DM, VT, 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 in den Testcentren ihre Einwilligung erteilen, ohne dass diese etwa die Datenübermittlung an die CWA ab- und einschätzen könnten. Dritte könnten sich negative Testergebnisse auch von Minderjährigen anzeigen lassen (etwa in Schule, Verein).	Ja	3	3	3	3	1	1	1	3	3	3	9	DM, VT,IG, IV, TR, ZB	Siehe Designentscheidungen a. D-3.1-2, eine Altersabfrage erfolgt im Rahmen der CWA nicht; die Auswertemöglichkeiten des RKI und Rückschluss auf Minderjährige sind nicht möglich // Eine Altersabfrage erfolgt durch die PoC. Es ergeht der Hinweis, dass Minderjährige, die Nutzung der CWA mit ihren	bedingt akzeptabel
R4- Betreiber Server (T)	Abhängigkeiten von Dienstleistern/ Software- und Firmware Hersteller (Ausfall externer Dienstleistern)	Bei einem Ausfall des Dienstleisters könnten sowohl die PoC als auch die CWA nicht mehr betrieben werden. Der Dienst (Schnelltest-Anbindung und Anzeigefunktion) wäre nicht verfügbar und die Nutzung wäre eingeschränkt.	Ja	2	0	0	0	2	0	2	2	3	2	6	VF, TR	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen D-11-1)	akzeptabel, mit Evaluation
R4- Testcenter	Fehlende/ unzureichende vertragliche Regelungen mit Point-of-Care (PoC)	Soweit die Systemintegration der PoC nicht rechtmäßig, zweckgebunden, datenschutzkonform und IT-sicher, entstehen Risiken für CWA-Nutzer.	Ja	2	3	3	3	3	0	2	2	3	3	6	ZB , TR	Partnerverträge und Leistungsbeschreibung mit PoC, siehe Designentscheidungen c.) D-3.1-2	akzeptabel, mit Evaluation
R4- Betreiber Server (T)	Fehlende unzureichende vertragliche Regelungen mit Dienstleistern (Auftragsverarbeitung/ Vertrag zur gemeinsamen Verantwortung) - mit T/SAP	Fehlende Vertragsanpassungen mit T/SAP könnten zu Lücken in der Gewährleistung der Sicherheit der Verarbeitung führen, da durch die Anbindung der Testcenter personenbezogene Daten als Klardaten verarbeitet werden, obwohl die bisherigen Verträge/ TOM lediglich von der Verarbeitung von Pseudonymen ausgehen.	Ja	1	3	3	3	3	0	2	2	3	3	3	ZB, TR	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen a. D-11-1)	akzeptabel
R4- Betreiber Server (T)	Identifizierung der Nutzer (direkte Identifizierung) auf CWA-Komponenten	Nicht-pseudonymisierte personenbezogene Daten liegen nur auf dem Schnelltest-Poc-Backend. In die CWA-Infrastruktur (zu Testresult-Server) werden nur das Testergebnis und Hash (CWA Test ID) übertragen.	Ja	1	1	4	1	1	1	1	1	1	1	4	DM	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen a. D-11-1)	akzeptabel
R4- Testcenter	Erhebung und Speicherung nicht-notwendiger Daten, inklusive Nutzer- und Metadaten durch Testcenter	Durch die Testcenter könnten Nutzer- und Metadaten gespeichert werden, die zur Identifikation von CWA-Nutzern/ PoC-Mitarbeitern genutzt werden könnten.	Ja	3	4	4	0	0	0	0	2	0	4	12	DM, IG, ZB	Die Einwilligung der CWA - Nutzer ist erforderlich. Datenverarbeitung in Verantwortung der PoCs; Leistungsbeschreibungen & zusätzliche Bedingungen für PoC vorhanden.	bedingt akzeptabel
R4- Betreiber Server (T)	Erhebung und Speicherung nicht-notwendiger Daten, inkl. Metadaten (TK-Daten) durch Betreiber CWA (Backend)	Durch die Betreiber der CWA könnten - über die Schnittstellen zu den PoC - Nutzer- und Metadaten gespeichert werden, die zur Indentifikation von CWA-Nutzern oder PoC-Mitarbeitern genutzt werden könnten.	Ja	2	4	4	0	0	0	0	2	0	4	8	DM, IG, ZB	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen a.) D-11-1) + Designentscheidungen c (Die pseudonymen Daten werden (auch durch die PoC) in die CWA verschlüsselt übertragen und verschlüsselt gespeichert).	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 mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen D-11-1)	akzeptabel
	Verarbeitung wider Treu und Glauben																

Datenschutzfolgenabschätzung (DSFA)
VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für

			Risikobewertung														
					Schadensausmaß											
Risiko-Quelle	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	Restrisiko
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	3	3	ZB, DSMS/ ISMS	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen D-11-1)	akzeptabel
R4- Testcenter	Auftreten von Sicherheitslücken und Datenschutzvorfällen bei den Testcentern (Vertrauensverlust der Bevölkerung in Vertrauenswürdigkeit der CWA und IT-Infrastruktur)	Die Umsetzung der Point-of-Care (PoC) Lösung liegt nicht im Verantwortungs-/Zuständigkeitsbereich der CWA Lösung. Aus diesem Grund gibt es auch keine Möglichkeit die Sicherheits-/Datenschutzkonzepte der PoC Lösung zu prüfen und/oder zu validieren. Daher könnten „Datenleck" Risiken durch das CWA Team nicht mitigiert werden. Dies gilt umso mehr, als Drittanbieter (mittels API) an das System angeschlossen werden können.	Ja	3	1	3	3	1	1	1	1	1	3	9	VT, IG, ZB, DSMS/ ISMS	Die Umsetzung der Security-/DPP-/Compliance Vorgaben für die PoC-Lösung sollte externe geprüft und bewertet werden, um Probleme im Kontext der CWA-Lösung vermeiden zu können. Verträge (Leistungsbeschreibungen) mit den PoC-werden	akzeptabel mit Evaluation
	Für die Betroffenen intransparente Verarbeitung																
R8- Behörden	Unvollständige, unverständliche Datenschutzinformationen für die weiteren Funktionalitäten der CWA (Schnelltest-Anbindung + Anzeige)		Ja	1	2	2	2	0	0	0	3	4	4	4	TR, ZB	Datenschutzinformation vorhanden. Siehe Designentscheidungen c.) D-4-4	akzeptabel
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	Datenschutzinformationen und Informationen auf GitHub und AV-Vertrag mit SAP/ T	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 und AV-Vertrag mit SAP/ T	akzeptabel mit Evaluation
	Unbefugte Offenlegung von und Zugang zu Daten																
R4- Betreiber Server (T)	Re-Identifizierung durch Korrelation der erhobenen Daten (+ Publikation)	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 aktive nutzen) Rückschlüsse auf einzelne Nutzer (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	Ja	2	2	2	1	1	1	1	1	1	2	4	DM, VT, ZB	AV-Verträge mit DL, inkl. TOM , Designentscheidungen a. D-11-1	akzeptabel
R4- Betreiber Server (T)	Offenlegung von personenbezogenen Daten von Mitarbeiter der Schnelltestzentren	Personenbezogenen Daten von PoC Mitarbeiter werden bei der Schnelltest-Portal-Lösung in einem IAM Server im Backend gespeichert. Bei mangelhafter Konfiguration der Server könnten diese Informationen für Dritte oder für anderen Mandanten sichtbar werden. Ein Risiko besteht auch während der Entwicklung, dass User-Daten des Testers für Support-Mitarbeiter sichtbar sind, die dies nicht zur Aufgabenerledigung brauchen.	Ja	2	1	2	1	1	1	1	1	1	2	4	VT, ZB	1, Mandantentrennung im Backend, Berechtigungskonzept und Monitoring /Alerting // Mit Anbindung des UC wird ein Level Switch eingebaut, der es nur den zuständigen Mitarbeitern des	akzeptabel
R4- Testcenter	Unbefugter Zugriff auf Testberichte in PoC (Ausnutzung der Schnittstelle des PoC)	Im PoC gibt es eine Schnittstelle, die es erlaubt, Testberichte mit allen persönlichen Daten von Getesteten, etwa des vergangenen Tages zu ziehen, um Meldepflichten an das Gesundheitsamt zu erfüllen. Diese Schnittstelle könnte von Mitarbeitern des PoC (über die Aufgabenerfüllung hinaus) missbraucht und die Vertraulichkeit verletzt werden.	Ja	3	1	3	1	1	1	1	3	3	3	9	VT, IV, TR, ZB	Gewährleistung der Vertraulichkeit durch PoC (Verantwortung der PoC). Einsatz von Rollen- und Berechtigungskonzepten und technische und organisatorische Zugriffsbeschränkungen.	akzeptabel mit Evaltuation
R2- Hacker	Re-Identifizierung von CWA-Nutzern durch unbefugten Zugriff (Auslesen des QR-Codes bei der personalisierten Übertragung von Schnelltestergebnissen durch Dritte im PoC) oder Erfassung Schnelltest-Profil	unbefugten Dritten gegenüber offenbart werden, wenn sie Zugriff auf den QR-Code erlangen. Dies könnte im PoC erfolgen, wenn die Vertraulichkeit nicht gewahrt wird, etwa indem QR-Codes von Dritten oder CWA-Nutzer ausgedruckt und nicht entsorgt werden oder Dritte die Möglichkeit erlangen, nicht für sie bestimmte QR-Codes zu scannen. Ab CWA v2.2: Beim Warten an einer Teststation könnte es passieren, dass Schnelltest-Profile von Dritten erfasst werden (z.B.	Ja	2	1	3	1	1	1	1	3	3	3	6	VT, TR, IV, ZB	Maßnahmen zur IT-Sicherheit der Verarbeitung durch PoC, Sensibilisierung der PoC-Mitarbeiter	akzeptabel mit Evaluation
R2- Hacker	Re-Identifizierung von CWA-Nutzern durch unbefugten Zugriff (Auslesen des QR-Codes bei der personalisierten Übertragung von Schnelltestergebnissen durch Dritte im CWA-Backend)	In den Fällen der personalisierten Übertragung des Schnelltestergebnisses wird nicht der QR-Code und nicht die personenbezogenen Daten an das CWA-Backend weitergeleitet, sondern lediglich die Hash(CWA Test ID). Ein "De-Hashing" mit der Folge der Re-Identifizierung von CWA-Nutzern ist nicht ausgeschlossen, aber nur unter extrem hohen Aufwand möglich.	Ja	1	1	3	1	1	1	1	3	3	3	3	VT, TR, IV, ZB	Einsatz von Hash-Funktionen. Siehe Designentscheidung a.) B-2-1 und Designentscheidungen c.) 5-1-8	akzeptabel
R1-CWA-Nutzer	Re-Identifizierung von CWA-Nutzern/ Offenlegung von Gesundheitsdaten durch unbefugten Zugriff (Auslesen der QR-Code Anzeige bei der personalisierten Übertragung von Schnelltestergebnissen oder Mitlesen der Anzeige von Zertifikatsarten auf dem Smartphone - "Shoulder-Surfing")	Schnelltestergebnissen in den QR-Code geschrieben werden, auf dem Smartphone lesbar. Bei der Anzeige auf dem Smartphone könnten diese gegenüber unbefugten Dritten offenbart werden, die Zugriff auf das Smartphone oder Einblick in die Anzeige erhalten. Ebenso kann bei Anzeige von Impf-, Test- und Genesenenzertifikaten durch nahestehende Personen unbefugt Einsicht in den Impf- oder Teststatus einer Person genommen werden bzw. über	Ja	2	1	3	1	1	1	1	3	3	3	6	VT, TR, IV, ZB	Anzeigen der CWA-App zu erlauben. Nach dem Scannen des QR-Codes im PoC werden die Daten auf dem Smartphone (verschlüsselt in der Sandbox) gespeichert. Mit der Version 2.5	akzeptabel mit Evaluation
R9 - DCC - Verifier	Unbefugter Zugriff auf Gesundheitsdaten im Zusammenhang mit der Prüfung von Impf-, Test-, Genesenenzertifikaten	Bei Vorlage von Impf-, Test- und Genesenenzertifikaten zur Prüfung nach Version 2.4 könnten sowohl der Prüfer als auch umstehende Personen unbefugt Kenntnis vom Impf- oder Teststatus des CWA-Nutzers erlangen bzw. über frühere Erkrankungen, durch Anzeige der Zertifikatsart zusammen mit dem QR-Code. Daraus könnten Diskriminierungen folgen.	Ja	3	3	3	1	1	1	1	3	3	3	9	DM, VT, TR, IV, ZB	zur Prüfung vorzulegen, hat die prüfende Stelle Vorkehrungen zu treffen, um den CWA-Nutzern die vertrauliche Nutzung zu ermöglichen (Sichtschutzmaßnahmen, Mindestabstand zu	akzeptabel mit Evaluation
R4- Testcenter	Manipulation von QR-Code Anzeige (Attributen von Testergebnissen) und Kollision von CWA Test ID infolge zu niedriger Entropie von kryptographischen Funktionen	und deren Ergebnis in das QR Code einkodiert. Der Hash wird kalkuliert aus einer bestimmten Zeichenkette. Hier werden 2 Parameter von der PoC erzeugt, nämlich „testid" und „salt". Der Salt wird kryptographisch generiert, mithilfe vorhandenen Krypto-Bibliotheken und für die TestID werden UUIDv4 empfohlen. Selbst in Situationen wo der „Salt" Wert immer gleich ist (z.B. wenn kryptographischen Funktionen immer mit dem gleichen „Seed" Wert initialisiert werden)	Ja	1	1	1	3	3	1	3	1	1	3	3	IG, VF, ZB	anders sein werden, selbst bei eine Salt von NULL wird genug Entropie vorhanden sein um Kollisionen zu vermeiden. Replay-Attacke werden durch die Gültigkeitsdauer der Tests erschwert.	akzeptabel
R2- Hacker	Zugang/ Zugriff auf (Gesundheits-) Daten auf CWA Komponenten (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 a. D-11-1 // Verschlüsselung der Daten beim Transport und in Storage, Sicherheitsprozesse im CWA - Bankend Verantwortlichkeit für PoC-Backend bei PoC	akzeptabel mit Evaluation
R4- Betreiber Server (T)	Unberechtigter Administratorenzugriff auf Daten auf CWA 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 a. D-11-1	akzeptabel
R4- Betreiber Server (T)	Unberechtigter Administratorenzugriff auf Daten auf Poc-Server der Testcentren und Korrelation mit Daten auf CWA Servern		Ja	1	0	4	1	1	1	1	4	4	4	4	VT, IV, TR, ZB	Verantwortung der PoC, Verträge, Leistungsbeschreibung und zusätzliche Bedingungen zur Gewährleistung von Datenschutz und Datensicherheit werden abgeschlossen.	akzeptabel
R4- Betreiber Server (T)	Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts-, Zugangs- und Zugriffskontrolle …(TOM) für die CWA Komponenten und die Mitarbeiter des Betreibers		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
R4- Testcenter	Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts-, Zugangs- und Zugriffskontrolle … inkl. Wiederherstellungsprozesse für Zugangsdaten (TOM) für die PoC-Komponenten/ PoC-Mitarbeiter	Mitarbeiter mit einem gültigen Konto und Multi-Faktor Authentisierung könnten Tests verwalten und durchführen, etwa auch remote, ohne ausreichende Beschränkung z.B. auf Netzwerkebene und Kontrolle durch Verantwortliche im Testzentrum vor Ort.	Ja	1	1	3	3	1	1	1	1	1	3	3	VT, IG, ZB	zwingend 2-Faktoren (Empfehlung an die PoC: einer örtlich beschränkt), Logs der Aktivitäten der PoC Mitarbeiter dem Admin Nutzer zur Verfügung stellen. Die PoCs werden einzeln mit	akzeptabel mit Evaluation
R6 - Krimineller	Unbefugter Zugang zu/ Missbrauch der Nutzungsdaten/ Schnelltest-Profil durch "Malicious Schnelltest - Station"	Schnelltest-Stelle zu vereinfachen und zu beschleunigen, sofern diese über die entsprechenden Mittel (z.B. QR-Code Scanner) verfügt. Die Daten aus dem Schnelltest-Profil sind mgl.weise für bestimmte Personen/ Personengruppen von einem hohen Interesse. So könnte es z.B. passieren, dass diese über eine „malicious" Schnelltest-Stelle für kurze Zeit Schnelltest kostenlos für CWA-Nutzer anbietet, um die Schnelltest-Profil-Daten von CWA-Nutzern einzuscannen	Ja	3	3	3	1	1	1	1	3	3	3	9	DM, VT, Z, IV, T, ZB	Anbindung von PoC erfordert Vertragsabschluss //	akzeptabel mit Evaltuation
R1-CWA-Nutzer	Verbreitung von Impfzertifikaten/ Testzertifikaten/ Genesenenzertifikaten über Social Media	die Gefahr, dass der QR-Code des Impf- ,Test- oder Genesenennachweises (in der CWA App) auf Social Media oder anderweitig durch den CWA-Nutzer oder einer anderen Person publiziert wird (unabsichtlich/absichtlich). Sollte ein CWA-Nutzer seinem Impf-, Test-, Genesenennachweis mit anderen Personen teilen, können diese den QR-Code z.B. in ihrer eigenen CWA App einscannen und so an die persönlichen Informationen des CWA-Nutzers gelangen. Dies kann für	Ja	3	3	3	2	1	1	1	1	1	1	9	DM, VT	Aufklärung, dass nur Wallet-Funktion; Missbrauch nur dann möglich, wenn Dritter seiner Prüfpflicht nicht nachkommt und zweckwidrig als Nachweis verwenden lässt. Designentscheidungen c) D-2-4	akzeptabel mit Evalution
	Verweigerung der Betroffenenrechte (Betrachtung der Unterstützung durch SAP/T)																
R4 - Softwareentwickler / SAP	Fehlende Verfügbarkeit des Testzertifikates nach Verlust	Berechtigte könnten ein auf ihrer CWA-App nicht mehr verfügbares Testzertifikat innerhalb des Gültigkeitszeitraums nicht erneut abrufen. Damit könnten ggf. Rechte und Freiheiten nicht mehr ausgeübt werden.	Ja	2	1	1	1	3	1	3	1	1	1	6	VT, BL	Aktuell kann das Testzertifikat durch di CWA-App nur einmal abgerufen werden. Diese haben nur eine begrenzte Gültigkeit, des weiteren bestehen Alternativen für Betroffene (eigener Ausdruck // CovPass-App)	akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	Fehlende Umsetzung der Widerrufsmöglichkeit, speziell für Schnelltest-Anbindung + Anzeige		Ja	3	2	2	2	1	1	1	2	2	2	6	IV, T, ZB	Widerruf der Einwilligung per Einstellung möglich, Designentscheidung aD-2-2c, auf dem Servern keine Herstellung Personenbezug zur Erfüllung Betroffenenrechte, Designentscheidung a 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 a D-8-1	akzeptabel

Datenschutzfolgenabschätzung (DSFA)

VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für

				Risikobewertung														
					Schadensausmaß													
Risiko-Quelle	**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**	**Restrisiko**
R4 - Softwareentwickler / SAP	Nichtbeachtung von Löschungsersuchen, 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 a. 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 a. D-8-1	akzeptabel
R4- Betreiber Server (T)	Fehlende/ unzureichende Löschung der Daten auf den CWA Servern bei Löschersuchen		Ja	3	3	3	0	0	0	0	3	3	3	9	DM, VT, IV, TR, ZB	Siehe Designentscheidung a, D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23.	akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	Fehlende/ unzureichende Löschung der Daten bei "In-App-Reset" (nur Android)	Im Falle eines „In-App Reset's" werden möglicherweise nicht alle persönlichen Daten, die im Rahmen der App Nutzung vom Android Betriebssystem erstellt werden, vollständig gelöscht. Ein Angreifer könnte hierauf unberechtigt Zugriff erhalten, wenn er in der Lage wäre, das Android-Gerät zu rooten.	Ja	2	3	3								6		Um eine vollständige Löschung aller Daten der CWA (und der von Android Betriebssystem erstellen Log's sicherzustellen, kann/muss die App de-installiert werden. (Beschreibung in DSK CWA App v2.2, Kap. 7.4.17)	akzeptabel mit Evaluation
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-Live Verhaltens der App (Designentscheidung a. D-9-9)	akzeptabel
R8- Behörden	Fehlende Invalidierung-/ Revoke-Funktion für Schnelltestergebnisse	dass ein „positives" Corona-Schnelltest Ergebnis einer Überprüfung mittels PCR Test nicht standhält (False-Positive Meldung). In einem solchen Fall müsste das Schnelltestergebnis zurückgezogen werden können, um mögliche Nachteile für den CWA Nutzer ausschließen zu können. Wenn Warnungen erfolgten, die auf einem False-Positive-Schnelltest basierten, entstehen auch durch die Gewarnten Nachteile, die sich ggf. freiwillig in Quarantäne begaben.	Ja	2	2	2	2	0	0	0	3	0	3	6	IV, ZB	Trennung von PCR-Schnelltestergebnisanzeigen inkl. der jeweiligen Berücksichtigung der Chronologie der Testzeitpunkte, um so „alte" Testergebnisse durch „neuere " überschreiben zu können und so eine korrekte und konsistente Anzeige zu gewährleisten	akzeptabel mit Evaluation
R1-CWA-Nutzer	Verweigerung der Betroffenenrechte bei Nutzung der Familienfunktion	App zu speichern. Eine Löschung erfolgt nicht automatisch, sondern muss manuell vom CWA - Nutzer initiiert werden. Für Familienmitglieder, deren Zertifikat verwaltet wird, besteht das Risiko, dass die Zertifikate nicht gelöscht werden, selbst wenn dies von diesem gewünscht wird. Es sind auch Fälle denkbar, in denen CWA-Nutzer die Funktion nicht nur für Familienangehörige nutzen, sondern darüber hinaus, etwa im Rahmen einer Reise oder Klassenfahrt.	Ja	2	2	2	1	1	1	1	2	2	2	4	DM, VT, TR, IV, ZB	siehe Risikomatrix VT_1_2_4, Zeile 104 (Verweigerung von Betroffenenrechten durch CWA-Nutzer im Rahmen KTB), keine automatische Löschung (siehe Designentscheidung D-9-5e) oder andere technische Mitigationsmaßnahmen	akzeptabel
	Verwendung der Daten zu inkompatiblen Zwecken																
R8- Behörden	De-Anonymisierung/ De-Pseudonymisierung von Nutzern anhand von optionalen Lokalisierungsdaten		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
R1-CWA-Nutzer	Nutzung der negativen Schnelltestergebnisse für Verifikation oder als "Eintrittskarte"	der Nutzer als negativ oder positiv getestet. Die Funktion als "Eintrittskarte" könnte trotzdem (ohne Rechtsgrundlage) von Dritten angefragt werden. Aktuell ist es nicht möglich, den angezeigten Schnelltest zu verifizieren. Ein Dritter könnte nur die Anzeige auf dem Smartphone des CWA - Nutzers sehen. Zwar zeigt die eingebaute und im Sekundentakt zurückzählende Uhr an, dass nicht nur ein Bild vorgezeigt wird, aber die Fälschung von Negativanzeigen	Ja	3	4	4	0	0	0	0	1	1	4	12	VT, IG, ZB	Information der CWA - Nutzer, dass die Funktionalität nur für den privaten Gebrauch und keine Verpflichtung Dritten vorzuzeigen. Designentscheidungen c D-3.2-2	bedingt akzeptabel
R4- Testcenter	Zweckwidrige Speicherung oder (Weiter-)nutzung des Schnelltest-Profils in den PoC	ermöglicht es dem Anbieter in einem großen Umfang personenbezogene Daten zu erfassen und zu verarbeiten. Es kann daher nicht ausgeschlossen werden, dass die von der CWA App über den CWA-Nutzer bereitgestellten Daten nicht auch für andere Zwecke weiterverwendet werden, etwa auch per Exportfunktion eine Übermittlung an Gesundheitsamt oder Dritte.	Ja	1	3	4	1	1	1	1	3	3	3	4	DM, VT, IV, T, ZB	Verträge mit PoC bestimmen den Umfang der DV im Zusammenhang mit CWA // PoC erheben die Daten aufgrund eigener Rechtsgrundlage, wenn Schnelltest-Profil nicht genutzt wird.	akzeptabel
R1-CWA-Nutzer	Teilung Schnelltest-Profil über Social Media	Ein CWA-Nutzer könnte ein Foto mit dem Schnelltest-Profil oder das Schnelltest-Profil selbst auf Social Media stellen. Dieses könnte dann von Dritten ausgewertet, verkauft werden.	Ja	2	2	4	1	1	1	1	2	2	2	8	VT	keine technischen Mitigationsmaßnahmen möglich; Verantwortung der CWA - Nutzer // Aufklärung und öffentliche Infomationskampagnen des BMG	akzeptabel mit Evaluation
R1-CWA-Nutzer	Teilung negatives Testergebnis über Social Media	Ein CWA-Nutzer könnte ein Foto mit dem negativen Testergebnis oder das Testergebnis selbst auf Social Media stellen. Dieses könnte dann von Dritten ausgewertet, verkauft werden.	Ja	2	2	4	1	1	1	1	2	2	2	8	VT	Auf der Anzeige auf Android-Geräten wird ein "Counter" angezeigt, womit ein Testnachweis durch Screen-Shot erschwert wird. Darüber hinaus keine technischen Mitigationsmaßnahmen möglich; Verantwortung der CWA - Nutzer // Aufklärung und öffentliche Informationskampagnen des BMG	akzeptabel mit Evaluation
R5-Arbeitgeber, Versicherungen	CWA wird als Nachweis-App für Impf-/ Test- und Genesenenzertifikate angesehen, nicht als Wallet App	ermöglicht diese es dem CWA-Nutzer die jeweiligen Nachweise anzuzeigen (QR-Code + Details auf dem entsprechenden Screen). Die CWA App fungiert als Wallet App. Daher findet aktuell keine Prüfung statt, ob es sich um einen gültigen Impfnachweis handelt oder nicht. Eine Überprüfung des Impfnachweises auf Gültigkeit erfolgt über eine dafür freigebende Anwendung zur Verifikation von Impfnachweisen. Wird daher auf die Überprüfung verzichtet, kann	Ja	3	1	1	3	1	1	1	1	1	3	9	VT, ZB	Aufklärung, dass nur Wallet-Funktion; Missbrauch nur dann möglich, wenn Dritter seiner Prüfpflicht nicht nachkommt und zweckwidrig als Nachweis verwenden lässt. Designentscheidungen c) D-2-4 und D-2-5	akzeptabel mit Evaluation
R2- Hacker	Missbrauch/ Sammlung von pD mittels Anzeige von Impf-, Test-, Genesenenzertifikaten in der CWA App	wurde bzw. sein Testzertifikat, dass er getestet wurde, könnte diese Person Infomationen (wie z.B. das Impfdatum oder den Impfstoff oder den Teststatus) über den CWA-Nutzer erhalten. Auf Grund der in Deutschland vorgebenden Impf-Priorisierung gemäß der Impfgruppen ist es unter Umständen möglich, Rückschlüsse auf die Gruppenzugehörigkeit und/oder die Berufszugehörigkeit des CWA-Nutzers zu ziehen. Auch sind Diskriminierungen	Ja	3	3	3	1	1	1	1	1	1	3	9	DM, VT, ZB	Funktion ist freiwillig. Aufklärung, dass nur Wallet-Funktion verwenden lässt. Designentscheidungen c) D-2-4 und D-2-5	akzeptabel mit Evaluation
R6 - Krimineller	Malicious Verifier App	Echtheit des Zertifikat überprüfen kann. Diese App kann zur Validierung des Testzertifikates genutzt werden. Es ist daher vorstellbar, dass ein Angreifer sich selber eine Validierungs App baut und alle eingescannten QR-Code als valide markiert. Dadurch wäre es möglich beliebigen Personen auch ohne valides Testzertifikat Zugang zu einem Ort oder Veranstaltung zu gewähren. Zudem wäre es auch möglich, die modifizierte Validierungs App dazu zu nutzen, um die	Ja	3	3	3	3	1	3	1	3	3	3	9	DM, VT, IG, IV, TR, ZB	Sensibilsierung der CWA-Nutzer. Keine Mitigation im Rahmen der CWA möglich (Verifier out of scope).	akzeptabel mit Evaluation
R1-CWA-Nutzer	Zweckwidrige Verwendung von Daten Dritter im Rahmen der Funktion Familienzertifikate	App zu speichern. Zweck ist es, dem CWA-Nutzer hiermit das Halten von Zertifikaten von Familienmitgliedern zu ermöglichen, um die damit zusammenhängenden Rechte und Freiheiten für die gesamte Familie ermöglichen zu können. Die Funktion könnte für andere Zwecke missbraucht werden, etwa durch Reiseleiter, die die Zertifikate von Reisenden einscannen und dann Impfregister o.ä. erstellen.	Ja	2	3	2	1	1	1	1	3	2	3	6	DM, IV, ZB	Hinweis an CWA-Nutzer erfolgt, dass dies eine Funktion für Familienzertifikate.	akzeptabel mit Evaluation
	Verarbeitung nicht richtiger Daten																
R4- Testcenter	Falsche Aufnahme des Namens	Durch die Vielfalt von Kulturen, Sprachen ist es möglich, dass der Namen falsch aufgenommen wird, eine falsche Zuordnung erfolgt und die Schnelltestanzeige nicht mit dem richtigen Namen des CWA-Nutzers erfolgt.	Ja	1	1	1	2	1	1	1	1	1	2	2	IG, ZB	Sensibilisierung der Mitarbeiter, Verifikation mit einem offiziellen Personaldokument	akzeptabel
R4- Testcenter	Unbewusste/ fahrlässige falsche Zuordnung eines "negativen Schnelltestergebnisses" zu einer mit Corona infizierten Person oder falsche Zuordnung eines "positiven Schnelltestergebnisses" zu einer nicht-infizierten Person (Vertauschte Test-ID) durch PoC	falsch zugeordnet werden, kann es passieren, dass einer an Corona infizierten Person fälschlicherweise ein "negatives Schnelltestergebnis" an die CWA - App übermittelt und dort angezeigt wird. Sofern die GUID's/Proben IDs zur Zuordnung von Tests zu getesteten Personen vertauscht oder falsch zugeordnet werden sollten, kann nicht ausgeschlossen werden, dass Testergebnisse an die „falschen" Personen übermittelt werden. Sofern die	Ja	1	1	3	3	1	1	1	1	1	2	3	VT, IG; ZB	Schulung des Personals, Festlegung strikter/überprüfbarer Validierungsprozesse, Planung geeigneter TOM's, Verwendung von ausgedruckten Probenetiketten zur Kennzeichnung der Proben	akzeptabel
R4- Testcenter	Unbewusste/ fahrlässige falsche Zuordnung eines "negativen Schnelltestergebnisses" zu einer mit Corona infizierten Person oder falsche Zuordnung eines "positiven Schnelltestergebnisses" zu einer nicht-infizierten Person (Vertauschte Test-ID) durch Drittanbieter (DM, Testlabor)	falsch zugeordnet werden, kann es passieren, dass einer an Corona infizierten Person fälschlicherweise ein "negatives Schnelltestergebnis" an die CWA - App übermittelt und dort angezeigt wird. Sofern die GUID's/Proben IDs zur Zuordnung von Tests zu getesteten Personen vertauscht oder falsch zugeordnet werden sollten, kann nicht ausgeschlossen werden, dass Testergebnisse an die „falschen" Personen übermittelt werden. Sofern die	Ja	2	1	3	3	1	1	1	1	1	2	6	VT, IG, ZB	Schulung des Personals, Festlegung strikter/überprüfbarer Validierungsprozesse, Planung geeigneter TOM's, Verwendung von ausgedruckten Probenetiketten zur Kennzeichnung der Proben	akzeptabel mit Evaluation
R4- Testcenter	Bewusst falsche Zuordnung eines Testergebnisses zu einer anderen Person durch das Personal im Testcentrum	Sofern ein negatives Schnelltestergebnis für eine getestete Person zu Vergünstigungen führt, könnte diese Person andere Personen die „sicher" nicht infiziert sind, zum Test schicken und deren „negatives" Testergebnis für sich selber – z.B. inkl. Anzeige des Ergebnisses in der App – nutzen, um z.B. Zugang zu einer Einkaufsmöglichkeit zu bekommen, obwohl möglicherweise eine Corona Infektion vorliegt.	Ja	3	1	3	3	1	1	1	1	1	3	9	VT, IG, ZB	Festlegung strikter/überprüfbarer Validierungsprozesse, Planung geeigneter TOM's/ Prüfung des Ausweises der getesteten Person	akzeptabel mit Evaluation
R4- Testcenter	False Positive - Schnelltests	Auch wenn sich die Zuverlässigkeit von Schnelltests verbessert hat, so kann dennoch nicht ausgeschlossen werden, dass ein „positives" Corona-Schnelltest fälschlicherweise zustande gekommen ist (falsche Testdurchführung/…). Dadurch könnten sich Nutzer grundlos in „Selbstquarantäne" begeben.	Ja	2	1	3	3	1	1	1	1	1	3	6	VT, IG, ZB	Konkrete Beschreibung der Limitationen/ begrenzten Aussagekraft der Schnelltestergebnisse und Darlegung konkreter nächster Schritte, um zu prüfen ob es sich eine ein „falsches positives Schnelltestergebnis" handelt oder ob tatsächlich eine Corona-Infektion vorliegt. Idealerweise würden	akzeptabel mit Evaluation
R1-CWA-Nutzer	Verschicken bewusst falscher Warnungen an andere CWA - Nutzer	Sofern es einem Nutzer gelingen sollte falsche „positive" Schelltestergebnisse zu erhalten (z.B. durch die Bereitstellung von Proben positiv auf Corona getesteter Personen), könnte er andere CWA Nutzer fälschlicherweise vor mögliche Risiken warnen.	Ja	3	1	3	3	1	1	1	1	1	3	9	VT, IG, ZB	Sicherstellung entsprechender Test-Vorgehensweisen in PoC und Festlegung entsprechender TOM's um auch technische Missbrauchsoptionen zu vermeiden.	akzeptabel mit Evaluation
R6 - Krimineller	Verkauf "negativer" Schnelltestergebnisse	Sofern ein negatives Schnelltestergebnis für eine getestete Person zu Vergünstigungen führt, könnte Interesse bestehen – gegen entsprechende Bezahlung" negativer Testergebnisse „on-demand" anzubieten und zu verkaufen.	Ja	3	1	3	3	1	1	1	1	1	3	9	VT, IG, ZB	Festlegung strikter/überprüfbarer Validierungsprozesse, Planung geeigneter TOM's/ Prüfung des Ausweises der getesteten Person	akzeptabel mit Evaluation
R6 - Krimineller	Ausnutzung der Schnelltests durch Bevölkerungsgruppen	ist vorstellbar, dass ein Anteil dieser Bevölkerung möglicherweise Zugang zu Schnelltest-Zentren haben, wo Sie sich und anderen der Bevölkerungsgruppe negativ/positive Schnelltest-Ergebnisse ausstellen könnten. Diese Ausgestellten Testergebnisse würde dann auch möglicherweise in der CWA App landen. •Sollte der Schnelltest positiv sein, könnte dieser dazu verwendet werden, um andere CWA-Nutzer damit zu warnen.	Ja	3	1	3	3	1	1	1	1	1	2	9	VT, IG, ZB	Festlegung strikter/überprüfbarer Validierungsprozesse, Planung geeigneter TOM's/ Prüfung des Ausweises der getesteten Person	akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA)

VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für

			Risikobewertung														
					Schadensausmaß												
Risiko-Quelle	**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**	**Restrisiko**
R1-CWA-Nutzer	Ausnutzung der Fehleranfälligkeit der Schnelltests (Durchführung von mehreren Schnelltests, bis ein Test negativ ist)	dass ein „positives" Corona-Schnelltest Ergebnis durch falsche Anwendung des Tests oder durch Manipulationen bei der Testdurchführung zu einem falschen „negativen" Testergebnis führt (False Negative). Durch die mehrfache Testdurchführung könnte einen Nutzer versuchen die für ihn negativen Konsequenzen eines positiven Schnelltestergebnisses zu umgehen, indem er so lange weitere Tests durchführen lässt/durchführt, bis ein Test	Ja	3	1	3	3	1	1	1	1	1	3	9	VT, IG, ZB	Technische Mitigation schwer umsetzbar, wenn es keine zentralen System zum Monitoring der individuellen Schnelltestungen der Nutzer gibt, die einen solchen Missbrauch erschweren würden.	akzeptabel mit Evaluation
R1-CWA-Nutzer	Manipulation von Daten: Fake-Anzeige von negativen Testergebnissen in der CWA	Nutzer oder auch Hacker könnten versuchen, die Anzeige des Schnelltestergebnisses (eines früheren negatives Tests) so zu manipulieren, dass er in der App wie ein aktuelles reales Schnelltestergebnis aussieht. Wenn diese Anzeige als "Eintrittskarte" nutzbar, könnte der CWA-Nutzer damit diese unrichtigen Daten veröffentlichen, selbst Vorteile erlangen und das Vertrauen in die Richtigkeit der Funktion durch Andere stören.	Ja	1	1	3	3	1	1	1	1	1	3	3	VT, IG, ZB	Um die Integrität von QR-Code und Test zu erhöhen, werden digitale Signaturen verwendet, die auch den Zeitstempel und die personenbezogenen Daten umfassen. App und Backend prüfen diese Signaturen.	akzeptabel
R1-CWA-Nutzer	Manipulation von Daten: Manipulation von Daten mit verzögerter QR-Code-Registrierung	manipulieren. Ohne Validierung der Daten, eine Vielfalt von Angriffe auch von niedrigen technischen Komplexität können umgesetzt werden. Die Auswirkungen sind durchaus höher indem Testergebnisse auf der CWA App als Nachweis angewendet werden können.	Ja	1	1	3	3	1	1	1	1	1	3	3	VT, IG, ZB	Zeitstempel in den gehashten und signierten Daten werden hinzugefügt und geprüft.	akzeptabel
R2- Hacker	Manipulation von Daten: Manipulation von Schnelltest-Nutzerdaten	Wenn Nutzerdaten nicht Verifiziert werden, ein gesunder Nutzer könnte ein Test registrieren, und seine persönlichen Daten im QR Code durch jemand anders ersetzen	Ja	1	1	3	3	1	1	1	3	3	3	3	VT, IG, ZB, T, IV	Einsatz von Digitalen Signaturen.	akzeptabel
R4- Testcenter	Ausstellung und Signierung von Impfzertifikaten/ unrichtigen Testzertifikaten über PoC (Malicious PoC)	anstatt des Hashes eines Testzertifikates den Hash eines Impfzertifikats an den DCC Server, welches dann signiert wird. Da durch die CWA und den DCC nur Hashwerte verarbeitet werden und keine Prüfung auf Richtigkeit erfolgt, erhält ein ggf. Unberechtigter über den PoC ein vermeintlich gültiges Impfzertifikat, erschleicht sich damit weitgehende Erleichterungen und gefährdet u.U. Dritte. Dieses Risiko besteht auch, wenn der Verifier bei der Prüfung nicht	Ja	2	1	1	4	1	1	1	4	4	4	8	IG, IV, TR, ZB	Eine Prüfung des von den Testcentern übergebenen Payloads auf Richtigkeit erfolgt durch die CWA und den DCC Server nicht, da nur Hashes übertragen werden. Die Fälschung von Zertifikaten durch PoC (Mitarbeiter) erfüllt ggf. einen Straftatbestand. Um die Risiken durch ein Malicious PoC zu	akzeptabel mit Evaluation
R1-CWA-Nutzer	Erschleichung von Freiheiten durch legitime/ modifizierte Impfzertifikate/ Testzertifikate/ Genesenenzertifikate anderer Personen	diesen in seiner CWA App einscannt (mittels QR-Code). Die CWA App würde den Impfnachweis erkennen und dementsprechend in der CWA App anzeigen. Alternativ könnte der Angreifer versuchen den QR-Code zu manipulieren, bevor der QR-Code von dem Angreifer in dessen CWA App eingescannt wird. Das würde dazu führen, sofern der Angreifer die (modifizierten) Daten richtig aufbereitet, dass die CWA App modifizierte Daten anzeigen würde. Der	Ja	3	1	3	3	1	1	1	1	1	3	9	VT, IG, ZB	Das Gewähren von Freiheiten und Privilegien muss an eine Prüfung der in der CWA App angezeigten Impfzertifikate (durch entsprechende externe Anwendungen inkl. Prüfung der Personalien) gebunden werden.	akzeptabel mit Evaluation
R2- Hacker	(Massenhafte) Erstellung von QR-Codes (Impfnachweise/ Testzertikate) für die CWA App	Impfnachweise beim Registrieren in der CWA App zu erkennen, sofern diese den Datenstruktur-Vorgaben der CWA App entsprechen. Die Datenstruktur-Vorgaben für die Impfzertifikate sind öffentlich verfügbar. Daher könnten (qualifizierte) Angreifer Impfnachweise inkl. QR-Code erstellen und in Umlauf bringen. Diese Impfnachweise würden von der CWA App als valide erkannt und importiert werden. Dadurch könnte ein CWA-Nutzer dazu verleitet werden sich	Ja	3	3	3	3	1	1	1	1	1	3	9	VT, IG, ZB, DM	Das Gewähren von Freiheiten und Privilegien muss an eine Prüfung der in der CWA App angezeigten Impfzertifikate (durch entsprechende externe Anwendungen inkl. Prüfung der Personalien) gebunden werden.	akzeptabel mit Evaluation
	Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler)																
R6 - Krimineller	Diebstahl/ ungerechtfertigte Nutzung (Kopien) von Zertifikaten im Testcenter	Angreifer stiehlt Zertifikat vom Testcenter und lässt damit für sich ein Zertifikat ausstellen.	Ja	2	1	4	4	1	1	1	2	2	2	8	VT, IG	Verantworung für Diebstahlsschutz beim PoC, Designentscheidung c.) D-2-5 (zusätzliches Datum zur Dublettenvermeidung)	akzeptabel mit Evaluation
R6 - Krimineller	Diebstahl/ ungerechtertigte Nutzung von Zertifikaten im Testcenter durch "Spearfishing"	Zetteln verwenden. Angreifer überredet eine Person sich dort testen zu lassen und versucht so an dessen Testzertifikat zu gelangen, indem er den Test direkt in seiner App registriert bevor das Opfer sich registrieren konnte. (Mit Mitigationsmaßnahme nach Z78, mithin Annahme: Angreifer hat bereits einen QR-Code und kennt das Geburtsdatum vom Opfer).	Ja	2	1	4	4	1	1	1	2	2	2	8	VT, IG	Siehe Zeile 78 // Hinweis an CWA-Nutzer, QR-Code möglichst unverzüglich einzucannen. Nach Scan durch Berechtigten besteht Missbrauchsrisiko nicht mehr.	akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	Falsche Zuordnung von PCR-Testergebnissen zu Schnelltestergebnissen oder Chronologie der individuellen Testabfolge (Schnelltest / PCR-Test/ Schnelltest...) führt zum Überschreiben von Testergebnissen	PCR Tests als auch Schnelltests verwenden SHA-256 Hashwerte als CWA Test ID. Diese IDs dienen als eine „Verbindung" zu einem Testergebnis. Im Moment sollen die PCR Tests als auch die Schnelltests von der CWA App vom CWA Test Result Server über den Verifikation Server durch „Polling" heruntergeladen werden. Es werden dabei die Schnelltests als auch die PCR-Tests in einer Datenbank unter den verschiedenen IDs gespeichert. Sofern bei der Erstellung der IDs gleiche IDs (Schnelltest	Ja	1	1	1	3	1	1	1	1	1	1	3	IG	Verwendung von Algorithmen zur Erzeugung von eindeutigen Hashcodes, die nicht zu Duplikaten führen. Die Gültigkeit der Tests ist maximal 14 Tage. Die Eintrittswahrscheinlichkeit von Kollisionen über UUIDs ist sehr gering. Logische Trennung von PCR und Schnelltests im Test Result Server	akzeptabel
R4- Betreiber Server (T)	Falsche Zuordnung/ Verzerrungen hinsichtlich von Aussagewert von Schnelltests und PCR-Tests	Durch die fehlende Trennung von Schnelltests und "Labortests" von der Eingabe in den Schnelltestzentren/ Laboren bis zur Speicherung im Backend kann der Aussagewert der Testergebnisse verzerrt werden. Dies ist ein Risiko für die Integrität.	Ja	1	1	1	3	1	1	1	1	1	3	3	IG, ZB	PCR und Schnelltests bekommen unterschiedliche Wertebereiche (Designentscheidungen c.,D-6-2). Die Wahrscheinlichkeit einer Kollision bei der Erstellung von SHA-256 Werten ist sehr gering.	akzeptabel
R2- Hacker	DNS-Spoofing / Man-in-the-Middle Attacke, dass PoCs statt mit PoC-Backend mit einem Server seiner Wahl zu kommunizieren (Vorgetäuschter Server)	Durch DNS Spoofing oder eine Man-in-the-Middle Attacke könnte ein Angreifer die PoC dazu bringen, statt mit den legitimen Servern mit einem Server seiner Wahl zu kommunizieren. Das betrifft auch den PoC-Server der Testcenter. Durch Senden unzulässiger oder gefälschter Inhalte könnte der Angreifer die Funktion der PoC beeinträchtigen oder gar zum Erliegen bringen.	Ja	1	0	0	0	4	4	4	4	4	4	4	VT, DM, ZB, T , IV	Designentscheidungen a. B-1-5ff. Einsatz von mutual-TLS	akzeptabel
R2- Hacker	Denial of Service (Mutwillige Überlastung) Angriffe auf CWA-Komponenten über Schnelltest-Netzwerk-Schnittstellen	Die Netzwerk Schnittstellen sind mit mutual-TLS geschützt und weiteren DDoS Angriff Versuchen werden durch den Anti-DDOS der OTC abgewehrt (Verfügbarkeitsrisiko).	Ja	1	0	0	0	3	0	3	0	0	3	3	VF, R, ZB	AV-Verträge mit DL, inkl. TOM , Designentscheidungen D-11-1 (Einsatz von Anti-DDoS Gegenmaßnahmen für die Schnelltest-Netzwerk-Schnittstellen)	akzeptabel
R2- Hacker	Denial of Service (Mutwillige Überlastung) Angriffe auf PoC-Komponenten	Schnelltestzentren (etwa Flughafen) können ihre Schnelltest-Anbindung an die CWA nicht nutzen, wenn die Schnelltestsanbindung an das PoC-Backend nicht verfügbar ist.	Ja	3	0	0	0	3	0	3	0	0	3	9	VF, R, ZB	Verantwortung der PoC und Drittanbieter auch ihre Systeme ausreichend gegen DDoS-Angriffe zu schützen.	bedingt akzeptabel
R4- Testcenter	Nicht ausreichende Sicherheit für Mandanten, die ihre Ergebnisse über den Proxy in die CWA hochladen	Falls die Kommunikationschnittstelle zur Proxy kompromitiert wird, können falsche Informationen übertragen werden.	Ja	1	0	1	2	1	1	1	1	1	1	2	IG	TOM (Absicherung der Kommunikation durch Einsatz von mTLS, whitelisting)	akzeptabel
R2- Hacker	Mutwillige Überlastung über QR-Code ("ZIP-Bombe")	könnte eine sogenannte Archivbombe erstellen und diese in einem schädlichen QR Code einpacken. Beim entkomprimieren der Archivbombe werden die lokalen Ressourcen der QR Code Leser ausgeschöpft. (Ein Beispiel für Archivbombe ist die Datei 42.zip: mit einer komprimierten Größe von 42 kB beim entpacken werden insgesamt Dateien in einer Größe von 4,5 PetaBytes entpackt).	Ja	1	0	0	0	1	0	1	0	0	0	1	VF, BT	. Maximale Größe wurde definiert (10 MB) für die dekomprimierte Information (DSK CWA App v2.3, 7.4.17.3.1).	akzeptabel
	Verarbeitung über die Speicherfrist hinaus																
R4- Betreiber Server (T)	Speicherung von pD im Rahmen DCC-Records über die Gültigkeitsdauer von Testzertifikaten hinaus	Art. 9 Abs. 3 der DCC-I-VO bestimmt, dass die zur Ausstellung verwendeten personenbezogenen Daten nicht länger gespeichert werden dürfen, als das DCC selbst gültig ist. Die Nachverfolgung von Missbräuchen, etwa die Ausstellung von unrichtigen Zertifikaten durch Testcenter, ist für die IT-Forensik in dieser kurzen Zeitspanne nicht gewährleistet. Es droht die Verletzung des Grundsatzes der Datenminimierung und Speicherbegrenzung.	Ja	2	3	1	1	1	1	1	3	3	3	6	DM, IV, TR, ZB	Festlegung von Aufbewahrungspflichten in Abstimmung mit der verantwortlichen Stelle // Erstellung Löschkonzept (Designentscheidungen c.) D-9-5c	akzeptabel mit Evaluation
R4- Betreiber Server (T)	Unbefristete Speicherung von Daten (inkl. Metadaten) auf CWA Server und mögliche spätere Verkettung mit anderen personenbezogenen Daten		Ja	1	4	1	1	0	0	0	3	3	4	4	DM, ZB	Designentscheidungen a. 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	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	AV-Verträge mit DL inkl. TOM , Designentscheidungen D-11-1	akzeptabel
	Risiken durch Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt																
R8- Behörden	Ausweitung der in die CWA-App integrierten Funktionen		Nein	3	4	0	0	0	0	0	0	0	0	-	DM		
R8- Behörden	Diskriminierung von Personen, denen die CWA-Nutzung nicht möglich ist bzw. die keinen Zugang zu Impfzertifikaten haben	MJ unter 16 Jahre können die CWA nicht nutzen und aktuell auch keine Zugang zu Impfstoffen. Sie haben daher auch nicht die Möglichkeit, sich „Freiheiten" mittels der CWA-Infrastruktur zurückzuholen. Es droht daher Diskriminierungen dieser Personengruppen beim Zugang zu (öffentlichen) Einrichtungen, Veranstaltungen zu verstetigen.	Ja	3	0	0	0	3	0	0	0	0	0	9	VF		akzeptabel mit Evaluation