			Datenschutzfolgenabschätzung (DSFA) -																		T
VT 3: Verifika	ion Hotline (Stan	nd: 13.06.) // Bericht	igung RS-Fehler und Anpassungen in Spalte T am 24.07.2020 // Aktualisierung: 10.10.2020	Retroffenences					R	isikobewer Sci	tung hadensausm	тав									
Prüfgegenstand/ Risikoursprung	Risiko-Quelle	Nr.	Bedrohung/ Risiko	Betroffenengruppen (CWA-Nutzer, Nutzer anderer nat. Corona- Apps, Personen im Umfeld, Personen, die von Falschmeldungen Betroffen sein könnten). Soweit keine Auswahl	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilionz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	etablierte Maßnahmen	geplante Maßnahmen	Bewertung, warum "rote" Risiken akzeptiert werden könne	en Restrisiko
Allgemein	19- Hotline Mitarbeiter		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
	t9- Hotline Mitarbeiter		Datenverarbeitungen ohne/ nach widerrufener Einwilligung (am Telefon)		Ja	1	4	4	4	0	4	0	4	0	4	4	RM, IV	siehe Designentscheidung D-4.2-2 + DSK Verifikations-Hotline			akzeptabel
	19- Hotline Mitarbeiter		Erhebung/ Speicherung nicht - notwendiger pD (inkl. Erhebung Mobilfunknummer)		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 Hotline Mitarbeiter, regelmäßige stichprobenhafte Überprüfung im Sinne von MysteryCalls)		akzeptabel, mit Evaluati
	19- Hotline Mitarbeiter																				
	19- Houine Mitarbeiter		Verarbeitung wider Treu und Glauben  Vortäuschen Identität gegenüber Hotline + Vortäuschen positiver Testergebnisse		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 Holline- Mitarbeiter seine Rufnummer mit und erhält tele TAN bei Rückruf. Plausibilitätsfragen werden gestellt, um falsche Ergebnisse zu verhindern. Plausibilitätsfragen sind abgestimmt mit Auftraggebes und regelmäßige Schärfung dieser.	Beschleunigte Anbindung der Labore. Mögliche Handlungsoptionen: Abgestuftes Verfahren zur Persistierung eines minimalen Sets an personenbezogenen Daten, um stichprobenhaft möglichen Missbrauch zu überprüfen. Prüfung alternativer Verflikationsprozesse.	Gemeinsame Entwicklung der Lösung im Workstream	bedingt (zeitlich) akzeptabel,
			Für die Betroffenen intransparente Verarbeitung													0					
	19- Hotline Mitarbeiter		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
	3- Hourse with Deter																				
	t1-CWA-Nutzer		Unbefugte Offenlegung von und Zugang zu Daten  Unbefugte Weltergabe 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
	t9- Hotline Mitarbeiter		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 Evalua
	t4- 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-Überprüfung der Hardware durch Betriebsteam der Hotline		akzeptabel , mit Evaluation
	12- 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 hierbel eine Brutle-Force-Atlacke entsprechend Zeit in Anspruch nehmen würde)	IT-Sicherheit gewährteisten: Es sollte ermöglicht werden, die Konfliguration der teleTAN Länge über die signierten Konfiguration Parameter zu ändern um sich auf entwickelnde Bedrohungen, an sich ändernde Situationen und Belastungen anzupassen	durch geplante Maßnahmen IT-Security akzeptabel	bedingt akzeptabel, Adressierung IT- Sicherheit,
	t9- Hotline Mitarbeiter		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
	t9- Hotline Mitarbeiter		Nutzung Internetitelefonie		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
	19- Hotline Mitarbeiter		Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten																		
	11-CWA-Nutzer		Verlust teleTan vor Nutzung		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
ı	t7-Labormitarbeiter/ Arz Berufsgeheimnisträger)	zt )	Verweigerung der Betroffenenrechte		Ja	2	0	0	0	0	0	0	4	4	4	8	IV, T, ZB	Auf Widerrufsmöglichkeit der Einwilligung wird ausdrücklich hingewiesen			
	19- Hotline Mitarbeiter		Verwendung der Daten zu inkompatiblen Zwecken		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 Holline-Betreiber vor der Pflicht befreit, Daten zu speichern.			akzeptabel
	19- Hotline Mitarbeiter		Verarbeitung nicht vorhergesehener Daten		Ja	2	4	4	4	0	0	0	4	4	4	8	DM, VT, IG, IV, TR, ZB	Verpflichtung zur Einhaltung der Zweckbindung (Verpflichtung zur Vertraulichkeit und AVV-Vertag),, besondere Regelung, dass Hotline-Betreiber von der Pflicht befreit, Daten zu speichern.			akzeptabel, mit Evalua
					Ja	2	4	4	1	0	1	0	4	4	4	8	VT, ZB , DM	Alle Daten, welche der Anrufer mitteilt werden allein über das Telefon übermittelt. Es wird der Name sowie die Telefonnummer für den Rückruf festgehalten und dreikt danach sicher entsorgt. Sollten zusätzliche Informationen übermittelt werden, ist der Hotline Mitarbeiter darauf geschult diese nicht zu persistieren oder welterzugeben siehen Designentscheidungen D-5.1-21			akzeptabel , mit Evaluation
	9- Hotline Mitarbeiter		Speicherung freiwilliger Angaben des Anrufers																		
			Verarbeitung nicht richtiger Daten		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 frür über synklatisch unrichtige leitFANs in dermiert wird. Sollten telei FANs bei der Schnittstelle als ungültig erkannt werden, ist dies entsprechend bei der Anthord der Schnittstelle berücksichtigt.			akzeptabel , mit Evaluation
	9- Hotline Mitarbeiter		Verarbeitung ungültiger/ unrichtiger teleTANs		Ja	2	2	2	2	0	0	0	2	4	4	8	DM, ZB, T	DSK Verifikations-holline 8.2.1 - Fehlerhafte Verarbeitungen in der Holline wellen protokolliert. Hierbei wird darauf geschiet nich die fachlichen personenbezogenen Daten zu protokollieren, sondern den anonymisierten fachlichen Arwendungsfall zur Fehlerandigee.			akzeptabel, mit Evalu
	19- Hotline Mitarbeiter		Fehlerhafte Verarbeitung  Verarbeitung über die Speicherfrist hinaus																		

Datenschutzfolgenabschätzung (DSFA) - VT 3: Verifikation Hotline (Stand: 13.06.) // Berichtigung RS-Fehler und Anpassungen in Spalte T am 24.07.2020 // Aktualisierung: 10.10.2020						Risikobewertung Schadensausmaß															
Prüfgegenstand/ Risikoursprung	Risiko-Quelle	Nr.		Betroffenengruppen (CWA-Nutzer, Nutzer anderer nat. Corona- Apps, Personen im Umfeld, Personen, die von Falschmeldungen Betroffen sein könnten). Soweit keine, Auswahl	Risikoverantwortlicher	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Vorfügbarkeit	Authentizität Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	etablierte Maßnahmen	geplante Maßnahmen	Bewertung, warum "rote" Risiken akzeptiert werden können	n Restrisiko
	R9- Hotline Mitarbeiter		Rufnummer wird nach Rückruf nicht sachgerecht entsorgt	Tonia dissam		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		akzeptabel , mit Evaluation
			Risiken durch Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt															DSK Verifikations-Hotline 8.2.1: Durch Input Validierung bzw. Ausgabebreinigung wird bereits vor der talsächlichen fachlichen Verarbeitung von Daten sichregestellt, dass keine fehlerhaften Daten im System gespichert werden bzw. aus dem System kommen.			
Allgemein																					