Datenschutzfolgenabschätzung (DSFA) -
VT 3: Verifikations-Hotline + Stellvertreterwarnung (02.09.2021)
(Stand: 02.09.2021)

				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
R9- Hotlinemitarbeiter	4	**1) 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	5	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
R9- Hotlinemitarbeiter	6	Stellvertreterwarnung: Datenverarbeitungen von Mitarbeiterdaten der GA ohne Rechtsgrundlage		Nein											-		Verantwortliche Stelle für die Weitergabe von Mitarbeiterdaten an die Hotline zur Aufgabenerfüllung (bsp. zur Amts- oder Verwaltungshilfe für das RKI) liegt bei GA. Diese sollte im geplanten Umfang erforderlich sein.			
R9- Hotlinemitarbeiter	7	[Release 2.9] Erhebung/ Speicherung nicht-notwendiger personenbezogener Daten (inkl. Erhebung Mobilfunknummer)	[Release 2.9] Stellvertreterwarnung: Ein Hotline-Mitarbeiter könnte die Namen und Kontaktdaten der Anrufer ohne Notwendigkeit erheben.	Ja	2	4	1	1	0	0	0	4	4	4	8	DM , IV, TR, ZB	Siehe Designentscheidungen D-5.1-21 (AVV).	Explizites Hinweis bei der Schulung der Hotline-Mitarbeiter, regelmäßige stichprobenhafte Überprüfung im Sinne von MysteryCalls.		akzeptabel, mit Evaluation
R9- Hotlinemitarbeiter	8	**2) Verarbeitung wider Treu und Glauben**																		
R1-CWA-Nutzer	9	Vorgetauschte Identität gegenüber Hotline + Vortäuschen positiver Testergebnisse		Ja	3	4	1	4	0	4	0	4	4	4	12	DM, IG, 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 Auftraggeber und werden regelmäßig geschärft.	Beschleunigte Anbindung der Labore. Mögliche Handlungsoptionen: Abgestuftes Verfahren zur Persistierung eines minimalen Sets an personenbezogenen Daten, um stichprobenhaft möglichen Missbrauch zu überprüfen. Prüfung alternativer Verifikationsprozesse.	Gemeinsame Entwicklung der Lösung im Workstream	bedingt (zeitlich) akzeptabel,
R8- Behörden	10	Stellvertreterwarnung: Falsche/ missbräuchliche Warnung für eine andere Veranstaltung + ausbleibende Warnungen	Die für den Prozess der Stellvertreterwarnungen benötigte TAN könnte *von GA-Mitarbeitern* versehentlich oder absichtlich zum Warnen für eine Veranstaltung genutzt werden, an dem keine Person teilgenommen hat, die positiv auf Corona getestet wurde. Dies könnte zu unnötigen Warnungen von CWA-Nutzern führen, die an einem Event teilgenommen haben, an dem keine positiv auf Corona getestete Person teilgenommen hat. Zudem könnte es passieren, dass die TAN, die wissentlich/unwissentlich zum Warnen für eine falsche Veranstaltung genutzt wurde, dann nicht mehr genutzt wird/werden kann, um ein Warnungen für die „richtige" Veranstaltung auszusprechen, an der tatsächlich eine positiv auf Corona getestete Person teilgenommen hat. Auch könnte ein Veranstalter wissentlich/unwissentlich zeitlich falsch zugeordnete Warnungen für seine Veranstaltung aussprechen, die dazu führen, dass für den Zeitraum, an dem eine positiv auf Corona getestete Person an seiner Veranstaltung teilgenommen hat, keine Warnungen an die anderen Teilnehmer (CWA Nutzer) ausgesprochen wird, wohl aber für solche Teilnehmer, die während eines anderen Zeitraums an der Veranstaltung teilgenommen haben, an dem eigentlich kein bekanntes Infektionsrisiko bestanden hat.	Ja	2	1	1	3	1	3	1	2	2	3	6	IG, AT, ZB		In der Dokumentation gegenüber dem GA sollte ein Hinweis aufgenommen werden, dass das Gesundheitsamt die Voraussetzungen der jeweiligen Weitergabe und des eigenen Vorgehens sicherstellen sollte (z. B. durch geeigneten Einsatz des Veranstalters als Verwaltungshelfer). Missbrauchskontrolle (ggf. Logging in Verantwortung der GA).		akzeptabel, mit Evaluation
R9- Hotlinemitarbeiter	11	Stellvertreterwarnung: Falsche/ Missbräuchliche Warnung für eine andere Veranstaltung	Die für den Prozess der Stellvertreterwarnungen benötigte PIW-TAN könnte absichtlich zum Warnen für eine Veranstaltung genutzt werden, an dem keine Person teilgenommen hat, die positiv auf Corona getestet wurde. Dies könnte zu unnötigen Warnungen von CWA-Nutzern führen, die an einem Event teilgenommen haben, an dem keine positiv auf Corona getestete Person teilgenommen hat.	Ja	1	1	1	3	1	1	1	2	2	3	3	IG, ZB		Explizites Hinweis bei der Schulung der Hotlinemitarbeiter. Logging zur Mißbrauchskontrolle im Auftrag des RKI (an welches GA wurde PIW-TAN herausgegeben), um nachvollziehen zu können, ob eine Weitergabe an GA in Missbrauchsfällen nicht erfolgte.		akzeptabel
	12	**3) Für die Betroffenen intransparente Verarbeitung**													0					
R9- Hotlinemitarbeiter	13	Unvollständige, unverständliche Datenschutzinformationen durch Hotline		Ja	2	0	0	0	0	0	0	4	4	4	8	TR, ZB, IG	Datenschutzinformationen für Hotline	Regelmäßige Überprüfung der Datenschutzinformationen auf Vollständigkeit, Verständlichkeit und Aktualität durch den Verantwortlichen.		akzeptabel , mit Evaluation
	14	**4) Unbefugte Offenlegung von und Zugang zu Daten**																		
R1-CWA-Nutzer	15	Unbefugte Weitergabe von teleTan nach Erhalt mittels Hotline (Gültigkeit 1h)		Ja	1	0	4	4	0	0	0	4	0	4	4	ZB, IG, VT, IV	Sensibilisierung der Nutzer durch Datenschutzinformationen.	Inhaltliche Belehrung des Nutzers und Hinweis auf mögliche Konsequenzen bei Zuwiderhandlung		akzeptabel
R9- Hotline Mitarbeiter	16	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)	17	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
R2- Hacker	18	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 gewährleisten: Es sollte ermöglicht werden, die Konfiguration der teleTAN-Länge über die signierten Konfigurationsparameter zu ändern, um sich auf entwickelnde Bedrohungen, an sich ändernde Situationen und Belastungen anzupassen.	Durch geplante Maßnahmen IT-Security akzeptabel	bedingt akzeptabel, mit Adressierung IT-Sicherheit,
R2- Hacker	19	Stellvertreterwarnung: Erschleichen von PIW-TAN zur Diskreditierung von Veranstaltungen/ Veranstaltern	Sofern ein Angreifer die Möglichkeit bekommt, eine PIW-TAN anzufragen, die er dann wissentlich/ absichtlich nutzt, um für falsche Veranstaltungen – also solche an denen keine Person teilgenommen hat, die positiv auf Corona getestet wurde – Warnungen an CWA-Nutzer zu veranlassen, könnte es dem Angreifer gelingen, der Veranstaltung oder den Veranstalter einen Reputationsschaden zuzufügen.	Ja	2	1	1	3	1	3	1	2	2	3	6	IG, AT, ZB		Authentifizierungprozess bei der Hotline (PIW-TAN nur nach Rückruf nach Prüfung der anrufenden Nummer mit einer hinterlegten Kopfnummer).		akzeptabel mit Evaluation
R2- Hacker	20	Stellvertreterwarnung: Ausspähen von PIW TAN um Stellvertreterwarnungen zu ermöglichen bzw. Ausspähen von Veranstaltungen, für die gewarnt werden soll ("shoulder surfing")	Ein Angreifer könnte versuchen durch „Shoulder surfing" (bei der Hotline, beim GA oder Veranstalter) und weitere Ablenkungsmanöver die TAN die zum Warnen für eine Veranstaltung genutzt werden soll beim Veranstalter abzugreifen/absculesen, um so unberechtigterweise für eine andere Veranstaltung eine Warnung aussprechen zu können. Auch könnte ein Angreifer versuchen dheraauszubekommen, für welche Veranstaltung ein Veranstalter im Kontext der Stellvertreterwarnung eine Warnung aussprechen möchte.	Ja	2	1	3	1	1	1	1	1	1	3	6	VT, ZB	Allgemeine Regeln zur Wahrung Vertraulichkeit bei DL und GA			akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA) -
VT 3: Verifikations-Hotline + Stellvertreterwarnung (02.09.2021)
(Stand: 02.09.2021)

				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
R2- Hacker	21	Stellvertreterwarnung: Re-Identifikation von Teilnehmern an einem Event	1.) Ein Angreifer könnte durch gezielte Warnungen für bestimmte Events herauszufinden, ob ein CWA-Nutzer an dem Termin teilgenommen hat oder nicht. Dies wäre möglich, indem er gezielt Warnungen für bestimmte Veranstaltungen veranlasst und das Smartphone des Nutzers beobachtet. Sollten dann Warnungen beim CWA-Nutzer eintreffen, wäre dies ein möglicher Hinweis für die Teilnahme an dem fraglichen Event. 2.) In bestimmten Konstellationen (kleines Event, kleine Lokalität, wenige Teilnehmer..) besteht auch bei Stellvertreterwarnungen das Risiko der Re-Identifikation von Teilnehmern	Ja	1	1	3	1	1	1	1	3	3	3	3	VT, IV, TR, ZB		CWA-Nutzer werden bereits gegenwärtig darauf hingewiesen, dass in bestimmten Konstellationen bei Warnungen ein Re-Identifizierungsrisiko besteht. Der Hinweis könnte etwas erweitert werden, um auch die Stellvertreter-Warnungen einzubeziehen.		akzeptabel
R9- Hotlinemitarbeiter	22	**5) Ungerechtfertigter Datentransfer in Drittland**		Ja	1	0	4	4	0	0	0	4	4	4	4	VT, IG, IV, TR, ZB	Siehe Designentscheidungen D-5.1-21 (Abschluss AVV, inkl. Verpflichtung auf Vertraulichkeit/ §203).			akzeptabel
R9- Hotlinemitarbeiter	23	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
R9- Hotlinemitarbeiter	24	**6) Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten**																		
R1-CWA-Nutzer	25	Verlust der 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 eine neue teleTan angefordert werden).			akzeptabel
R7-Labormitarbeiter/ Arzt (Berufsgeheimnisträger)	26	**7) 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.			
R9- Hotlinemitarbeiter	27	**8) 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 Hotline-Betreiber von der Pflicht befreit ist, Daten zu speichern.			akzeptabel
R9- Hotlinemitarbeiter	28	**9) 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 Evaluation
R9- Hotlinemitarbeiter	29	Speicherung freiwilliger Angaben des Anrufers		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 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
	30	**10) Verarbeitung nicht richtiger Daten**																		
R9- Hotlinemitarbeiter	31	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 teleTANs informiert wird. Sollten teleTANs bei der Schnittstelle als ungültig erkannt werden, ist dies entsprechend bei der Antwort der Schnittstelle berücksichtigt.			akzeptabel, mit Evaluation
	32	**11) Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler)**		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, mit Evaluation
	33	**12) Verarbeitung über die Speicherfrist hinaus**																		
R9- Hotlinemitarbeiter	34	Rufnummer wird nach Rückruf nicht sachgerecht entsorgt		Ja	2	4	4	0	0	0	0	4	4	4	8	VT, TR, ZB, DM, IG, IV	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
R9- Hotlinemitarbeiter	35	Stellvertreterwarnung: Rufnummer und Namen der anfragenden Mitarbeiter der Gesundheitsämter werden nicht sachgerecht entsorgt		Ja	2	4	4	0	0	0	0	4	4	4	8	DM, VT, IV, TR, ZB		keine Persistierung von Mitarbeiterdaten nach Rückruf		akzeptabel, mit Evaluation
	36	**13) Risiken durch Verarbeitung 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.			
	37																			