Risiko Analyse

							Risikobewertung																	
							Schadenshöhe																	
Risiko-quelle	ID	Bedrohung	Beschreibung des Risikos (optional)	Beschreibung des drohenden Schadens für Betroffene (siehe auch die Schadensszenarien im Tabellenblatt "Schadenskategorien")	Betroffenen-gruppen (CWA-Nutzer, Nutzer anderer nat. Corona-Apps, Personen im Umfeld, Personen, die von [illegible]	Schutzbedarf der Daten	Schwerwiegende (physisch)	Einschränkung (physisch)	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Rechtmäßigkeit	Intervenierbarkeit	Transparenz	Zweckbindung / Unverkettbarkeit	Risikowert / Risikoindex	Vorgesehene Risikominimierungsmaßnahmen (zu den allgemeinen Erwägungen siehe Abschnitte 13.2 und 15 Entwurf DPIA-Report)	Vorgesehene Maßnahmen	Geplante Maßnahmen	Bewertung, warum "rote" Risiken akzeptiert werden können (zu den allgemeinen Erwägungen der Risikoakzeptanz siehe Kap. 15 des EFGS_DPIA_Draft)	Restrisiko
	1	**Rechtswidrige Verarbeitung im Rahmen der europäischen Interoperabilitätslösung und Verletzung der Fairness-Voraussetzung, Art. 8 Grundrechte-Charta**																						
RB -staat. Behörden		Unklare Verantwortlichkeiten in Bezug auf die Datenverarbeitungen noch zu prüfen: Joint Controller Verträge durch Gesetz ersetzt, Joint Controller Verträge mit DIGIT notwendig (nennen der Unterauftragsverarbeiter von DIGIT)?	Zweck und Mittel der Datenverarbeitung werden nicht nur von den Verantwortlichen bestimmt.	Unverhältnismäßige, rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	4	4	4	4	4	4	4	4	4	4	Festlegung eindeutiger Verantwortlichkeiten für die gemeinsam Verantwortlichen, die Kommission und die Auftragsverarbeiter (gemäß bindender EU Entscheidung 2020/1023 und durch Abschluss der erforderlichen Verträge mit den Auftragsverarbeitern (Art. 28 DSGVO))				akzeptabel
RB -staat. Behörden		Datenverarbeitungen ohne Rechtsgrundlage wie beispielsweise einer wirksamen Einwilligung	Keine weitere Beschreibung erforderlich.	Unverhältnismäßige, rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	3	4	4	0	0	0	0	4	4	4	12	Design-Entscheidungen EFGS D-3-7 (Bewertung der Rechtmäßigkeit durch das eHealth Netzwerk); Aufnahmeprozedur, Zuständigkeit der Mitgliedsstaaten als gemeinsame Verantwortliche			siehe Anlage 7 zum DSFA-Bericht, Ziff. 2.3.2 (3) - Teilnahme am EFGS bedingt gewissen Vertrauen der joint controller	bezdingt akzeptabel
RB -staat. Behörden		**Datenverarbeitungen ohne Rechtsgrundlage: Jede Art von nochmaligem Upload durch empfangende nationale Backends auf EFGS Server. Weitere und von der ursprünglichen Datenverarbeitung zu unterscheidende Datenverarbeitung, die von Rechtsgrundlage nicht umfasst wird.**	**Ein nationales Backend lädt personenbezogene Daten vom EFGS herunter. Es kann sich hierbei auf die von dem die Daten erhebenden Mitgliedsstaat geschaffene Rechtsgrundlage berufen. Diese Rechtsgrundlage begründet jedoch nicht einen erneuten Upload durch das herunterladende nationale Backend.**	Unverhältnismäßige, rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	3	4	4	0	0	0	0	4	4	4	12	**Klare Trennung der Verarbeitungswege personenbezogener Daten in den nationalen Backends nach der Herkunft der Daten. Vorzugsweise werden die personenbezogenen Daten mit einem Herkunftskennzeichen während der Verarbeitung versehen.**			siehe Anlage 7 zum DSFA-Bericht, Ziff. 2.3.2 (3) - Teilnahme am EFGS bedingt gewissen Vertrauen der joint controller	bedingt akzeptabel
RB -staat. Behörden		Datenverarbeitungen durch das EFGS (speichern, übermitteln oder andere Datenverarbeitungen) nach dem Widerruf der Einwilligung	Verarbeitung von Diagnoseschlüsseln (Speichern, Herunterladen) trotz Widerruf einer Einwilligung, weil die Diagnoseschlüssel bereits auf das nationale Backend oder den EFGS hochgeladen worden sind.	Unverhältnismäßige, rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	4	4	4	0	0	0	0	4	0	4	12	Design-Entscheidungen EFGS D-3-9 (Widerruf der Einwilligung), D-8-1 (Löschung von Daten, wenn alle teilnehmenden Backend-Servder diese heruntergeladen haben oder 14 Tage nach Upload, der frühere Zeitpunkt ist maßgeblich). Die Löschung von Daten im EFGS ist auf Grund eines Widerrufs unmöglich, wenn die nationalen Backends die Daten übertragen haben, weil die Daten nicht erfolgbare Pseudonyme dersolben			siehe Anlage 7 zum DSFA-Bericht, Ziff. 2.3.2 (3) - Teilnahme am EFGS bedingt gewissen Vertrauen der joint controller	bedingt akzeptabel
RB -staat. Behörden		Nicht ausreichende Rechtsgrundlage gem. Art. 8 Grundrechte-Charta: Einwilligung oder gesetzliche Grundlage verstoßen gegen die Anforderungen an die Freiwilligkeit der Verarbeitung.	Keine weitere Beschreibung erforderlich.	Unverhältnismäßige, rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	4	4	0	0	0	0	4	0	4	8	Design-Entscheidungen EFGS D-3-7 (Bewertung der Rechtmäßigkeit durch das eHealth Netzwerk); Aufnahmeprozedur, Zuständigkeit der Mitgliedsstaaten als gemeinsame Verantwortliche				akzeptabel mit Evaluation
RS-Arbeitgeber, Versicherungen		Nicht ausreichende Rechtsgrundlage gem. Art. 8 Grundrechte-Charta: Einwilligung oder gesetzliche Grundlage verstoßen gegen die Anforderungen an die Freiwilligkeit der Verarbeitung.	Durch Zwang Dritter herbeigeführte Einwilligung. Die Wahrnehmung von Rechten und Opportunitäten wird von der Nutzung der Funktionen des EFGS abhängig gemacht.	Unverhältnismäßige, rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß. Ökonomische Nachteile.		3	yes	2	3	3	0	0	0	0	3	0	3	6	Zuständigkeit der Mitgliedsstaaten (Ausführung gesetzlicher Anordnungen)				akzeptabel mit Evaluation
RB -staat. Behörden		Nicht ausreichende Rechtsgrundlage gem. Art. 8 Grundrechte-Charta: Einwilligung oder gesetzliche Grundlage verstoßen gegen die Anforderungen an die Freiwilligkeit der Verarbeitung.	Keine weitere Beschreibung erforderlich.	Unverhältnismäßige, rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	4	4	0	0	0	0	4	0	4	8	Design-Entscheidungen EFGS D-3-7 (Bewertung der Rechtmäßigkeit durch das eHealth Netzwerk); Aufnahmeprozedur, Zuständigkeit der Mitgliedsstaaten als gemeinsame Verantwortliche				akzeptabel mit Evaluation
RB -staat. Behörden		Nicht ausreichende Rechtsgrundlage gem. Art. 8 Grundrechte-Charta: Einwilligung oder gesetzliche Grundlage verstoßen gegen die Anforderungen an die Transparenz der Rechtsgrundlage. Mögliche Intransparenz auf Grund des Fehlens oder der Unklarheit von Angaben über Zweck, Umfang, Verantwortliche oder notwendiger Details der Verarbeitung.	Keine weitere Beschreibung erforderlich.	Unverhältnismäßige, rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	4	4	0	0	0	0	4	0	4	8	Design-Entscheidungen EFGS D-3-7 (Bewertung der Rechtmäßigkeit durch das eHealth Netzwerk); Aufnahmeprozedur, Zuständigkeit der Mitgliedsstaaten als gemeinsame Verantwortliche				akzeptabel mit Evaluation
RB -staat. Behörden		Nicht ausreichende Transparenz der Aufklärung über die Verarbeitung, um eine informierte Einwilligung für die Datenverarbeitungen durch das EFGS zu erteilen (insbesondere Sprachbarrieren, zu technische Beschreibung/fehlendes technisches Verständnis des Betroffenen).	Keine weitere Beschreibung erforderlich.	Unverhältnismäßige, rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	4	4	0	0	0	0	4	0	4	8	Design-Entscheidungen EFGS D-3-7 (Bewertung der Rechtmäßigkeit durch das eHealth Netzwerk); Aufnahmeprozedur, Zuständigkeit der Mitgliedsstaaten als gemeinsame Verantwortliche				akzeptabel mit Evaluation
RB -staat. Behörden		Fehlende Einsichtsfähigkeit von Minderjährigen zur Abgabe wirksamer Einwilligungserklärung und daraus resultierend fehlende Rechtsgrundlage	Verarbeitung von Diagnoseschlüsseln unter 16 Jähriger in Mitgliedsstaaten ohne ausreichende rechtliche Grundlage.	Datenschutzverstoß. Negative soziale Auswirkungen auf Minderjährige, weil diese keine Einwilligung erteilen können oder negative Auswirkungen einer zu Unrecht erteilten Einwilligung.		3	yes	2	4	4	0	0	0	0	4	0	4	8	Design-Entscheidungen EFGS D-3-7 (Bewertung der Rechtmäßigkeit durch das eHealth Netzwerk), Design-Entscheidungen EFGS D-3-8 (Wahrung nationalen und europäischen Rechts - Mindestalter für Einwilligung); Zuständigkeit der Mitgliedsstaaten als gemeinsame Verantwortliche				akzeptabel mit Evaluation
R4- Apple / Google		Abhängigkeiten einer rechtskonformen Verarbeitung durch das EFGS und durch die Implkementierung in der CWA von den Eigenschaften des ENF, die von Apple und Google vorgegebenbestimmt werden und die Abhängigkeit von der Verfügbarkeit des ENF	Updates und neue Funktionen des ENF (d.h. Mitteilungen, neue Algorithmen zur Bewertung des Infektionsrisikos etc.) können zu Fehlfunktionen der bestehenden mobilen Applikation führen und Benutzer in die Irre leiten. Einschränkung der Verfügbarkeit.	Dauerhafte Nichtverfügbarkeit der Funktionen der Applikation. Verlust personenbezogener Daten und Gefühl des Verlusts der Privatsphäre. Datenschutzverstoß.		3	yes	3	3	3	0	3	0	3	3	3	3	9	Es ist eine Annahme des Designs des EFGS, dass die teilnehmenden Mitgliedsstaaten das Google/Apple Exposure Notification API (GAEN) verwenden (siehe Design-Entscheidungen EFGS D-1-8). Änderungen des EFGS müssen dokumentiert und kommuniziert werden, um die Möglichkeit zu schaffen, Nutzer über die Datenverwendung zu informieren und Empfehlungen für Einstellungen auszusprechen.				akzeptabel mit Evaluation
R4 - Software und Service Provider // SAP/ T		Abhängigkeit des Betriebs des EFGS von externen Dienstleistern (wie DIGIT und TSI)	Einschränkung oder Verlust der Verfügbarkeit der Datenverarbeitungsfunktionen (grenzüberschreitende Verteilung von Diagnoseschlüsseln).	Dauerhafte Nichtverfügbarkeit der Funktionen der Applikation. Verlust personenbezogener Daten und Gefühl des Verlusts der Privatsphäre. Datenschutzverstoß.		3	yes	1	3	3	0	3	0	3	3	3	3	3	Vertrag gemäß Art. 28 DSGVO und SLA für den Betrieb EFGS. Technische und organisatorische Maßnahmen für die Einrichtungen, die den EFGS hosten. Die Kommission muss Sicherheitsmaßnahmen nach aktuellem Stand der Technik in physischer und logischer Hinsicht für die Einrichtungen vorsehen, die den EFGS hosten. Außerdem müssen Sicherheitsmaßnahmen für den Datenzugriff und die Sicherheitseinrichtungen getroffen werden (Design-Entscheidungen EFGS T-II-9, Design-Entscheidungen EFGS T-II-10, Überwachung des Betriebs durch die EU-Kommission). Angewendete DIGIT Sicherheitsanweisungen für IT-Systeme:				akzeptabel
R4- Dienstleister Mitgliedstaaten		Abhängigkeit des Betriebs des EFGS von der Verfügbarkeit der Infrastruktur der nationalen Backends der Corona Warning Systeme der Mitgliedsstaaten	Einschränkung oder Verlust der Verfügbarkeit der Datenverarbeitungsfunktionen (grenzüberschreitende Verteilung von Diagnoseschlüsseln).	Dauerhafte Nichtverfügbarkeit oder Verlust personenbezogener Daten. Datenschutzverstoß.		3	yes	1	3	3	0	3	0	3	3	3	3	3	Design-Entscheidungen EFGS D-2-3, D-2-6, D-2-8, D-2-9: Die Mitgliedsstaaten sind für die Umsetzung der durch die Gesundheitsbehörden festgelegten Vorgehensweisen zuständig. Design-Entscheidungen D-2-1-3: Die Kommission unterstützt alle Funktionen des EFGS.				akzeptabel
R4- Apple / Google		Fehlende oder unzureichende vertragliche Grundlage (AVV oder Art. 26 Vertrag) zwischen dem Verantwortlichen (für Implementierung CWA und EFGS) und Apple/Google.	Zweck und Mittel der Datenverarbeitung werden nicht nur von den Verantwortlichen bestimmt.	Unverhältnismäßige, rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	no											0	Es ist kein Datenfluss vom EFGS zu Apple/Google vorgesehen. Vertragliche Regelungen sind nicht erforderlich. Es bestehen keine Beziehungen zwischen den Betreibern des EFGS und Apple/Google. Entsprechende Beziehungen sind Angelegenheiten der Mitgliedsstaaten.				
Software und Service Provider // SAP/ T		Fehlende oder unzureichende vertragliche Grundlage (AVV) zwischen den Verantwortlichen und externen Dienstleistern (wie DIGIT, SAP, TSI)	Zweck und Mittel der Datenverarbeitung werden nicht nur von den Verantwortlichen bestimmt.	Unverhältnismäßige, rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	3	3	3	3	0	3	3	3	3	3	Vertrag gemäß Art. 28 DSGVO, SLA (Betrieb EFGS und Hosting).				akzeptabel
R4- Apple / Google		Exzessive und unnötige Datenverarbeitungen durch die Betreiber des ENF und Betriebssystems (Apple/ Google) (siehe Z 32)	Verknüpfung personenbezogener Daten (Diagnoseschlüssel) mit Standortdaten und Benutzerdaten (Metadaten).	Reidentifikation, Profiling, Diskriminierung, Datenschutzverstoß, ökonomische Nachteile.		3	yes	3	4	4	4	0	0	0	4	4	4	12	Siehe Zeile 32			verweisen wird auf die Akzeptanz der Risiken, die auf der Entscheidung beruhen, auf das Framework von Apple/ Google zurück zu greifen. Siehe Z 32.	bedingt akzeptabel
Software und Service Provider // SAP/ T		Erhebung und Verarbeitung von veralteten, überflüssigen oder nicht benötigten personenbezogenen Daten durch Auftragsverarbeiter beim Betrieb des EFGS.	Verknüpfung personenbezogener Daten (Diagnoseschlüssel) mit Standortdaten und Benutzerdaten (Metadaten).	Reidentifikation und Datentransfer zu öffentlichen Einrichtungen. Datenschutzverstoß.		3	yes	1	4	4	4	0	0	0	4	4	4	4	Vertrag gemäß Art. 28 DSGVO, SLA (Betrieb EFGS) - technische und organisatorische Maßnahmen (Datenminimierung, Zweckbindung)				akzeptabel
Software und Service Provider // SAP/ T		Erhebung und Verarbeitung von veralteten, überflüssigen oder nicht benötigten personenbezogenen Daten durch Dienstleister, die den Betrieb des EFGS unterstützen.	Verknüpfung personenbezogener Daten (Diagnoseschlüssel) mit Standortdaten und Benutzerdaten (Metadaten).	Reidentifikation und Datentransfer zu öffentlichen Einrichtungen. Datenschutzverstoß.		3	yes	1	4	4	4	0	0	0	4	4	4	4	Vertrag gemäß Art. 28 DSGVO, SLA (Unterstützung Betrieb EFGS) - technische und organisatorische Maßnahmen (Datenminimierung, Zweckbindung) Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: ST_operational_mgt.doc, Logging and Monitoring security standard.pdf, ST_weblinking.doc, Access Control & Authentication security standard.doc				akzeptabel
R4- Dienstleister Mitgliedstaaten		Erhebung und Verarbeitung von veralteten, überflüssigen oder nicht benötigten personenbezogenen Daten durch Mitgliedsstaaten als gemeinsame Verantwortliche.	Verknüpfung personenbezogener Daten (Diagnoseschlüssel) mit Standortdaten und Benutzerdaten (Metadaten).	Reidentifikation und Datentransfer zu öffentlichen Einrichtungen. Datenschutzverstoß.		3	yes	1	4	4	4	0	0	0	4	4	4	4	Zuständigkeit der Mitgliedsstaaten				akzeptabel
R2- Hacker		Erhebung und Verarbeitung von personenbezogen Daten durch Drittstaaten.	Verknüpfung personenbezogener Daten (Diagnoseschlüssel) mit Standortdaten und Benutzerdaten (Metadaten).	Reidentifikation, Profiling, Diskriminierung, Datenschutzverstoß, ökonomische Nachteile.		3	yes	1	4	4	4	0	0	0	4	4	4	4					akzeptabel
	3	**Intransparente Verarbeitung**		Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.														0					
RB -public authorities (member states)		Nicht ausreichende Rechtsgrundlage gem. Art. 8 Grundrechte-Charta: Einwilligung oder gesetzliche Grundlage verstoßen gegen die Anforderungen an die Transparenz der Rechtsgrundlage. Mögliche Intransparenz auf Grund des Fehlens oder der Unklarheit von Angaben über Zweck, Umfang, Verantwortliche oder notwendiger Details der Verarbeitung.	Keine weitere Beschreibung erforderlich.	Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	3	0	0	0	0	0	3	3	0	6	Design-Entscheidungen EFGS D-4-3 (Datenschutzregelungen)	Entwurf einer EFGS Datenschutzerklärung.			akzeptabel mit Evalution
R4- Apple / Google		Intransparente Informationen über die Funktionsweise des Exposure Notification Framework der Plattformanbieter Apple und Google (unvollständige, nicht nachvollziehbare und nicht nachprüfbare Informationen).	Keine weitere Beschreibung erforderlich.	Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	3	0	0	0	0	0	0	3	3	0	9	Die Funktionsweise des ENF ist eine Angelegenheit des Betriebs der nationalen App.				akzeptabel mit Evaluation
Software und Service Provider // SAP/ T		Intransparente Information über die Funktionsweise des EFGS (ausgenommen die von Apple und Google bereitzustellen Leistungen).	Keine weitere Beschreibung erforderlich.	Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	0	0	0	0	0	0	3	3	0	6	Design-Entscheidungen EFGS D-4-1 (Datenschutzfolgeabschätzung, Datenschutzkonzepte, Designentscheidungen werden veröffentlicht) und D-4-2 (Transparenz und Bewertbarkeit - Open Source)				akzeptabel mit Evaluation
RB -staat. Behörden		Intransparente Funktionsweise der nationalen Backends einschließlich undokumentierter Funktionen.	Keine weitere Beschreibung erforderlich.	Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	3	0	0	0	0	0	3	3	0	6	Zuständigkeit der Mitgliedsstaaten				akzeptabel mit Evaluation
R4- Apple / Google		Unzureichende Prüfungsmöglichkeiten bezüglich der Verarbeitung in Apples und Googles Exposure Notification Framework und Apples und Googles Telemetrie-Überwachung.	Keine weitere Beschreibung erforderlich.	Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	3	3	3	0	0	0	0	3	3	3	9	Das Ausreichen der Überwachbarkeit wird von den Mitgliedsstaaten im Rahmen des Betriebs der nationalen App bewertet.				akzeptabel mit Evaluation
	4	**Nicht-autorisierte Offenbarung oder nicht-autorisierter Zugriff auf personenbezogene Daten**																					
R4- Apple / Google		Nicht-autorisierter und/oder unbekannter Zugriff auf personenbezogene Daten (einschließlich Infektionsstatus) durch die Anbieter des Exposure Notification Frameworks einschließlich Telemetrie.	Keine weitere Beschreibung erforderlich.	Verarbeitung für neue Zwecke, die von Apple und Google vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	3	4	4	4	0	0	0	4	0	4	12	Angemessenen Gegenmaßnahmen können auch in den nationalen Apps nicht ergriffen werden. Die Nutzer sollten informiert werden.			verweisen wird auf die Akzeptanz der Risiken, die auf der Entscheidung beruhen, auf das Framework von Apple/ Google zurück zu greifen. Siehe Designentscheidungen und Anlage 7 zum DSFA-Bericht. Veröffentlichungen über das "Ausspähen" durch Google werden zum Anlass genommen, die Risiken	bedingt akzeptabel
R2- Hacker		**Nicht-autorisierter Zugriff auf personenbezogene Daten durch nicht-autorisierter Zugriff auf den EFGS, dessen Betrieb und dessen Infrastruktur (Betroffenendaten und Protokolldaten).**	Im Falle eines die Sicherheit betreffenden Vorfalls kann ein Angreifer Zugriff auf die Datenbank erlangen und die dort gespeicherten Daten lesen. Dies kann zur Offenbarung von Protokolldaten an nicht-autorisierte Dritte und eine Behinderung der Rekonstruktion der Ereignisse, die die Zuweisung eines Infektionsstatus an einen bestimmten Eintrag bedingt haben, führen.	Verarbeitung für neue Zwecke, die vom Betreiber des EFGS vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	4	4	4	0	0	0	4	0	4	8	Design-Entscheidungen EFGS D-3.3-1 (EFGS verarbeitet nur stark pseudonymisierte Daten. Es ist nicht möglich, den Betroffenen zu identifizieren und zu diskriminieren). Protokolldaten werden durch das nationale Backend erhoben. Keine personenbezogenen Daten in den EFGS-Protokolldateien. Angreifer benötigen zusätzliche Informationen für die Reidentifikation. Zusätzlicherweise, Designs				akzeptabel mit Evaluation

Risiko Analyse

							Risikobewertung																
							Schadenshöhe																
Risiko-quelle	ID	Bedrohung	Beschreibung des Risikos (optional)	Beschreibung des drohenden Schadens für Betroffene (siehe auch die Schadensszenarien im Tabellenblatt "Schadenskategorien")	Betroffenen-gruppen (CWA-Nutzer, Nutzer anderer nat. Corona-Apps, Personen im Umfeld, Personen, die von [illegible]	Schutzbedarf der Daten	Schwerwiegende (physisch)	Einschränkung Grundrechte	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Interoperabilität	Transparenz	Zweckbindung / Unverkettbarkeit	Risikoindex / Risikoindex	Vorgesehene Risikominimierungsmaßnahmen (zu den allgemeinen Erwägungen siehe Abschnitte 13.2 und 15 Entwurf DPIA-Report)	Vorgesehene Maßnahmen	Geplante Maßnahmen	Bewertung, warum "rote" Risiken akzeptiert werden können (zu den allgemeinen Erwägungen der Risikoakzeptanz siehe Kap. 15 des EFGS_DPIA_Draft)	Restrisiko
R2-Hacker		Nicht-autorisierter Zugriff auf personenbezogene Daten durch das Überwachen von WIFI- oder Internetdatenverkehr: Netzwerküberwachung des Datenverkehrs zwischen nationalem Backend und dem EFGS.	Ein Angreifer könnten den Datenverkehr zwischen nationalem Backend und dem EFGS abhören (Netzwerkkommunikation, Upload/Download der Diagnoseschlüssel) um Daten zu erheben, speichern und auszuwerten.	Verarbeitung für neue Zwecke, die von Dritten/Kriminellen vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	4	4	4	0	0	0	4	0	4	8	Pseudonymisierung der übertragenen personenbezogenen Daten (siehe Zeile 31). Design-Entscheidungen EFGS D-5.1-2 (Übertragung von Pseudonymen), D-5.1-3 (Die gesamte Netzwerkkommunikation sollte verschlüsselt sein), D-5.1-4, Design-Entscheidungen EFGS T-1-3 (TLS) Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: Transport Layer Security technical standard.pdf, Access Control & Authentication security standard.pdf				akzeptabel mit Evaluation
R2-Hacker		Verknüpfung von Metadaten.	Nicht-autorisierte Reidentifikation eines Betroffen durch die Kombination verfügbarer Metadaten. Durch die Auswertung von Mustern der Daten des relevanten-Länder-Feldes kann es möglich sein, folgende Informationen zu ermitteln: 1. relevante Länder, die einen Bezug zu einem Schlüssel aufweisen, 2. Ursprungsland des Schlüssels, 3. Heatmap: Die Bürger welchen Mitgliedsstaates reisen in welche anderen Mitgliedsstaaten (statistische Daten).	Verarbeitung für neue Zwecke, die von Dritten/Kriminellen vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	3	3	3	0	0	0	0	3	0	3	9	Design-Entscheidungen EFGS D-5.1-2 (Übertragung von Pseudonymen), D-5.1-3 (Die gesamte Netzwerkkommunikation sollte verschlüsselt sein)				akzeptabel mit Evaluation
R2-Hacker		Offenbarung der Anzahl der relevanten Länder eines Daten zur Verfügung stellenden Betroffenen (Kodierfänge einer hochgeladenen Zeichenkette).	Eine Kodierung des Felds "relevante Länder" als variable Zeichenkette kann zur Offenbarung von Informationen führen, z.B. bezüglich des Reiseverhaltens des Betroffenen auf Grund der Erkennbarkeit der Anzahl der Länder, die der Betroffene als relevant angibt.	Verarbeitung für neue Zwecke, die von Dritten/Kriminellen vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	1	4	4	0	0	0	4	4	4	4		Die Verwendung einer Zeichenkette fester Länge zur Darstellung der relevanten Länder mitigiert dieses Risiko.			akzeptabel
R2-Hacker		Reidentifikation eines Betroffenen durch die Verknüpfung von Angaben zu relevanten Ländern mit externen Informationen über das Reiseverhalten.	Das Datenfeld "relevante Länder" kann zur Reidentifikation eines Betroffenen verwendet werden, wenn die Kombination der relevanten Länder hinreichend einmalig ist. Wird diese Information mit weiteren Informationen kombiniert, die außerhalb des Anwendungsbereiche des EFGS gewonnen werden, z.B. durch Fluggesellschaften oder Reisebüros oder statistische Informationen bezüglich der möglichen Ethnie des Betroffenen, können weitere personenbezogene Informationen	Verarbeitung für neue Zwecke, die von Dritten/Kriminellen vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	3	1	4	4	0	0	0	4	4	4	12		Mögliche Gegenmaßnahmen: Hinzufügen zufälliger nicht EU-Staaten beim Upload vom nationalen Backend. Dies wird einen kleinen Overhead entstehen lassen, da die Anzahl der Empfänger für diese Schlüssel sehr klein ist, aber es würde die Zuordnung von Schlüsseln erschweren, die die Liste der Länder		keine Implementierung in CWA - siehe Anlage 7 zum DSFA-Bericht Ziff. 2.3.2 (1)	bedingt akzeptabel
R2-Hacker		Nicht-autorisierter Zugriff auf personenbezogene Daten (hier: relevante Länder) durch das Überwachen von Internetverkehr beim Download.	Das Datenfeld "relevante Länder" kann als URL-Bestandteil eventuell für Dritte beim Download von Daten mittels der App erkennbar sein, wenn die Dritten den Datenverkehr der App gezielt abhören.	Verarbeitung für neue Zwecke, die von Dritten/Kriminellen vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	3	2	2	2	0	0	0	2	0	2	6	Design-Entscheidungen EFGS D-5.1-2 (Übertragung von Pseudonymen), D-5.1-3 (Die gesamte Netzwerkkommunikation sollte verschlüsselt sein), D-5.1-4				akzeptabel mit Evaluation
R2-Hacker		Nicht-autorisierter Zugriff auf personenbezogene Daten (hier: relevante Länder) durch das Überwachen von Internetverkehr beim Download.	Die Vorlegen von Reisetätigkeit eines Betroffenen an sich kann durch das Herunterladen von Schlüsseln erschlossen werden, wenn die heruntergeladenen Daten aufgestellt werden, um nicht die Mobiltelefone im Allgemeinen mit dem Download aller Daten von EFGS zu überlasten. Genauer: Wenn ein Benutzer kürzlich beispielsweise Italien besucht hat, ist es sehr wahrscheinlich, dass sie die mobile Applikation so einstellen, dass die italienischen Schlüssel heruntergeladen	Verarbeitung für neue Zwecke, die von Dritten/Kriminellen vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		2	yes	4	2	2	2	0	0	0	2	2	2	8		Mögliche Gegenmaßnahmen: - Feste Größe der Download-Pakete für die nationalen Backends - Eine Form der Längenanpassung kann hier erforderlich sein - Herunterladen aller Schlüssel in allen Nutzungsfällen			akzeptabel mit Evaluation
R2-Hacker		Nicht-autorisierter Zugriff durch Vornahme einer SQL-Code Injektion.	Nicht-autorisierter Zugriff mittels einer Code-Injektion in unspezifizierte Datenstrukturen.	Verarbeitung für neue Zwecke, die von Dritten/Kriminellen vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	4	4	4	0	0	0	4	0	4	4	Design-Entscheidungen EFGS D-5.1-2 (Übertragung von Pseudonymen), D-5.1-3 (Die gesamte Netzwerkkommunikation sollte verschlüsselt sein)	Eine Form der Längenanpassung kann hier erforderlich sein			akzeptabel
R2-Hacker		Sonstige Code-Injektionen in den EFGS.	Nicht-autorisierter Zugriff mittels einer Code-Injektion in unspezifizierte Datenstrukturen, die anschließend verarbeitet werden (Tomcat, Load Balancer).	Verarbeitung für neue Zwecke, die von Dritten/Kriminellen vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	4	4	4	0	0	0	4	0	4	4	Design-Entscheidungen EFGS D-5.1-2 (Übertragung von Pseudonymen), D-5.1-3 (Die gesamte Netzwerkkommunikation sollte verschlüsselt sein)	Herunterladen aller Schlüssel un allen Nutzungsfällen			akzeptabel
R2-Hacker		Kaperm von Transaktionen (Aufschalten auf aktive Uploads von Schlüsseln).	Nicht-autorisierte Offenbarung von Diagnoseschlüsseln.	Verarbeitung für neue Zwecke, die von Dritten/Kriminellen vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	4	4	4	0	0	0	4	0	4	4	Design-Entscheidungen EFGS D-5.1-2 (Übertragung von Pseudonymen), D-5.1-3 (Die gesamte Netzwerkkommunikation sollte verschlüsselt sein), D-5.1-4	Verwendung von vorgetäuschten Herunterladevorgängen.			akzeptabel
Software und Service Provider // SAPI 7		Nicht-autorisierter Zugriff durch Administratoren auf EFGS-Daten.	Die Datenbankadministratoren des EFGS könnten die EFGS Datenbanken manipulieren, da sie unbeschränkten Zugriff auf die Datenbanken haben. Sie können Metadaten der Datenbank verändern, da die Metadaten nicht durch einen Dritten signiert worden sind.	Verarbeitung für neue Zwecke, die von Dritten/Kriminellen vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	4	4	4	4	4	4	4	0	4	4	Verpflichtung des Betriebspersonals per Vertrag (Art. 28 DSGVO) und Implementierung angemessener technischer und organisatorischer Maßnahmen um Zugriffskontrolle sicherzustellen und nicht-autorisierte Zugriffe auszuschließen. Design-Entscheidungen EFGS T-2-4 (Autorisierte Personal).				akzeptabel
Software und Service Provider // SAPI 7		Unzureichende Kontrolle über den Zugriff auf gespeicherte Daten oder Datenverteilungseinrichtungen wie zum Beispiel fehlende Zugriffskontrolle, Fehlkonfiguration von Zugriffskontrollsystemen oder Funktionsstörungen von Zugriffskontrollsystemen.	Nicht-autorisierter Zugriff von Insidern oder Außenseitern.	Verarbeitung für neue Zwecke, die von Dritten/Kriminellen vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	4	4	4	4	4	4	4	4	4	8	Implementierung angemessener technischer und organisatorischer Maßnahmen um ausreichende Beherrschbarkeit sicherzustellen. Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: Access Control & Authentication security standard.pdf, Logging and Monitoring security standard.pdf				akzeptabel mit Evaluation
	5	**Nicht-autorisierte Übermittlung von personenbezogenen Daten**																					
Software und Service Provider // SAPI 7		Beabsichtigte oder unbeabsichtigte Übermittlung von personenbezogenen Daten durch das EFGS an einen nicht-berechtigten Empfänger.	Auf grund einer Fehlfunktion des EFGS kann dieses Daten an einen falschen Empfänger an Stelle des richtigen nationalen Backends übertragen.	Verlust der Vertraulichkeit, Datenschutzverstoß.		3	yes	2	2	1	0	0	0	2	2	2	2	4	Design-Entscheidungen EFGS T-4-4 (Beschreibung); Design des EFGS sollte die Risiken minimieren.				akzeptabel
R4- Apple / Google		Beabsichtigte oder unbeabsichtigte Übermittlung personenbezogener Daten durch Dienstleister wie Apple oder Google und Drittbasten auf Grund von Telemetrie-Überwachung, Fehlfunktionen oder nicht offenbarter Zugriffsmöglichkeiten (Zeilen 20, 32).	Reidentifikation mittels Profiling durch Kombination mit anderen verfügbaren Daten.	Datenschutzverstoß.		3	yes	3	4	4	4	0	0	0	4	4	4	12	Siehe Zeile 32			siehe Zeile 32	bedingt akzeptabel
Software und Service Provider // SAPI 7		Intentional or unintentional transfer of personal data by processors (operators of EFGS, supporters of EFGS' operators) to third party state actors (+ combination with further personal data). Beabsichtigte oder unbeabsichtigte Übermittlung personenbezogener Daten durch Auftragsverarbeiter (Betreiber des EFGS, Dienstleister der Betreiber des EFGS) oder Drittbasten (in Kombination mit weiteren	Risiko der Beschlagnahme durch eine staatliche Einrichtung. Eine Reidentifikation wäre nur mit zusätzlichen Informationen möglich.	Datenschutzverstoß.		3	yes	2	1	4	4	0	0	0	1	4	4	8	Verpflichtung des Betriebspersonals per Vertrag (Art. 28 DSGVO) und Implementierung angemessener technischer und organisatorischer Maßnahmen um Die Kontroller über Datenübertragungen sicherzustellen. Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: Access Control & Authentication security standard.pdf, Logging and Monitoring security standard.pdf				akzeptabel mit Evaluation
	6	**Unbeabsichtigter Verlust oder Beschädigung personenbezogener Daten**																					
Software und Service Provider // SAPI 7		Verlustbeschädigung von Diagnoseschlüsseln.	Unerwarteter Verlust oder unerwartete Löschung personenbezogener Daten im EFGS mit in Folge aufretendes Nicht-Verfügbarkeit der Daten für die nationalen Backends. Die Speicherung und Bereitstellung der Daten kann gestört werden, hochgeladerne Daten werden dann nicht richtig gespeichert oder die Daten werden nicht korrekt bereitgestellt.	Datenschutzverstoß.		3	yes	2	1	3	3	3	0	3	3	3	3	6	EFGS Design-Entscheidungen D-3-1 (Löschung der Daten), wenn alle teilnehmenden Backend-Server diese heruntergeladen haben oder 14 Tage nach Upload, der frühere Zeitpunkt ist maßgeblich). und Fehlermeldungen vorsehen, um festzustellen, ob erneute Uploads oder ähnliche Maßnahmen erforderlich sind. Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: ST_operational_mgt.doc, Backup security standard.pdf				akzeptabel mit Evaluation
	7	**Missachtung von Betroffenenrechten**																					
RB- staatl. Behörden		Bereitstellung nicht ausreichender Mittel durch die verantwortlichen Mitgliedsstaaten zur Erfüllung von Betroffenenrechten.	Betroffenenrechte werden missachtet und nicht von den Betroffenen durchgesetzt.	Rechtswidrige, nicht-intervenierbare Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	3	3	0	0	0	0	4	3	0	4	Design-Entscheidungen EFGS D-8-5 (Verantwortlichkeit jedes Verantwortlichen für Verfangen von Betroffenen).				akzeptabel
RB- staatl. Behörden		Nichtbearbeitung von Anfragen von Betroffenen bezüglich ihrer Betroffenenrechte.	Betroffenenrechte werden missachtet und nicht von den Betroffenen durchgesetzt. Die Datenverarbeitung wird fortgesetzt.	Rechtswidrige, nicht-intervenierbare Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	3	3	0	0	0	0	4	3	0	4	Design-Entscheidungen EFGS D-8-5 (Verantwortlichkeit jedes Verantwortlichen für Verfangen von Betroffenen).				akzeptabel
RB- staatl. Behörden		Nicht-Erfüllung von Betroffenenrechten bezüglich Widerruf von Einwilligungen, Löschung, Berichtigung, Einschränkung der Verarbeitung und Datenübertragbarkeit bezogen auf personenbezogene Daten (keine Verpflichtung der Herstellung des Bezugs der Schlüssel zu einer Person).	Betroffenenrechte werden missachtet und nicht von den Betroffenen durchgesetzt. Die Datenverarbeitung wird fortgesetzt.	Rechtswidrige, nicht-intervenierbare Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	3	3	0	0	0	0	4	3	0	4	Design-Entscheidungen D-3-9 (Im Ergebnis sind auf Grund Art. 11 Abs. 2, 12 Abs. 2 DSGVO, und Art. 12 Abs. 2, 14 Abs. 2 EUGDPR die Regelungen über Betroffenenrechte im Rahmen des EFGS nicht anzuwenden).				akzeptabel
Software und Service Provider // SAPI 7		Unzureichende, unsichere Löschung von personenbezogenen Daten, die veraltet oder überflüssig geworden sind, durch das EFGS oder die weiteren Datenverarbeitungsschriftte der gemeinsam verantwortlichen Mitgliedsstaaten.	Das Risiko einer Reidentifikation eines Betroffenen steigt mit der Dauer der Speicherung personenbezogener Daten.	Rechtswidrige Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	3	3	3	3	0	3	3	3	3	3	Design-Entscheidungen D-9-1 (Löschung der Daten, wenn alle teilnehmenden Backend-Server diese heruntergeladen haben oder 14 Tage nach Upload, der frühere Zeitpunkt ist maßgeblich).				akzeptabel
R4- Apple / Google		Unzureichende, unsichere Löschung von personenbezogenen Daten, die veraltet oder überflüssig geworden sind, durch das Exposure Notification Framework von Apple und Google.	Das Risiko einer Reidentifikation eines Betroffenen steigt mit der Dauer der Speicherung personenbezogener Daten.	Rechtswidrige Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	4	0	0	0	0	0	0	0	0	8	Das Ausreichen der Löschprozeduren im Verhältnis zu Apple und Google ist Angelegenheit der Mitgliedsstaaten.				akzeptabel mit Evaluation
	8	**Verarbeitung von personenbezogenen Daten für neue oder anderweitige Zwecke**																					
RB- staatl. Behörden		Modifikation oder Wechsel des Zwecks der Verarbeitung im Rahmen der nachfolgenden Verarbeitung durch die Mitgliedsstaaten oder Missachtung des ursprünglichen Zwecks.	Durch das Einführen von Analysemöglichkeiten in nationale mobile Applikationen wird ein Risiko begründet, dass Daten außerhalb des mittels des EFGS verfolgten Zwecks verarbeitet werden. Dieses Risiko ist nicht unmittelbar auf den EFGS bezogen.	Datenschutzverstoß.		3	no											0	**Design-Entscheidungen EFGS D-3-1 (Die nationalen Gesundheitsbehörden bestimmen die Schranken des Verarbeitungszwecks), D-3-2, D-3-3. Keine Angelegenheit des EFGS.**				
RB- staatl. Behörden		**Anfänglicher oder späterer Missbrauch des Parameters "Transmission Risk Level".**	**Dieser Parameter kann von den Mitgliedsstaaten unterschiedlich verwandt werden. Auf Grund der erwarteten Abtönung des Datenfelds kann es zur Übertragung beliebiger Daten verwendet werden.**	Datenschutzverstoß.		3	yes	3	0	0	0	0	0	0	3	3	3	9	Weiterzuverteilende Diagnoseschlüssel werden in den nationalen Backends vor der Verteilung an die Apps normalisiert.				akzeptabel mit Evaluation
Laborärzte / Arzt (Berufsgenossenschaft)		Mißbrauch der über das EFGS gestellten personenbezogenen Daten zur Durchsetzung und Sanktionierung von Maßnahmen zur sozialen Distanzierung, der Quarantänesicherung und/oder Einschränkungen der Bewegungsfreiheit.	Dieses Risiko wird durch die nationale mobile Applikation begründet und bestimmt. Es kann nicht unmittelbar dem EFGS zugerechnet werden.	Datenschutzverstoß.		3	no											0	**Design-Entscheidungen EFGS D-1-5 (Keine Verwendung für die Überwachung von Quarantäne-Maßnahmen). Keine Angelegenheit des EFGS.**				
RB- kommerzielle Datensammler		Mißbrauch der über das EFGS gestellten personenbezogenen Daten für andere kommerzielle oder interne Zwecke von Dritten.	Dieses Risiko wird durch die nationale mobile Applikation begründet und bestimmt. Es kann nicht unmittelbar dem EFGS zugerechnet werden.	Datenschutzverstoß.		3	no											0	Die Mitgliedsstaaten überwachen die Einhaltung der Freiwilligkeitsbedingungen abhängig vom nationalen Gesetzesrecht. Keine Angelegenheit des EFGS.				
RB- Arbeitgeber, Versicherungen		Benachteiligung von Betroffenen auf Grund der Nicht-Benutzung von Daten, die über das EFGS gestellt werden, oder auf Grund des Nicht-Teilens personenbezogener Daten mittels des EFGS.	Der Zugang zu Beschäftigungsmöglichkeiten, die Ausübung von Rechten und die Nutzung von öffentlichen Einrichtungen wird von der Benutzung der Funktionalität des EFGS abhängig gemacht.	Umweltbilanzmäßige, rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß. Ökonomische Nachteile.		3	yes	2	3	3	0	0	0	0	3	0	3	6	Die Mitgliedsstaaten überwachen die Einhaltung der Freiwilligkeitsbedingungen und der Zweckbindung abhängig vom nationalen Gesetzesrecht. Keine Angelegenheit des EFGS.				akzeptabel mit Evaluation
R4- Apple / Google		Mißbrauch der über das EFGS gestellten Daten durch Kombination mit Standortdaten und weitergehende Verwendung zu kommerziellen Zwecken.	Dieses Risiko wird durch die nationale mobile Applikation begründet und bestimmt. Es kann nicht unmittelbar dem EFGS zugerechnet werden.	Datenschutzverstoß.		3	no											0	**Design-Entscheidungen EFGS D-1-7 (Keine Bestimmung des Standorts des Betroffenen). Keine Angelegenheit des EFGS.**				
Software und Service Provider // SAPI 7		Reidentifikation von Betroffenen auf Grund bei der Benutzung von Telekommunikationseinrichtung anfallender Daten (z.B. Übertragungsprotokolle, Tyvisierung von Datenverkehr etc.).	Aufgrund nicht bestehender oder fehlender Isolierung von Komponenten des EFGS untereinander wird einem Angreifer der Zugriff auf weiterstehende Systemeinrichtungen ermöglicht.	Datenschutzverstoß.		3	yes	1	3	3	0	0	0	0	0	0	3	3	Trennung von System-Komponenten - DIGIT-Standard				akzeptabel

Risiko Analyse

							Risikobewertung																	
							Schadenshöhe																	
Risiko-quelle	**ID**	**Bedrohung**	**Beschreibung des Risikos (optional)**	**Beschreibung des drohenden Schadens für Betroffene (siehe auch die Schadensszenarien im Tabellenblatt "Schadenskategorien")**	**Betroffenen-gruppen (CWA-Nutzer, Nutzer anderer nat. Corona-Apps, Personen im Umfeld, Personen, die von**	**Schutzbedarf der Daten**	**Schwachstelle (physisch)**	**Einsatzmöglichkeit (physisch)**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Rechtmäßigkeit**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Unverkettbarkeit**	**Risikowert / Risikoindex**	**Vorgesehene Risikominimierungsmaßnahmen (zu den allgemeinen Erwägungen siehe Abschnitte 13.2 und 15 Entwurf DPIA-Report)**	**Vorgesehene Maßnahmen**	**Geplante Maßnahmen**	**Bewertung, warum "rote" Risiken akzeptiert werden können (zu den allgemeinen Erwägungen der Risikoakzeptanz siehe Kap. 15 des EFGS_DPIA_Draft)**	**Restrisiko**
RI-Nutzer		Offenbarung von Betroffenenidentitäten auf Grund Mitteilungen an den Betroffenen.	Risiko der Veröffentlichung personenbezogener Daten.	Datenschutzverstoß.		3	no											0	Das Risiko wird durch die die Mitgliedsstaaten und deren nationale Apps bestimmt. Kein weiteres Risiko durch das EFGS.					
R2-Hacker		Reidentifikation von Betroffenen auf Grund der Erstellung von Bewegungsprofilen des Betroffenen.	Risiko der Ermöglichung von Profiling. Weitere Zusatzinformationen werden benötigt.	Datenschutzverstoß.		3	yes	1	4	4	4	0	0	0	4	4	4	4	Design-Entscheidungen EFGS D-5.1-2 (Übertragung von Pseudonymen), D-5.1-3 (Die Netzwerkkommunikation sollte verschlüsselt erfolgen).					akzeptabel
RB- staatl. Behörden		Reidentifikation von Betroffenen auf Grund der Abfrage der relevanten Länder: Erzeugung einer Reisehistorie, Reidentifikation auf Grund der Einmaligkeit der Reisehistorie oder weiterer Daten, die staatlichen Einrichtungen zur Verfügung stehen (siehe Zeilen 36 bis 39).	Siehe Zeilen 36 bis 39.	Datenschutzverstoß.		3	yes	1	2	2	0	0	0	0	2	0	2	2	Die konkrete Implementation wird noch diskutiert. Die Wahlmöglichkeiten des Benutzers hängen von der Konfiguration der nationalen Backends ab. Das Traveller Pattern der Anbieter Google/Apple wurde für die Europäische Union nicht akzeptiert (Wenn der Status "traveller" zutrifft, werden alle Diagnoseschlüssel mit allen Ländern geteilt). Das begründet Problemstellungen bezüglich der Verwendung der Daten. Eine Implementation, die eine statische Länge des übertragenen Werts vorsieht, um Ähgreifern keine Informationsgewinnung zu ermöglichen, wurde vorgeschlagen.					akzeptabel
R2-Hacker		**Herstellung eines "Ausländerscanners".**	**Reidentifikation von Nutzern von mobilen Applikationen aus Drittstaaten auf Grund der Kennzeichnung der Herkunft der Diagnoseschlüssel: Ein Angreifer kann die RPI nach einem Kontakt ableiten und auf Grund der Herkunftsinformation der Diagnoseschlüssel Informationen bezüglich der Nationalität eines Kontakts ableiten.**	Datenschutzverstoß. Diskriminierung		3	yes	3	2	2	0	0	0	0	2	0	2	6	**Design-Entscheidungen EFGS (Normalisierung)**					akzeptabel mit Evaluation
	9	**Verarbeitung zufälliger, unerwarteter oder beiläufig anfallender Daten**																						
Software und Service Provider // SAP/ T		Verarbeitung verfälschter oder überflüssiger personenbezogener Daten (z.B. Daten, die bei der Benutzung von Telekommunikationseinrichtungen beiläufig anfallen).	Verknüpfung von personenbezogenen Daten (Diagnoseschlüssel) mit Standortdaten und Benutzerdaten (Metadaten).	Unverhältnismäßige rechtswidrige Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	4	4	0	0	0	4	4	4	4	8	Design-Entscheidung EFGS D-3-9 (Design setzt das Prinzip der Datenminimierung durch Verminderung der Korrelation zwischen Pseudonymen und Identitäten der Betroffenen um).					akzeptabel mit Evaluation
RB- staatl. Behörden		Unzulässige Verarbeitung personenbezogener Daten, die bei der Nutzung der nationalen Warnapplikation beiläufig anfallen können, z.B. Speicherausätze auf Grund von Programmabbrüchen.	Verknüpfung von personenbezogenen Daten (Diagnoseschlüssel) mit Standortdaten und Benutzerdaten (Metadaten).	Unverhältnismäßige, rechtswidrige Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	2	2	0	0	0	0	0	0	2	2	Das Risiko wird durch die nationale App bestimmt. Kein weiteres Risiko durch EFGS.					akzeptabel
	10	**Verarbeitung unzutreffender personenbezogener Daten**																						
RI-Nutzer		Upload von falsch-positiven Ergebnissen auf Grund unzureichender Zuverlässigkeit der Prüfmechanismen des Bestehens einer Infektion (Mißbräuchlicher Upload nicht-infektiöser Diagnoseschlüssel, Injektion unzutreffender Testresultate).	Länder mit schwächeren Mechanismen zur Überprüfung einer Infektion mit SARS-CoV-2 können eine große Anzahl unzutreffend als infiziert bezeichneter Schlüssel an das EFGS übertragen. Schwächere Mechanismen können z.B. in der Verwendung eines einzigen bekannten Codes zur Infektionsmeldung für eine Testeinrichtung bestehen.	Selbstbeschränkung in der Ausübung von Grundrechten und Datenschutzverstösse. Verlust des Vertrauens in die Vertraulichkeit und Integrität von		3	yes	4	4	2	4	0	0	0	4	4	4	16	Design-Entscheidungen EFGS D.2.3.4 (Überprüfung eines positiven Testergebnisses durch Gesundheitsbehörde)	T-1-4: (Filterung von Diagnoseschlüsseln - nicht klar), T-2-1 (Injektion falscher Testresultate) // Die durch die nationale Gesundheitsbehörde erstellten Condeas sollten nur einmalig benutzt werden und pseudo-zufällig sein. Dies stellt sicher, dass sie nicht mehrfach durch Angreifer zur Verfälschung des		bei Implementierung in CWA mitgiert (siehe Anlage 7 zum DSFA-Bericht Ziff.2.3.2 (2)	bedingt akzeptabel
RI-Dienstleist er Mitgliedsstaaten		**Mutwilliger Upload von falsch-positiven Schlüsseln durch eine staatliche Einrichtung, die berechtigter Weise an den EFGS angeschlossen war.**	Ein Angreifer, der Zugang zu einem nationalen Backend erlangt, kann dieses Nutzen, um über den EFGS durch den Angreifer generierte Diagnoseschlüssel zu verteilen. Der EFGS ist nicht in der Lage, festzustellen, ob ein nationales Backend in feindlicher Absicht betrieben wird.	Selbstbeschränkung in der Ausübung von Grundrechten und Datenschutzverstösse. Verlust des Vertrauens in die Vertraulichkeit und Integrität von		3	yes	1	4	4	4	0	0	0	4	4	4	4	DoS-Maßnahmen des EFGS verhindern DoS-Angriffe. Design-Entscheidungen EFGS T-2-3 (Sicherheitsstandards, Filterung). T-2-5. Um die EFGS-Datenbank gegen den Import nicht-autorisierter Daten zu schützen, werden die hochgeladenen Daten von den nationalen Backends signiert. Der Server überprüft die Signatur des Datenpackets anhand von Zertifikaten.					akzeptabel
RI-Dienstleist er Mitgliedsstaaten		Verteilung fehlerhafter Daten durch das EFGS auf Grund von Uploads durch berechtigter Weise angeschlossene nationale Backends.	Ein Angreifer könnte die Identität eines nationalen Backends oder des EFGS annehmen, um Daten an die nationalen Backends zu verteilen.	Selbstbeschränkung in der Ausübung von Grundrechten und Datenschutzverstösse. Verlust des Vertrauens in die Vertraulichkeit und Integrität von		3	yes	1	3	3	3	0	3	0	0	0	0	3	Design-Entscheidungen EFGS T-1-1 (Nutzung von Algorithmen zur digitalen Signatur)					akzeptabel
RI-Dienstleist er Mitgliedsstaaten		Manipulation personenbezogener Daten in der EFGS Infrastruktur durch Dienstleister.				3	yes	2	3	3	3	0	0	0	0	0	3	6	Vertrag mit Dienstleister (Art. 28 DSGVO) und technische und organisatorische Maßnahmen.					akzeptabel mit Evaluation
R2-Hacker		Manipulation personenbezogener Daten in der EFGS Infrastruktur durch außenstehende Angreifer.	Vorsätzliche Veränderung von Informationen - Diagnoseschlüssel können verfälscht werden mit der Folge der Beschädigung personenbezogener Daten. Die Verfälschung von Diagnoseschlüsseln, der Verlust oder die Löschung von personenbezogenen Daten können zur Nichtverfügbarkeit zum Download führen.	Rechtswidrige Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	3	3	3	0	0	0	0	0	3	6	Technische und organisatorische Maßnahmen von DIGIT.					akzeptabel mit Evaluation
R2-Hacker		Manipulation personenbezogener Daten durch außenstehende Angreifer bei der Übertragung.	Vorsätzliche Veränderung von Informationen - Diagnoseschlüssel können verfälscht werden mit der Folge der Beschädigung personenbezogener Daten. Die Verfälschung von Diagnoseschlüsseln, der Verlust oder die Löschung von personenbezogenen Daten können zur Nichtverfügbarkeit zum Download führen.	Rechtswidrige Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	3	3	3	0	0	0	0	0	3	3	Design-Entscheidungen D-5.1-2 (Übertragung von Pseudonymen), D-5.1-3 (Netzwerkkommunikation sollte verschlüsselt erfolgen)					akzeptabel
RI-Dienstleist er Mitgliedsstaaten		Mißbrauch von Zugangsdaten zum Zweck fehlerhafter schädigender Uploads.	Mißbrauch von Zugangsdaten durch Insider (Administrator).	Rechtswidrige Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	2	3	3	3	0	0	0	0	0	3	6	Vertrag mit Dienstleister und technische und organisatorische Maßnahmen.	Aufnahmeprozess, Zertifikate				akzeptabel mit Evaluation
	11	**Unzutreffende Verarbeitung personenbezogener Daten (technisches Versagen, Fehlfunktionen in Programmen, menschliches Versagen)**																						
RI-Dienstleist er Mitgliedsstaaten		Fehlfunktionen in der Infrastruktur des EFGS (z.B. vollständiger Ausfall der Stromversorgung oder der Kühlsysteme etc.)	Keine weitere Beschreibung erforderlich.	Nichtverfügbarkeit wichtiger Verarbeitungsvorgänge bezüglich personenbezogener Daten (Upload/Herunterladen von Diagnoseschlüsseln). Verlust		3	yes	2	4	4	4	4	4	4	4	4	4	8	EFGS/DIGIT technische und organisatorische Maßnahmen Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: ST_business_continuity_management.doc, ST_incident_mgt.doc					akzeptabel mit Evaluation
RI- Apple / Google		Technische Einschränkungen des Exposure Notification Frameworks der Anbieter Apple und Google, einschließlich Problemstellungen in Bezug auf Sicherheitskopie- und Wiederherstellungsfunktionen.	Keine weitere Beschreibung erforderlich.	Nichtverfügbarkeit wichtiger Verarbeitungsvorgänge bezüglich personenbezogener Daten (Upload/Herunterladen von Diagnoseschlüsseln). Verlust		3	yes	4	4	4	4	4	0	0	4	4	4	16	Das Risiko wird durch die nationale App bestimmt. Kein weiteres Risiko durch EFGS.			Dieses Risiko wird beobachtet. Siehe Anlage 7 zum DSFA-Bericht (Ziff. 2.3.2 (3)		bedingt akzeptabel
Software und Service Provider // SAP/ T		Unsichere Programmierung des EFGS, Nebeneffekte und unerwartete Auswirkungen und Ergebnisse der Ausführung der Software, nicht-autorisierte Änderungen.	Unbeabsichtigte Änderung von Informationen und personenbezogenen Daten - Die Verfälschung von Diagnoseschlüsseln kann zum Verlust oder zur Beschädigung personenbezogener Daten führen.	Datenschutzverstoß.		3	yes	1	4	4	4	4	0	0	4	4	4	4	Vertrag mit Dienstleister (Betrieb).					akzeptabel
Software und Service Provider // SAP/ T		Fehlkonfiguration von sicherheitsbezogenen Unterstützungssystemen.	Unbeabsichtigte Änderung von Informationen und personenbezogenen Daten - Die Verfälschung von Diagnoseschlüsseln kann zum Verlust oder zur Beschädigung personenbezogener Daten führen.	Datenschutzverstoß.		3	yes	1	4	4	4	4	4	4	4	4	4	4	Vertrag mit Dienstleister (Betrieb).					akzeptabel
Software und Service Provider // SAP/ T		Fehlende Absicherung des Zugriffs auf Verwaltungsfunktionen.	Mißbrauch administrativer Zugänge durch Dritte (schwache Passworte).	Datenschutzverstoß.		3	yes	2	4	4	4	4	4	4	4	4	4	8	Autorisierung und Authentifizierung und andere technische Standard-Gegenmaßnahmen werden implementiert. Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: Access Control & Authentication security standard.pdf					akzeptabel mit Evaluation
RI-User CWA-App		Nicht-Verfügbarkeit auf Grund Inkompatibilität des EFGS mit dem mobilen Endgerät des Nutzers.	Nicht-Verfügbarkeit von EFGS-Funktionen (Upload/Download von Diagnoseschlüsseln) für Nutzer der mobilen Applikationen.	Datenschutzverstoß.		3	yes	1	0	0	0	4	0	0	4	2	0	2	4						akzeptabel
RI-User CWA-App		Überlastung des mobilen Endgeräts des Nutzers auf Grund Herunterladens zu großer Datenpakete im Hinblick auf das Feld "relevante Länder".	Risiko des Überlastens der mobilen Applikation und Frustration der Nutzer kann zur Deinstallation der App führen.	Datenschutzverstoß.		3	yes	3	0	0	0	4	0	0	4	2	0	2						
RI-Dienstleist er Mitgliedsstaaten		Vorübergehende oder permanente Nicht-Verfügbarkeit der vom EFGS dem nationalen Backend bereitgestellten Daten, z.B. auf Grund von Fehlfunktionen, Problemen mit Zertifikaten und Autorisierungsfunktionen.	Keine weitere Beschreibung erforderlich.	Datenschutzverstoß.		3	yes	3	0	0	0	3	0	0	3	2	0	2	9	Zusätzlich müssen Schnittstellen Status- und Fehlermeldungen vorsehen, um festzustellen, ob erneute Uploads oder ähnliche Maßnahmen erforderlich sind. Zertifikate auf Ebene (1) Infrastruktur (DIGIT), (2) Betrieb EFGS (T-Systems), (3) Infrastruktur der nationalen App. Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme:					akzeptabel mit Evaluation
RI-Dienstleist er Mitgliedsstaaten		Vorübergehende oder permanente Nicht-Verfügbarkeit der Upload-Funktion des EFGS, z.B. auf Grund von Fehlfunktionen, Problemen mit Zertifikaten und Autorisierungsfunktionen (siehe Zeile 84).	Siehe Zeile 84.	Siehe Zeile 84.		3	yes	3	0	0	0	3	0	0	3	2	0	2	9	Zusätzlich müssen Schnittstellen Status- und Fehlermeldungen vorsehen, um festzustellen, ob erneute Uploads oder ähnliche Maßnahmen erforderlich sind. Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: ST_business_continuity_management.doc, ST_incident_mgt.doc					akzeptabel mit Evaluation
Software und Service Provider // SAP/ T		Verlust personenbezogener Daten gefolgt von einer Fehlfunktion der Sicherheitskopie- und Wiederherstellungssysteme.	Keine weitere Beschreibung erforderlich.	Datenschutzverstoß.		3	yes	2	0	0	0	3	0	3	2	0	2	6	Backup Konzept . Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: Backup security standard.pdf					akzeptabel mit Evaluation
Software und Service Provider // SAP/ T		Nicht-autorisierte oder irrtümliche Löschung im EFGS gespeicherter personenbezogener Daten.	Keine weitere Beschreibung erforderlich.	Datenschutzverstoß.		3	yes	1	0	0	0	3	0	3	2	0	2	3	Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: Access Control & Authentication security standard.pdf					akzeptabel
R2-Hacker		DNS-Spoofing / Man-in-the-Middle Angriffe auf den EFGS.	Ein Angreifer könnte ein nationales Backend täuschen, mit einem Server nach seiner Wahl zu kommunizieren an Stelle mit dem dem EFGS. Hierzu können DNS-Spoofing und man-in-the middle Angriffe eingesetzt werden. Diese Art von Angriff kann auch umgekehrt gegen den EFGS durch ein feindliches Backend geführt werden.	Verarbeitung für neue Zwecke, die von Dritten/Kriminellen vorgegeben werden. Rechtswidrige, intransparente Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	1	0	3	3	0	0	0	2	0	2	3	Design-Entscheidungen EFGS T-1-2 (HTTP Public Key Pinning); Um einen Kommunikationspartner (EFGS/nationales Backend) zu authentifizieren, verwendet das System digitale Signaturen.					akzeptabel
R2-Hacker		Denial of Service-Angriffe auf die EFGS Server mit der Folge der beabsichtigten Überlastung.	Ein Angreifer kann einen Denial-of-Service Angriff zur Störung des EFGS verwenden. Sind die Funktionen des EFGS nicht verfügbar, können Diagnoseschlüssel nicht geteilt werden. Gelingt es dem Angreifer, große Mengen falscher Diagnoseschlüssel in den EFGS einzuschleusen, werden diese eventuell automatisch an die nationalen Backends verteilt. Diese werden so auch Opfer des Angriffs.	Datenschutzverstoß.		3	yes	3	0	3	0	3	0	3	2	0	2	9	Design-Entscheidungen EFGS T-5-2, T-5-3 und T-5-4 (DoS Absicherung im Betrieb)					akzeptabel mit Evaluation
Software und Service Provider // SAP/ T		Unzureichende Durchführung von Software-Test- und Qualitätssicherungsmaßnahmen.	Mißbrauch von System-Ressourcen Ein Angreifer kann die System-Resourcen zweckentfremden, z.B. für Crypto Mining, und geheime Zugänge einrichten. Um die (einfache) Entdeckung zu verhindern wird der Hacker versuchen, alle Änderung am System und Aktivitäten zu vertuschen, z.B. durch das Löschen von Protokollen und Sourcen.	Datenschutzverstoß.		3	yes	2	4	4	4	4	0	4	4	4	4	8	Design-Entscheidungen EFGS D-2.3-1 (Überwachungsschnittstelle und Integrität); D-2.3-2 (Unterstützung durch Durchführung der notwendigen Tests und Prüfungen); T-3-1 und T-3-2 (Alle sicherheitsrelevanten Änderungen müssen in einem dedizierten, revisionssicheren und geschützten Sicherheitsprüfungs-Protokoll gespeichert werden). Anzuwendende DIGIT Sicherheitsanweisungen für IT-Systeme: IT Security Compliance					akzeptabel mit Evaluation

							Risikobewertung																	
															Schadenshöhe									
Risiko-quelle	ID	Bedrohung	Beschreibung des Risikos (optional)	Beschreibung des drohenden Schadens für Betroffene (siehe auch die Schadensszenarien im Tabellenblatt "Schadenskategorien")	Betroffenen-gruppen (CWA-Nutzer, Nutzer anderer nat. Corona-Apps, Personen im Umfeld, Personen, die von	Schutzbedarf der Daten	Schwerwiegende (gesamt)	Einzelschwerwiegende (gesamt)	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Rechtmäßigkeit	Intervenierbarkeit	Transparenz	Zweckbindung / Unverkettbarkeit	Risikowert / Risikoindex	Vorgesehene Risikominimierungsmaßnahmen (zu den allgemeinen Erwägungen siehe Abschnitte 13.2 und 15 Entwurf DPIA-Report)	Vorgesehene Maßnahmen	Geplante Maßnahmen	Bewertung, warum "rote" Risiken akzeptiert werden können (zu den allgemeinen Erwägungen der Risikoakzeptanz siehe Kap. 15 des EFGS_DPIA_Draft)	Restrisiko
	12	**Verarbeitung veralteter oder überflüssiger personenbezogener Daten**																						
Software und Service Provider // SAP/ T		Unbegrenzte Speicherung personenbezogener Daten (einschließlich Metadaten) in Datenbanken des EFGS.	Risiko der unsicheren oder nicht vollständigen Löschung von Daten nach 14 Tagen oder Download durch alle Mitgliedsstaaten. Die Interoperabilität soll nicht zu einer weiteren Datenerhebung führen, längere Vorhaltezeiträume für Daten erhöhen das Mißbrauchsrisiko.	Unverhältnismäßige, rechtswidrige Verarbeitung personenbezogener Daten. Datenschutzverstoß.		3	yes	3	4	4	1	0	0	0	4	4	4	12	Implementierung des Löschkonzepts und -Prozesses. Fehlende notwendige Information des Dienstleisters.			Löschkonzept des Betriebes und Nachweis der Löschung lag zum Zeitpunkt der Risikoanalyse noch nicht vor. Wird im Rahmen des Betriebes umgesetzt.	bedingt akzeptabel
RK-service provider member states		Unbegrenzte Speicherung überflüssiger personenbezogener Daten (relevante Länder).	Ein Teilen des Herkunftskennzeichens für Diagnoseschlüssel über die nationalen Backends hinaus kann die Herkunft von Personen hinter den Diagnoseschlüsseln offenbaren.	Diskriminierung von Ausländern, Datenschutzverstoß.		2	yes	3	1	1	1	0	0	0	1	1	1	3	Löschung von Daten im nationalen Backend (Normalisierung)				akzeptabel
Software und Service Provider // SAP/ T		Unbegrenzte Speicherung personenbezogener Daten unzutreffender, veralteter oder überflüssiger Daten mit nachteiligen Konsequenzen.	Keine weitere Beschreibung erforderlich.	Diskriminierung, Datenschutzverstoß.		3	yes	3	4	4	4	0	0	4	2	4	4	12	Implementierung des Löschkonzepts und -Prozesses. Fehlende notwendige Information des Dienstleisters.			Löschkonzept des Betriebes und Nachweis der Löschung lag zum Zeitpunkt der Risikoanalyse noch nicht vor. Wird im Rahmen des Betriebes umgesetzt.	bedingt akzeptabel
	13	**Risiken für die Betroffenen auf Grund der Verarbeitung an sich**																						
RB- staatl. Behörden.		Gegenseitiges Misstrauen unter den Mitgliedsstaaten durch fehlgeleitete oder enttäuschte Erwartungen.	Unzureichende Prüfung des tatsächlichen Infektionsstatus oder fehlende Beteiligung am Upload von Diagnoseschlüsseln kann zu politischen Spannungen zwischen Mitgliedsstaaten führen, wenn Datenübertragungen einzelner Mitgliedsstaaten gesperrt oder herabgesetzt werden.	Diskriminierung. Gesellschaftliche und politische Risiken.		3	yes	2	0	0	0	4	0	0	2	2	2	8	Erstellen von Regeln und Definitionen für die Verteilung von Diagnoseschlüsseln, die leicht auf der Ebene des Backends angewendet werden können, wenn eine nationale Behörde entscheidet, zeitweise die Schlüssel eines Mitgliedsstaats nicht zu verteilen.				akzeptabel mit Evaluation
RB- staatl. Behörden.		Datenverarbeitung ohne epidemiologische Grundlagen und Wirkungen.	Durch den Dienstleister noch nicht bewertbar.	Diskriminierung. Gesellschaftliche und politische Risiken.		3	no											0	Design-Entscheidungen EFGS D-1-5 (Erforschung epidemiologischer Effekte).				
RB- Arbeitgeber / Versicherungen		Vorteilsgewährung für das Teilen personenbezogener Daten des Betroffenen mittels des EFGS oder für die Nutzung von Daten, die mittels des EFGS geteilt worden sind.	Durch den Dienstleister noch nicht bewertbar.	Diskriminierung. Gesellschaftliche und politische Risiken.		3	no											0	Vom Dienstleister nicht betrachtet.				
RB- Arbeitgeber / Versicherungen		Nachteilszufügung für die Weigerung, personenbezogene Daten mittels des EFGS zu Teilen oder solche mittels des EFGS geteilten personenbezogene Daten zu nutzen.	Durch den Dienstleister noch nicht bewertbar.	Diskriminierung. Gesellschaftliche und politische Risiken.		3	no											0	Vom Dienstleister nicht betrachtet.				
RB- staatl. Behörden.		Steigerung der allgemeinen Akzeptanz von Überwachungsmaßnahmen jenseits der Maßnahmen zur Bekämpfung der COVID-19 Pandemie.	Durch den Dienstleister noch nicht bewertbar.	Diskriminierung. Gesellschaftliche und politische Risiken.		3	no											0	Vom Dienstleister nicht betrachtet.				