	Datenschutzfolgenabschätzung (DSFA) - VT 3: Verification Hotline (Stand: 13.06.)	Risikobewertung																
Risiko-Quelle	Bedrohung/ Risiko	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resillenz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	etablierte Maßnahmen	geplante Maßnahmen	Bewertung, warum "rote" Risiken akzeptiert werden können	Restrisiko
R9- Hotlinemitarbeiter	Unbefugte oder unrechtmäßige Verarbeitung	Ja	2	4	4	4	4	4	4	4	4	4	4	RM	siehe Designentscheidungen D-5.1-21 (Abschluss AVV, inkl. Verpflichtung auf Vertraulichkeit/ §203)			akzeptabel
R9- Hotlinemitarbeiter	Datenverarbeitungen ohne/ nach widerrufener Einwilligung (am Telefon) (bisher nicht vorgesehen)	Nein	1	4	4	4	0	4	0	4	0	4	-	RM, IV	siehe Designentscheidung D-4.2-2 (keine DSGVO-relevante Verarbeitung)			akzeptabel
	Erhebung/ Speicherung nicht - notwendiger pD (inkl. Erhebung Mobilifunknummer)	Ja	2	4	1	1	0	0	0	4	4	4	8	DM , IV, TR, ZB	siehe Designentscheidungen D-5.1-21 (AVV)	Expliziter Hinweis bei der Schulung der Hotlinemitarbeiter, regelmäßige stichprobenhafte Überprüfung im Sinne von MysteryCalls)		akzeptabel, mit Evaluation
	Verarbeitung wider Treu und Glauben																	
		Ja	3	4	1	4	0	4	0	4	4	4	12	DM, I,G, IV, TR, ZB	siehe Designentscheidungen D-5.1-20. Anrufer teilt Hotline- Mitarbeiter seine Rufnummer mit und erhält teleTAN bei Rückruf. Plausibilitätsfragen werden gestellt, um falsche Ergebnisse zu verhindern. Plausibilitätsfragen sind abgestimmt mit Auftrageber und regelmäßigs Schäffung dieser.	Beschleunigte Anbindung der Labore. Mögliche Handlungsoptionen: Abgestuftes Verfahren zur Persistlerung eines minimalen Sets an personenbezogenen Daten, um stichprobenhaft möglichen Missbrauch zu überprüfen. Prüfung alternativer Verffikationsprozesse.	Gemeinsame Entwicklung der Lösung im Workstream	bedingt (zeitlich) akzeptabel
R1-CWA-Nutzer	Vortäuschen Identität gegenüber Hotline + Vortäuschen positiver Testergebnisse												0					
	Für die Betroffenen intransparente Verarbeitung Unvollständige, unverständliche Datenschutzinformationen durch Hotline	Ja	2	0	0	0	0	0	0	4	4	4	8	TR, ZB, IG	Datenschutzinformation Hotline	Regelmäßige Überprüfung der Datenschutzinformationen auf Vollständigkeit, Verständlichkeit und Aktualität durch den Verantwortlichen		akzeptabel , mit Evaluation
	Unbefugte Offenlegung von und Zugang zu Daten																	
R1-CWA-Nutzer	Unbefugte Weitergabe von teleTan nach Erhalt von Hotline (Gültigkeit 1h)	Ja	1	0	4	4	0	0	0	4	0	4	4	ZB, IG, VT, IV	Sensibilisierung der Nutzer durch Datenschutzinformation	Inhaltliche Belehrung des Nutzers und Hinweis auf mögliche Konsequenzen bei Zuwiderhandlung		akzeptabel
R9- Hotlinemitarbeiter	Unbefugte Weitergabe von teleTan, Daten des Nutzer an Dritte/ Gesundheitsbehörden	Ja	2	1	4	4	0	4	0	4	4	4	8	VT, IG, IV, T, ZB	Siehe Designentscheidungen D-5.1-21 (Abschluss AVV + Verpflichtung auf Vertraulichkeit / §203)			akzeptabel, mit Evaluation
R4- Betreiber Server (T)	Fehlende Sicherheitseinstellungen bei der Nutzung der Technik durch Hotline-Mitarbeiter	Ja	2	3	3	3	3	1	3	3	3	3	6	VT, IG, VF, ZB, TR		Compliance-Überbrüfung der Hardware durch Betriebsteam der Hotline		akzeptabel , mit Evaluation
R2- Hacker	Brute Force Angriff auf teleTAN	Ja	4	1	4	4	0	0	0	0	4	4	16	VT, ZB, TR, IG	DSK Verifikations-Hotline, 8.2.1/ Designentscheidungen B-1-3 (Gültigkeitsdauer der teleTAN ist limitiert. Ebenso ist die Länge entsprechend gesetzt, sodass hierbei eine BruteForce-Attacke entsprechend Zeit in Anspruch nehmen würde)	IT-Sicherheit gewähleisten: Es sollte ermöglicht werden, die Konfiguration der teleTAN Länge über die signierten Konfigurations Parameter zu ändern um sich auf entwickelnde Bedrohungen, an sich ändermde Situationen und Belastungen anzupassen	durch geplante Maßnahmen IT-Security akzeptabel	bedingt akzeptabel, mit Adressierung IT- Sicherheit,
	Ungerechtfertigter Datentransfer in Drittland	Ja	1	0	4	4	0	0	0	4	4	4	4	VT, IG, IV, TR, ZB	Designentscheidungen D-5.1-21 (Abschluss AVV, inkl. Verpflichtung auf Vertraulichkeit/ §203			akzeptabel
	Nutzung Internettelefonie	Ja	2	4	1	1	1	1	1	4	4	4	8	VT, ZB, TR, IV	DSK Verifikations-Hotline .8.2.1 (Keine Nutzung von Internettelefonie erlaubt - Compliance Überprüfung der Hardware durch Betriebsteam der Hotline sowie Regelungen in AVV)			akzeptabel , mit Evaluation
	Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten	Ja	1	0	4	4	0	0	0	4	4	4	4	TR, ZB, VT, IG, IV	DSK Verifikations-Server 8.2.1 (Gültigkeitsdauer ist limitiert/ es kann neue teleTan angefordert werden)			akzeptabel
R1-CWA-Nutzer R7-Labormitarbeiter/ Arzt	Verlust teleTan vor Nutzung	Nein	2	0	0	0	0	0	0	4	4	4		IV, T, ZB	keine DSGVO-relevante Datenverarbeitung			
	Verweigerung der Betroffenenrechte	Ja	1	1	4	1	0	0	0	4	4	4	4	VT, IV, TR, ZB	siehe Designentscheidungen D-5.1-21 (AVV, inkl. Verpflichtung zur Einhaltung der Zweckbindung (Verpflichtung zur Vertraulichkeit)+ besondere Regelung, dass Hotline-Betreiber von der Pflicht beferit, Daten zu speichern.			akzeptabel
	Verwendung der Daten zu inkompatiblen Zwecken	Ja	2	4	4	4	0	0	0	4	4	4	8	DM, VT, IG, IV, TR, ZB	Verpfichtung zur Einhaltung der Zweckbindung (Verpflichtung			akzeptabel, mit Evaluation
	Verarbeitung nicht vorhergesehener Daten Speicherung freiwilliger Angaben des Anrufers	Ja	2	4	4	1	0	1	0	4	4	4	8	VT, ZB , DM	speicnern. Alle Daten, welche der Anrufer mitteilt werden allein über das Telefon übermittelt. Es wird der Name sowie die Telefonnummer für den Rückruf festgehalten und direkt danach sicher entsorgt. Sollten zusätzliche Informationen übermittelt werden, ist der Hotline Mitarbeiter darauf geschult diese nicht zu persistieren oder weiterzugeben/ siehe Designentscheidungen D-5.1-21			akzeptabel , mit Evaluation
	Verarbeitung nicht richtiger Daten																	

R9- Hotlinemitarbeiter	Verarbeitung ungültiger/ unrichtiger teleTANs	Ja	2	4	4	1	0	1	0	4	4	4	8	VT, ZB; DM, IV, TR,	DSK Verifikationsserver 8.2.1 - Input Validierung bei allen Schnittstellen (inkl. Eingabe in der CWA-App) stellt sicher, dass der Nutzer bereits möglichst früh über syntaktisch unrichtige telef ANs informiert wird. Sollten telef ANs bei der Schnittselle als ungültig erkannt werden, ist dies entsprechend bei der Antwort der Schnittstelle berücksichtigt.		akzeptabel , mit Evaluation
R9. Hotlinemitarheiter	Fehlerhafte Verarbeitung	Ja	2	2	2	2	0	0	0	2	4	4	8	DM, ZB, T	DSK Verifikations-Hotline 8.2.1 - Fehlerhafte Verarbeitungen in der Hotline werden protokolliert. Hierbei wird darauf geachtet nicht die fachlichen personenbezogenen Daten zu protokollieren, sondern den anonymisierten fachlichen Anwendungsfall zur Fehleranalyse.		akzeptabel, miit Evaluation
	Verarbeitung über die Speicherfrist hinaus																
R9- Hotlinemitarbeiter	Rufnummer wird nach Rückruf nicht sachgerecht entsorgt	Ja	2	4	4	0	0	0	0	4	4	4	8	VT, TR, ZB, DM, IG,	siehe Designentscheidungen B-1-3 und D-5.1-21 (Abschluss AVV)	Stichprobenhafte Überprüfung auf Nichteinhaltung der Handlungsanweisung von Mitarbeitern, speziell bei Mißbrauchsverdacht	akezptabel , mit Evaluation
	Risiken durch Verabeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt														DSK Verifikations-Hotline 8.2.1: Durch Input Validierung bzw. Ausgabebereinigung wird bereits vor der tatsächlichen fachlichen Verarbeitung von Daten sichergestellt, dass keine fehlerhaften Daten im System gespeichert werden bzw. aus dem System kommen.		