

Datenschutzfolgenabschätzung (DSFA)			Risikobewertung																
VT 3: Testing_inkl_Laborschnittstelle (Stand: 01.10.2020) + Veränderung Screen Flow (02.12.2020)			Schadensausmaß																
Risiko-Quelle	Bedrohung/ Risiko	Beschreibung des Risikos (optional)	Schwachstelle (ja/nein)	EW	Datensminierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverketung	Risikoklasse	Soll-Maßnahmen - ID	etablierte Maßnahmen	geplante Maßnahmen	Bewertung, warum "rote" Risiken akzeptiert werden können	Restrisiko
R7-Labormitarbeiter/ Arzt (Berufsgeheimsträger)	Unbefugte oder unrechtmäßige Verarbeitung																		
R1-CWA-Nutzer	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	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	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 (Berufsgeheimsträger)	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 liegt vor (DSK Verifikation und Testergebnis, 9.1 (mitgeltende Dokumente Datenschutzerklärung)			akzeptabel, mit Evaluation
R1-CWA-Nutzer	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, Übersetzungen			akzeptabel, mit Evaluation
R1-CWA-Nutzer	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 bist, dann besprich bitte die Nutzung der App mit deinen Eltern." (dies kommt nicht in Version 1.2)	Gemeinsame Entwicklung der Lösung im Workstream	bedingt akzeptabel,
R4- Betreiber Schnittstelle	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 als Unterauftragnehmer der TSI vertraglich gebunden. Vertrag nach Art. 28 DSGVO liegt vor.			akzeptabel mit Evaluation
R7-Labormitarbeiter/ Arzt (Berufsgeheimsträger)	Herstellung Personenbezug zu 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			akzeptabel
	Verarbeitung wider Treu und Glauben																		
R1-CWA-Nutzer	Vortauschen 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
	Für die Betroffenen intransparente Verarbeitung																		
	Fehlende Offenlegung des SourceCodes der REST-Schnittstelle des CWA-Gateways	Sourcecode könnte eine Angriffsfläche bieten, fehlerhaft sein ohne dass dies transparent wird. Prüfung des Risikos in VT.3 durch veränderten Screenflow zur Einwilligung in das Telen der Testergebnisse: Screenflow könnte zu Fehlvorstellung des Betroffenen führen, dass dieser durch Betätigen des "X" seine Einwilligung widerrufen kann.... (siehe Z.32)	Ja	4	0	0	0	0	0	0	2	2	0	8	IV, TR	Source Code gegenüber TSI offen / SourceCode Audit ist geplant.			akzeptabel mit Evaluation
	Unvollständige, unverständliche Datenschutzinformationen VT3, Betroffenenrechte (und Laboranbindung an CWA)		Ja	1	0	2	2	0	0	0	3	4	4	4	TR, ZB	abgestimmte Datenschutzinformation liegt vor (siehe Z.8), ggf. muss diese um weitere Dienstleister ergänzt werden.			akzeptabel
	Unbefugte Offenlegung von und Zugang zu Daten																		
R1-CWA-Nutzer	Unbefugte Weitergabe QR-Code (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/ Datenschutzinformation, 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 (Berufsgeheimsträger)	Unbefugte Weitergabe QR-Code (vor Scannen)		Ja	1	0	4	4	4	4	4	4	4	4	4	VT, IG, VF, A, R, IV, TR, ZB	Zugangs- und Zugriffsschutz im Labor			akzeptabel
R6 - Krimineller	Diebstahl und Missbrauch QR-Code 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 (siehe Z.19) unmittelbar einscann, kann dieses Risiko minimiert werden.			akzeptabel
R1-CWA-Nutzer	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 des QR-Codes der QR-Code auf dem Verifikationsserver gegen ein Registration Token ausgetauscht und der QR-Code auf dem Server als verbraucht.			
	Unbefugter Zugang zum Laborgateway		Ja	2	0	4	4	2	2	2	2	2	4	8	VT, IG, ZB	zertifikatsbasierte Authentifikation der Server und Zertifikatsmanagement (Erstellung + Verteilung) wird implementiert			akzeptabel mit Evaluation
R2- Hacker	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 auf Person zu. Ausnahme: Sehr kleine Testmenge bzw. Labor testet nur 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	Ja	2	2	3	3	2	0	2	2	2	3	6	VT, ZB	Einsatz von Hardware mit "Backdoors" ist zu flankieren mit IT-Security auf Infrastrukturebene. Signatur erforderlich. Pentest wurde durchgeführt.			akzeptabel mit Evaluation
R2- Hacker	Re-Identifikation von Positiv-Getesteten durch Überwachung Internetverkehr Labor zum CWA Gateway (CWA Infrastruktur) (Zugriff auf GUID und Testergebnis)		Ja	2	2	3	3	2	0	2	2	2	3	6	VT, ZB	Einsatz von Hardware mit "Backdoors" ist zu flankieren mit IT-Security auf Infrastrukturebene. Signatur erforderlich. Pentest wurde durchgeführt.			akzeptabel mit Evaluation
R7-Labormitarbeiter/ Arzt (Berufsgeheimsträger)	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
	Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten																		
R7-Labormitarbeiter/ Arzt (Berufsgeheimsträger)	Beschädigung QR-Code, unbeabsichtigter oder unsachgemäße Entsorgung (beschädigter) 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	Verlust QR-Code 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 QR-Code kann der Nutzer den Alternativweg über die Verifikations-Hotline nutzen			akzeptabel
R7-Labormitarbeiter/ Arzt (Berufsgeheimsträger)	Verweigerung der Betroffenenrechte		Ja	1	1	1	1	0	1	1	1	1	1	1	keine Besonderheiten	abgestimmte Datenschutzinformation liegt vor (siehe Z.8) / zu Nicht-Erfüllung von Betroffenenrechten siehe Designentscheidungen B-8-1			akzeptabel

Datenschutzfolgenabschätzung (DSFA)			Risikobewertung																
VT 3: Testing_inkl_Laborschnittstelle (Stand: 01.10.2020) + Veränderung Screen Flow (02.12.2020)																			
			Schadensausmaß																
Risiko-Quelle	Bedrohung/ Risiko	Beschreibung des Risikos (optional)	Schwachstelle (ja/nein)	EW	Datensminierung	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
	Fehlende Löschung nach berechtigtem Löschersuchen von pD (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.			
	Beschränkung des Widerrufsrechts bzgl. Einwilligung in das Teilen Teilen der Positivschlüssel	Für VT.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	Ja	1	4	4	4	0	2	0	4	4	4	4	RM, DM, VT, IG, IV, ZB, T	Designentscheidungen D-3.1.6 und D-3.1.8 (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			akzeptabel
	Verwendung der Daten zu inkompatiblen Zwecken																		
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	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)	Ermöglichung Zugriff auf Testergebnisse an Unberechtigte durch Freigabe Schnittstelle (etwa Ermöglichung Zugriff durch Gesundheitsbehörden)		Nein											-		Risiko technisch ausgeschlossen, da es sich um eine reine Import-Schnittstelle handelt und keine Export/Bidirektionale Schnittstelle.			
R6 - Krimineller	Verwendung der Daten zu inkompatiblen Zwecken (Verkettung von Positivschlüssel zu gehashter GUID/ Tele Tan (intern) (nur mit Zusatzwissen von Labormitarbeitern/ ärztlichem 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)	Verarbeitung nicht vorhergesehener Daten																		
R6 - Krimineller	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.			akzeptabel mit Evaluation
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	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)	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)	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
	Fehlerhafte Verarbeitung																		
R4- Betreiber Schnittstelle	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)	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	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	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
	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 in DSK Rahmenkonzept als Restrisiko beschrieben		Bekannte Funktionseinschränkung	bedingt akzeptabel. Funktionseinschränkung ist bekannt.
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	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