Datenschutzfolgenabschätzung (DSFA) VT 3: Testing_inkl_Laborschnittstelle (Stand: 01.10.2020) + Veränderung Screen Flow (02.12.2020) (Stand: 23.12.2021)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nährere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilenz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum "rote" Risiken akzeptiert werden können**	**Restrisiko**
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	4	**1) Unbefugte oder unrechtmäßige Verarbeitung**																		
R1-CWA-Nutzer	5	Datenverarbeitungen ohne/ nach widerrufener Einwilligung		Ja	1	4	4	4	0	4	0	4	0	4	4	RM	Siehe Designentscheidungen D-3.1-5 (DSK Verifikation und Testergebnis, 6.4.1.1.2) + Designentscheidung (Widerruf) D-3.1-8.			akzeptabel
R1-CWA-Nutzer	6	Unwirksame Einwilligung durch fehlende Freiwilligkeit ("erzwungene Einwilligung")		Ja	1	4	4	4	0	4	0	4	4	4	4	RM	Siehe Designentscheidungen D-3.2-1.			akzeptabel
R1-CWA-Nutzer	7	Unwirksame Einwilligung aufgrund fehlender/ fehlerhafter ausdrückliche Einwilligungserklärung (technischer Einwilligungs-Akt)		Ja	1	4	4	4	0	0	0	4	4	4	4	RM	Siehe Designentscheidungen D-3.1-5 (DSK Verifikation und Testergebnis, 6.4.1.1.2).			akzeptabel
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	8	Unwirksame Einwilligung aufgrund fehlender Information über Umfang und Folgen		Ja	2	4	4	4	0	0	0	4	4	4	8	DM, VT, IG, IV, TR, ZB	Abgestimmte Datenschutzinformationen liegen vor (DSK Verifikation und Testergebnis, 9.1 (mitgeltende Dokumente Datenschutzerklärung).)			akzeptabel, mit Evaluation
R1-CWA-Nutzer	9	Unwirksame Einwilligung aufgrund Nichterreichbarkeit der notwendigen Informationen (sprachliche Barrieren, fehlendes Technikverständnis)		Ja	2	4	4	4	0	0	0	4	4	4	8	DM, VT, IG, IV, TR, ZB	Datenschutzinformationen in leichter Sprache sowie Übersetzungen liegen vor.			akzeptabel, mit Evaluation
R1-CWA-Nutzer	10	Unbefugte Nutzung durch Minderjährige unter 16 Jahre		Ja	4	4	4	4	4	4	4	4	4	4	16	DM, VT, IG, VF, A, R, IV, TR, ZB	Siehe Designentscheidungen D-3.1-2.	Für Phase 2 ist ein zusätzliches Popup-Fenster mit dem Hinweis für Jugendliche unter 16 geplant. Sinngemäß: "Wenn du unter 16 Jahre alt bis, dann besprich bitte die Nutzung der App mit deinen Eltern." (noch nicht im [Release 1.2] vorgesehen)	Gemeinsame Entwicklung der Lösung im Workstream.	bedingt akzeptabel
R4- Betreiber Schnittstelle	11	Abhängigkeit von Dienstleistern (hier: Betreiber der REST-Schnittstelle des CWA-Gateways) (Risiko: Ausfall)		Ja	2	0	0	0	3	0	3	2	2	1	6	VF, R	Schnittstellenbetreiber sind als Unterauftragnehmer der TSI vertraglich gebunden. Vertrag nach Art. 28 DSGVO liegt vor.			akzeptabel mit Evaluation
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	12	Herstellung eines Personenbezugs zum QR-Code		Ja	1	4	4	4	0	0	0	0	0	4	4	ZB, DM, VT, IG	Labormitarbeiter/ Arzt unterliegt dem Berufsgeheimnis/ Verpflichtung zur Vertraulichkeit besteht.			akzeptabel
	13	**2) Verarbeitung wider Treu und Glauben**																		
R1-CWA-Nutzer	14	Vortäuschen von positiven Testergebnissen mit QR-Code		Ja	1	4	4	4	0	4	0	4	4	4	4	DM, VT, IG, A, IV, TR, ZB	Siehe Designentscheidungen B-2-1.			akzeptabel
	15	**3) Für die Betroffenen intransparente Verarbeitung**																		
	16	Fehlende Offenlegung des Source-Codes der REST-Schnittstelle des CWA-Gateways	Source-Code könnte eine Angriffsfläche bieten/ fehlerhaft sein, ohne dass dies transparent wird.	Ja	4	0	0	0	0	0	0	2	2	0	8	IV, TR	Source-Code gegenüber TSI offen.	Source-Code Audit geplant.		akzeptabel mit Evaluation
	17	Unvollständige, unverständliche Datenschutzinformationen zur VT3, Betroffenenrechte (und Laboranbindung an CWA)	Prüfung des Risikos in [Release 1.9] durch veränderten Screenflow zur Einwilligung in das Teilen der Testergebnisse: Screenflow könnte zu Fehlvorstellung des Betroffenen führen, dass dieser durch Betätigen des "x" seine Einwilligung widerrufen kann…. (siehe Z 32 "Beschränkung des Widerrufsrechts bzgl. Einwilligung in das Teilen der Positivschlüssel").	Ja	1	0	2	2	0	0	0	3	4	4	4	TR, ZB	Abgestimmte Datenschutzinformationen liegen vor (DSK Verifikation und Testergebnis, 9.1 (mitgeltende Dokumente Datenschutzerklärung)), ggf. muss diese um weitere Dienstleister ergänzt werden.			akzeptabel
	18	**4) Unbefugte Offenlegung von und Zugang zu Daten**																		
R1-CWA-Nutzer	19	Unbefugte Weitergabe des QR-Codes (vor Scannen)		Ja	2	0	4	4	4	4	4	4	4	4	8	VT, IG, VF, A, R, IV, TR, ZB	Sensibilisierung des Nutzers/ Datenschutzinformationen, siehe DSK_Rahmenkonzept Kap. 10.2 (Der Nutzer ist durch entsprechende Aufklärungsmaßnahmen darauf hinzuweisen, dass er seinen QR-Code unmittelbar nach Empfang scannen und dabei eine Netzwerkverbindung ermöglichen soll).			akzeptabel, mit Evaluation
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	20	Unbefugtes Kopieren/ Weitergabe des QR-Codes (vor Scannen)	Durch das Kopieren des Muster C10-Formulars in Testcentren werden Dubletten verursacht. Von Dubletten Betroffene könnten falsche Testergebnisse angezeigt erhalten oder Fehlermeldungen. Im schlimmsten Fall könnten positv getesteten CWA - Nutzern in der CWA negatives Ergebnis angezeigt werden und Infektionsketten ausgelöst werden.	Ja	2	0	4	4	4	4	4	4	4	4	8	VT, IG, VF, A, R, IV, TR, ZB	Zugangs- und Zugriffsschutz in der Teststelle und im Labor. Hinweise an die Labore/ Teststellen werden wiederholt und anlassbezogen erteilt, dass die Muster C 10 - Formulare nicht kopiert werden dürfen und rechtzeitig nachbestellt werden sollten.			akzeptabel
R6 - Krimineller	21	Diebstahl und Missbrauch des QR-Codes (vor Scannen)		Ja	1	0	4	4	4	4	4	4	4	4	4	VT, IG, VF, A, R, IV, TR, ZB	Siehe Designentscheidungen B-2-1, wenn der Nutzer entsprechend der Sensibilisierung (ziehe Z 19) unmittelbar einscannt, kann dieses Risiko minimiert werden.			akzeptabel
R1-CWA-Nutzer	22	Unbefugte Weitergabe/ Verlust QR-Code (nach Scannen)		Nein											-		Siehe Designentscheidungen B-1-2 und DSK_Rahmenkonzept Kap. 10.2 (Um dem zu begegnen, wird von der Anwendung unmittelbar nach dem Scannen der QR-Code auf dem Verifikationsserver gegen ein Registration Token eingetauscht und der QR-Code auf dem Server als verbraucht gekennzeichnet).			
	23	Unbefugter Zugang zum Laborgateway		Ja	2	0	4	4	2	2	2	2	2	4	8	VT, IG, ZB	Zertifikatsbasierte Authentifikation der Server und Zertifikatsmanagment (Erstellung + Verteilung) wird implementiert.			akzeptabel mit Evaltualiton
R2- Hacker	24	Re-Identifikation von Positiv-Getesteten durch Angriff auf Rest-Schnittstelle (Zugriff auf GUID und Testergebnis)	Der Angreifer bräuchte Zusatzwissen, um den Personenbezug herzustellen. Allein die Kenntnis von GUID und Testergebnis lässt keinen Rückschluss aufeine Person zu. Ausnahme: Sehr kleine Testmenge bzw. Labor testet nur einen sehr eingeschränkten Personenkreis und man kann daraus dann Rückschlüsse ziehen, wie "3 Personen wurden getestet, es werden 3 positive Ergebnisse übermittelt -> alle positiv"	Ja	2	2	3	3	2	0	2	2	2	3	6	VT, ZB	Einsatz von Hardware mit "Backdoors" ist mit IT-Security auf Infrastrukturebene zu flankieren. Signatur erforderlich. Pentest wurde durchgeführt.			akeptabel mit Evaluation
R2- Hacker	25	Re-Identifikation von Positiv-Getesteten durch Überwachung des Internetverkehrs des Labors zum CWA-Gateway (CWA-Infrastruktur); Zugriff auf GUID und Testergebnis	Risiko existent, wenn ein Mapping der Person zu GUID vorhanden ist. Allein die GUID und Testergebnis bringen nur bedingt Informationen. Ausnahme: Labor testet nur einen sehr eingeschränkten Personenkreis und man kann daraus dann Rückschlüsse ziehen, wie "3 Personen wurden getestet, es werden 3 positive Ergebnisse übermittelt -> alle positiv".	Ja	2	2	3	3	2	0	2	2	2	3	6	VT, ZB	Einsatz von Hardware mit "Backdoors" ist mit IT-Security auf Infrastrukturebene zu flankieren. Signatur erforderlich. Pentest wurde durchgeführt.			akzeptabel mit Evaluation
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	26	**5) Ungerechtfertigter Datentransfer in Drittland**		Ja	1	0	4	4	0	0	0	4	4	4	4	VT, IG, IV, TR, ZB	Labormitarbeiter/ Arzt unterliegt Berufsgeheimnis und Verpflichtung zur Vertraulichkeit.			akzeptabel
	27	**6) Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten**																		
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	28	Beschädigung des QR-Codes, unbeabsichtigter oder unsachgemäße Entsorgung von (beschädigtern QR-Codes		Ja	1	1	1	1	1	1	1	1	1	1	1	keine Besonderheiten	Labormitarbeiter/ Arzt unterliegt Berufsgeheimnis und Verpflichtung zur Vertraulichkeit			akzeptabel
R1-CWA-Nutzer	29	Verlust des QR-Codes (vor Scannen)		Ja	1	4	4	4	4	4	4	4	4	4	4	VT, IG, VF, A, R, IV, TR, ZB	Sensibilisierung des Nutzers/ Nutzerverantwortung / Designentscheidungen B-1-2, siehe DSK_Rahmendokument Kap. 10.3 - nach Verlust des QR-Codes kann der Nutzer den Alternativweg über die Verifikations-Hotline nutzen.			akzeptabel
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	30	**7) Verweigerung der Betroffenenrechte**		Ja	1	1	1	1	1	0	1	1	1	1	1	keine Besonderheiten	Abgestimmte Datenschutzinformationen liegen vor. Zu Nicht-Erfüllung von Betroffenenrechten siehe Designentscheidungen B-8-1.			akzeptabel

Datenschutzfolgenabschätzung (DSFA) VT 3: Testing_inkl_Laborschnittstelle (Stand: 01.10.2020) + Veränderung Screen Flow (02.12.2020) (Stand: 23.12.2021)				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 "rote" Risiken akzeptiert werden können**	**Restrisiko**
	31	Fehlende Löschung nach berechtigtem Löschersuchen von personenbezogenen Daten (GUID+Testergebnis); Datenbank-Schnittstelle		Nein											-		Keine Pflicht zur Identifizierung, um Betroffenenrechte zu erfüllen (Art. 11 DSGVO); keine Speicherung in Datenbank der REST-Schnittstelle vorgesehen, Prüfung der fehlenden Speicherung erfolgt im Rahmen Quellcode-Analyse.			
	32	[Release 1.9] Beschränkung des Widerrufsrechts bzgl. Einwilligung in das Teilen der Positivschlüssel	Für [Release 1.9] wurde das Risiko für die rechtmäßige Datenverarbeitung durch den veränderten Screenflow für die Einwilligung in das Teilen der Positivschlüssel betrachtet (siehe Z 5) und für die transparente DV (Z 17) überprüft und in Z 32 als Risiko durch Verweigerung von Betroffenenrechten neu dokumentiert: Nachdem der Nutzer "Teilen" bestätigt hat, ist ein Widerruf nicht mehr möglich, auch wenn der CWA-Nutzer seine Eingaben zum Symptombeginn abbricht.	Ja	1	4	4	4	0	2	0	4	4	4	4	RM, DM, VT, IG, IV, ZB, T	Designentscheidungen D-2.1.6 und D-2.1.8 (der CWA-Nutzer wird zusammen mit der Einwilligung zum Abruf seines Testergebnisses frühzeitig auch um seine Einwilligung zum etwaigen Teilen dieses Testergebnisses, sprich seiner Positivschlüssel, gebeten - für den Fall, dass der Test auf Corona positiv ausfallen sollte. Dies soll sowohl der Einfachheit der Benutzerführung dienen als auch verhindern, dass ein CWA-Nutzer bei Bekanntwerden seines positiven Testergebnisses aus emotionaler Erregung das Teilen seiner Positivschlüssel vergisst. Auf Letzteres zielt ebenfalls eine etwaige Erinnerungsbenachrichtigung. Wenn der CWA-Nutzer die Einwilligung erteilt hat, wird ihm dieser Umstand im Laufe der weiteren Bedienung der CWA-App immer wieder angezeigt; durch Anklicken der Anzeige erhält er jeweils die Möglichkeit, seine Einwilligung zu widerrufen. Die letzte Möglichkeit zum Widerruf besteht auf der Bildschirmseite, in der dem CWA-Nutzer die Verfügbarkeit seines Testergebnisses präsentiert wird. Im Falle eines positiven Testergebnisses wird im nächsten Schritt nun auch betriebssystemseitig in einem Pop-up vom ENF die Zustimmung zum Teilen der Positivschlüssel eingeholt. Danach nimmt die CWA-App vom ENF die Positivschlüssel des CWA-Nutzers entgegen und visualisiert dem CWA-Nutzer sein positives Testergebnis. Von nun an kann ein Teilen seiner Positivschlüssel vom CWA-Nutzer nicht mehr verhindert werden (außer durch den erzwungenen Abbruch der CWA-App mit Betriebssystemmitteln). Im Nachgang wird der CWA-Nutzer noch um freiwillige Angaben zum Symptombeginn gebeten, bevor die Positivschlüssel endgültig auf den CWA-Server			akzeptabel
	33	**8) Verwendung der Daten zu inkompatiblen Zwecken**																		
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	34	Übertragung von Testergebnissen an Unberechtigte (via Internet, analog…)		Ja	1	1	1	1	0	0	0	4	4	4	4	IV, TR, ZB	Labormitarbeiter/ Arzt unterliegt Berufsgeheimnis und Verpflichtung zur Vertraulichkeit.			akzeptabel
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	35	Ermöglichung des Zugriffs auf Testergebnisse an Unberechtigte durch Freigabe der Schnittstelle (etwa Ermöglichung des Zugriffs durch Gesundheitsbehörden)		Nein											-		Risiko technisch ausgeschlossen, da es sich um eine reine Import-Schnittstelle handelt und keine Export-/ bidirektionale Schnittstelle.			
R6 - Krimineller	36	Verwendung der Daten zu inkompatiblen Zwecken (Verkettung von Positivschlüssel zu gehashter GUID/ Tele Tan (intern)	Nur mit Zusatzwissen von Labormitarbeitern/ ärtzlichem Personal möglich.	Ja	1	4	4	4	0	0	0	4	4	4	4	VT, IG, DM, ZB, TR, IV	Labormitarbeiter/ Arzt unterliegt Berufsgeheimnis und Verpflichtung zur Vertraulichkeit/ Designentscheidungen D-4.2-3 (Hash GUID).			akzeptabel
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	37	**9) Verarbeitung nicht vorhergesehener Daten**																		
R6 - Krimineller	38	Übertragung einer Vielzahl an fehlerhaften Daten (Denial of Service) führt zu Ausfall des CWA-Gateways oder fehlerhafter Verarbeitung		Ja	3	0	0	1	3	0	3	0	0	3	9	VF, R, ZB	Entsprechende Hardware-Absicherung als auch Berücksichtigung von Skalierbarkeit bei Software-Entwicklung. Neuübermittlung von Daten nach Wiederverfügbarkeit des Systems. In der Infrastruktur der OTC werden DoS-Angriffe detektiert und mit IT-Sicherheitsmaßnahmen behandelt. Zertifikate dienen der Risikomitigierung. Prüfung der Semantik erfolgt und führt zu Fehlermeldung.			akzeptabel mit Evaluation
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	39	Eingabe identifizierender Daten in Laborsoftware und nachfolgende Weiterverarbeitung im CWA-System		Ja	1	3	3	2	0	0	0	3	3	3	3	DM, VT, IG, IV, TR, ZB	Labormitarbeiter/ Arzt unterliegt Berufsgeheimnis und der Verpflichtung zur Vertraulichkeit. CWA-System kann technisch lediglich GUID und keine weiteren personenbezogenen Daten verarbeiten.			akzeptabel
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	40	**10) Verarbeitung nicht richtiger Daten**		Ja	1	4	4	4	0	4	0	4	4	4	4	DM, VT, IG, AZB, R	Labormitarbeiter/ Arzt unterliegt Berufsgeheimnis und der Verpflichtung zur Vertraulichkeit.			akzeptabel
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	41	Eingabe falscher Daten in Laborsoftware und Weiterverarbeitung im System		Ja	1	3	3	2	0	0	0	3	3	3	3	DM, IG,VT, IV, TR, ZB	Labormitarbeiter/ Arzt unterliegt Berufsgeheimnis und der Verpflichtung zur Vertraulichkeit. CWA-System überprüft übertragene Daten syntaktisch und verarbeitet nur gültige Datensätze. CWA-System prüft nicht auf inhaltliche Korrektheit.			akzeptabel
	42	**11) Fehlerhafte Verarbeitung**																		
R4- Betreiber Schnittstelle	43	Unsichere Programmierung	TSI-seitige Nutzung von Hard-, Software- Komponenten mit bekannten Schwachstellen, Modifikation von Software, um Verbindung CWA-Gateway herzustellen.	Ja	2	3	3	3	3	3	3	3	3	3	6	DM, VT, IG, VF, A, R, IV, TR, ZB	Regelmäßige Überprüfung der Software (Code-Review/ Penetrationtests) und Hardware im Rahmen von Audits.	Sourcecode Audit ist vorgesehen.		akzeptabel mit Evaluation
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	44	Unsichere Programmierung	Laborseitige Nutzung von Hard-, Software- Komponenten mit bekannten Schwachstellen, Modifikation von Software, um Verbindung CWA-Gateway herzustellen.	Ja	3	3	3	3	3	3	3	3	3	3	9	DM, VT, IG, VF, A, R, IV, TR, ZB	Regelmäßige Überprüfung der Software (Code-Review/ Penetrationtests) und Hardware im Rahmen von Audits (nicht in Verantwortung Service-Provider).			akzeptabel mit Evaluation
R4- Betreiber Schnittstelle	45	Fehlfunktion der REST-Schnittstelle des CWA-Gateway		Ja	3	3	3	3	3	3	3	3	3	3	9	DM, VT, IG, VF, A, R, IV, TR, ZB	Durchführung von Penetration-Tests sowie Code-Reviews.			akzeptabel mit Evaluation
R4- Betreiber Schnittstelle	46	Fehlende IT-Sicherheits-Tests- und Freigabeverfahren für Rest-Schnittstelle + CWA-Gateway (fehlendes Audit)		Ja	1	3	3	3	3	3	3	3	3	3	3	IG, VF, R, VT	Pentests erfolgen			akzeptabel
	47	Fehlfunktion bei dicht aufeinanderfolgenden Covid 19-Tests		Ja	3	1	1	1	0	1	0	4	4	4	12	ZB, IV, TR	Ungeeignetheit für dicht aufeinanderfolgende Tests ist im DSK-Rahmenkonzept als Restrisiko beschrieben.		Bekannte Funktionseinschränkung	bedingt akzeptabel. Funktionseinschränkung ist bekannt.
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	48	**12) Verarbeitung über die Speicherfrist hinaus**		Ja	2	2	1	1	0	0	0	4	4	4	8	ZB, IV, TR	Die gehashte GUID wird nach 14 Tagen von den Servern gelöscht - siehe Designentscheidungen B-5.1-11d.			akzeptabel, mit Evaluation
R4 - Softwareentwickler u Server Betreiber (SAP/ T)	49	Fehlende Löschung in Datenbanken des CWA-Gateway		Ja	1	4	1	1	0	0	0	4	4	4	4	DM, IV, TR, ZB	Siehe Systembeschreibung. Speicherung erfolgt nur während der Prozesslaufzeit, keine Persistierung in einer Datenbank.			akzeptabel
	50	**12) Risiken durch Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt**																		
	51																			