[EU – Hoheitszeichen wurde entfernt!]

EXTERN

Anlage 1 zum DSFA-Bericht:

b.) Designentscheidungen bei der Entwicklung des European Federation Gateway Service (EFGS)

Version 1.2 Entwurf

Angepasster Entwurf für CWA v1.5

A. Einleitung

Zahlreiche Mitgliedstaaten der EU (und Vertragsparteien des EWR-Abkommens) haben im Rahmen ihrer Strategien für die öffentliche Gesundheit zur Bekämpfung der Coronavirus-Pandemie (COVID-19) bereits mobile Apps eingeführt, mit der die Kontaktnachverfolgung vereinfacht werden soll, oder planen die Einführung einer derartigen App. Die Nutzung dieser Apps ist freiwillig und die übertragenen Daten werden nur temporär gespeichert. Um die Interoperabilität der App-Systeme der EU-Staaten zu ermöglichen, wurde eine gemeinsame Server-Infrastruktur, der „European Federation Gateway Service (EFGS)“, aufgebaut. Die Bürger der Europäischen Union sollen, unabhängig davon, wo sie sich in der EU aufhalten, gewarnt werden, wenn sie in Kontakt mit einem anderen Nutzer einer solchen zugelassenen App (App-Nutzer) gekommen sind, der positiv auf das Coronavirus (COVID-19) getestet wurde.

Mit diesem Dokument soll für die Öffentlichkeit nachvollziehbar dargestellt werden, welche Designentscheidungen getroffen wurden, um das EFGS grundrechtsschonend auszugestalten. Die Erkenntnisse aus der projektbegleitenden Datenschutz-Folgenabschätzung (DSFA) sind als Designentscheidungen in den Entwicklungsprozess eingeflossen.

Aufgrund fortlaufend neuer Erkenntnisse wird, neben dem EFGS selbst, auch dieses Dokument regelmäßig aktualisiert. Daher ist es als „dynamisches Dokument“ zu betrachten.

Das Konzept des „eingebauten Datenschutzes“ (Privacy by Design) ist eine grundlegende Voraussetzung für die wirksame Umsetzung des Datenschutzes. Es wird immer deutlicher, dass Innovation, Kreativität und Wettbewerbsfähigkeit aus einer Design-Thinking-Perspektive betrachtet werden müssen. Der Datenschutz muss auf eine ganzheitliche, integrative und kreative Weise in Technologien, Funktionen und Informationsarchitekturen eingebettet werden. Die ganzheitliche Herangehensweise ist wichtig, da immer ein zusätzlicher, breiterer Kontext berücksichtigt werden muss. Der integrative Aspekt ist von Bedeutung, da alle Stakeholder und Interessen einbezogen werden sollten. Der kreative Ansatz ist wesentlich, da die Einbettung des Datenschutzes es manchmal erforderlich macht, bereits bestehende Optionen neu zu definieren, da die Alternativen inakzeptabel sind. Daraus resultiert, dass der Datenschutz zu einem wesentlichen Bestandteil der bereitgestellten Kernfunktionen wird. Der Datenschutz ist ein integraler Bestandteil des Systems und dessen Funktionalität.

Um diese Ziele zu erreichen und um Risiken im Hinblick auf den Datenschutz zu vermeiden, wurden bei der Entwicklung des EFGS und seiner Infrastruktur die in diesem Dokument aufgeführten Designentscheidungen getroffen.

B. Inhaltsverzeichnis

C. Referenzen

Bei der Erstellung dieses Dokuments wurden die folgenden Veröffentlichungen berücksichtigt:

eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-19, Common EU Toolbox for Member States, Version 1.0 vom 15. April 2020[1]

eHealth Network, Interoperability guidelines for approved contact tracing mobile applications in the EU vom 13. Mai 2020[2]

[1] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.
[2] https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.

eHealth Network, Guidelines to the EU Member States and the European Commission on Interoperability specifications for cross-border transmission chains between approved apps, Basic interoperability elements between COVID+ Keys driven solutions V1.0 vom 12. Juni 2020[3]

eHealth Network, European Proximity Tracing, An Interoperability Architecture for contact tracing and warning apps V1.3 vom 2. September 2020[4]

eHealth Network European Interoperability Certificate Governance, A Security Architecture for contact tracing and warning apps, V1.0 vom 4. September 2020[5]

Europäischer Datenschutzausschuss (EDSA), Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 vom 21. April 2020[6]

Europäischer Datenschutzausschuss (EDSA), Erklärung über die Datenschutzfolgen der Interoperabilität von Kontaktnachverfolgungs-Apps vom 16. Juni 2020[7]

Durchführungsbeschluss (EU) 2020/1023 der Kommission vom 15. Juli 2020 zur Änderung des Durchführungsbeschlusses (EU) 2019/1765 hinsichtlich des grenzüberschreitenden Datenaustauschs zwischen nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung zwecks Bekämpfung der COVID-19-Pandemie[8]

Empfehlung (EU) 2020/518 der Kommission vom 8. April 2020 für ein gemeinsames Instrumentarium der Union für den Einsatz von Technik und Daten zur Bekämpfung und Überwindung der COVID-19-Krise, insbesondere im Hinblick auf Mobil-Apps und die Verwendung anonymisierter Mobilitätsdaten[9]

Mitteilung der Kommission, Leitlinien zum Datenschutz bei Mobil-Apps zur Unterstützung der Bekämpfung der COVID-19-Pandemie, (2020/C 124 I/01) vom 17. April 2020[10]

Chaos Computer Club (CCC), 10 Prüfsteine für die Beurteilung von „Contact Tracing"-Apps vom 6. April 2020[11]

---

[3] https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilityspecs_en.pdf.
[4] https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_architecture_en.pdf.
[5] https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_certificate_governance_en.pdf
[6] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_de.pdf.
[7] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_de_0.pdf .
[8] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32020D1023&from=EN.
[9] https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1587153139410&uri=CELEX:32020H0518.
[10] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020XC0417(08).
[11] https://www.ccc.de/de/updates/2020/contact-tracing-requirements.

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FifF), Datenschutz-Folgenabschätzung (DSFA) für die Corona-App, Version 1.6 vom 29. April 2020[12]

T-Systems/SAP Dokumentation zum European Federation Gateway Service (EFGS)[13]

[12] https://www.fiff.de/dsfa-corona.
[13] https://github.com/eu-federation-gateway-service/efgs-federation-gateway.

D. Zweck des Dokuments

Mit diesem Dokument soll für die Öffentlichkeit nachvollziehbar dargestellt werden, welche Designentscheidungen getroffen wurden, um das EFGS grundrechtsschonend auszugestalten.

Zur laufenden Verbesserung und Berücksichtigung der Datenschutzanforderungen wurde während des gesamten Entwicklungsprozesses für das EFGS eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt. Eine Datenschutz-Folgenabschätzung ist eine Risikoanalyse und -bewertung für die Verarbeitung personenbezogener Daten. Es wird abgeschätzt, welche Risiken für die Rechte und Freiheiten der von der Datenverarbeitung Betroffenen, etwa von (CWA/ App-)Nutzern, Personen im Umfeld von (CWA/ App-)Nutzern, etwa Haushaltsangehörige, und auch weiteren Personen, soweit auch diese bspw. von einer Falschwarnung des (CWA/ App-) Nutzers oder von Manipulationen o.ä. betroffen sein können. durch die Datenverarbeitung ausgehen und wie wahrscheinlich es ist, dass diese Risiken eintreten. Die Erkenntnisse aus der begleitenden DSFA sind als Designentscheidungen in den Entwicklungsprozess eingeflossen.

Die in der Datenschutz-Grundverordnung (DSGVO) geregelte DSFA stellt ein Instrument zur Steuerung der Risiken dar, die von der Datenverarbeitung für die betroffenen Personen ausgehen. Inhaltlich wurde daher bei der DSFA die Perspektive des von der Datenverarbeitung Betroffenen in den Fokus der Risikobetrachtungen genommen. Insbesondere wurden potentielle immateriellen Schäden betrachtet, also drohende gesellschaftliche und soziale Nachteile, Diskriminierungen, Einschüchterungseffekte und die (selbstauferlegte) Einschränkung von Grundrechten. Weiterführende Informationen finden sich in dem ausführlichen Bericht zur Datenschutz-Folgenabschätzung für das EFGS.

Dieses Dokument soll der datenschutzinteressierten Öffentlichkeit dazu dienen, anhand der aufgeführten Anforderungen von Behörden, Nichtregierungsorganisationen und der Zivilgesellschaft zu prüfen und zu bewerten, inwieweit ein grundrechtsschonendes „Privacy by Design“ gelungen ist, und damit die Transparenz fördern. Anregungen und Kritik sind zur weiteren Verbesserung der Prozesse ausdrücklich erwünscht.

E. Beschreibung des EFGS

Zur besseren Lesbarkeit des Dokumentes wird an dieser Stelle die Funktionsweise des EFGS aus Nutzersicht dargestellt.

Durch die Corona-Pandemie kam es zu dem weltweiten Ausbruch der neuen Atemwegserkrankung COVID-19. Verursacht wird die Erkrankung durch eine Infektion mit dem bisher unbekannten Coronavirus SARS-CoV-2. In zahlreichen Ländern der Welt gab es im Verlauf der Pandemie massive Einschnitte in das öffentliche Leben und in das Privatleben vieler Bürger. Die nationalen Apps zur Kontaktnachverfolgung sollen zu einer frühestmöglichen Unterbrechung der Infektionsketten beitragen. Hierzu sollen die Nutzer durch die Apps wegen des Kontakts zu einer infizierten Person möglichst früh gewarnt und bei dem Erhalt ihres Testergebnisses unterstützt werden.

Das Erfassen von möglichen Begegnungen mit infizierten Personen erfolgt durch die sog. „Kontaktnachverfolgung“. Das Ziel der Kontaktnachverfolgung besteht darin, die Nutzer darüber zu informieren, dass sie sich in der Nähe einer infizierten Person aufgehalten haben, ohne dabei die Identität der infizierten Person oder den Ort, an dem dieser Kontakt stattgefunden hat, preiszugeben. Dabei geht es vor allem darum, Kontakte zu erfassen, die nicht aus dem persönlichen Umfeld stammen und bei denen der Nutzer deshalb nicht erfahren kann, dass die betreffenden Kontaktpersonen infiziert waren. Derartige Kontakte können in öffentlichen Verkehrsmitteln, Supermärkten usw. stattfinden. Voraussetzung für die Kontaktnachverfolgung ist, dass der Nutzer sein Mobilgerät bei sich trägt, die App darauf installiert ist und er die Bluetooth-Schnittstelle des Mobilgerätes aktiviert hat. Die Bluetooth-Schnittstelle muss aktiviert sein, damit das Gerät Zufalls-IDs senden und die Zufalls-IDs von anderen Geräten erfassen und im Kontaktprotokoll des Geräts speichern kann. Durch ein von Google und Apple bereitgestelltes Framework, auf das die Kontaktnachverfolgungs-App zugreifen kann, wird berechnet, ob bei einem der Kontakte ein besonderes Risiko für eine Ansteckung bestand. Die für die Berechnung eingesetzten Algorithmen werden von den nationalen Gesundheitsbehörden zur Verfügung gestellt und entsprechen den neuesten wissenschaftlichen Erkenntnissen. Das Ergebnis der Risikoeinschätzung wird dem Nutzer mit entsprechenden Handlungsempfehlungen auf dem Mobilgerät angezeigt.

In den meisten europäischen Staaten wird hierfür die Exposure Notification API von Google und Apple verwendet. Obwohl die zur Abstandserfassung eingesetzten Funktionen der einzelnen nationalen App-Lösungen kompatibel sind, findet noch kein Datenaustausch zwischen den nationalen Backend-Servern dieser Apps statt. Dies ist bedauerlich, da die Bürger über ihre jeweiligen Landesgrenzen hinaus pendeln und reisen. Aus diesem Grund ist die Interoperabilität der nationalen Backend-Server unbedingt erforderlich.

Um die grenzüberschreitende Interoperabilität der Apps zur Kontaktnachverfolgung und Warnung zu erleichtern, hat die Europäische Kommission einen Durchführungsbeschluss zur Förderung der Einrichtung eines freiwillig zu nutzenden Gateway Service angenommen.[14] Damit wurde der European Federation Gateway Service (EFGS) ins Leben gerufen. Beim EFGS handelt es sich um eine Schnittstelle, mit der die relevanten pseudonymisierten Informationen, die durch die einzelstaatlichen Apps zur Kontaktnachverfolgung und Warnung erfasst werden, auf effiziente und sichere Weise zwischen den am EFGS beteiligten Mitgliedstaaten ausgetauscht werden. Jeder nationale Backend-Server lädt in regelmäßigen Abständen, mehrfach am Tag, die Schlüssel neu infizierter Bürger („Diagnoseschlüssel“) hoch und lädt die Diagnoseschlüssel aus anderen m EFGS beteiligten Ländern herunter. Durch das EFGS werden die Diagnoseschlüssel über alle nationalen Backend-Server hinweg synchronisiert. Das Design dieses Service folgt den Interoperabilitätsleitlinien[15], der zwischen den Mitgliedstaaten und der Europäischen Kommission vereinbarten technischer Spezifikationen[16], den in der EU Toolbox aufgeführten Leitlinien und den EU-Leitlinien zur Gewährleistung der uneingeschränkten Einhaltung der Datenschutzstandards durch Mobil-Apps[17].

Zum Austausch der Diagnoseschlüssel muss der Nutzer die für ihn „relevanten Länder“ angeben. Der Diagnoseschlüssel ist eine eindeutige kurzlebige Kennung für einen App-Nutzer, welcher meldet, mit COVID-19 infiziert zu sein oder möglicherweise COVID-19 ausgesetzt gewesen zu sein. Zu den „relevanten Ländern“ gehören der Mitgliedstaat bzw. die Mitgliedstaaten, in dem bzw. denen sich ein App-Nutzer in den 14 Tagen vor dem Datum des Hochladens der Schlüssel aufgehalten hat, oder die Länder, aus denen ein App-Nutzer in diesen 14 Tagen andere europäische Bürger (z. B. Touristen) getroffen hat. Diese Informationen werden den Diagnoseschlüsseln der App-Nutzer hinzugefügt und auf die nationalen Backend-Server hochgeladen. Darüber hinaus fügt der Backend-Server den Diagnoseschlüsseln das „Ursprungsland“ hinzu und lädt diese Information in das EFGS hoch. „Ursprungsland“ bezeichnet den Mitgliedstaat, in dem sich der Backend-Server befindet, der die Schlüssel in das Federation Gateway hochgeladen hat. Das EFGS wandelt das Format der Schlüssel in ein Standardformat um, das für alle Backend-Server lesbar ist, und leitet die Schlüssel an die nationalen Backend-Server aller teilnehmenden Mitgliedstaaten weiter. Die nationalen Backend-Server verteilen die Schlüssel an die Nutzer, je nach dem Ursprungsland der Schlüssel und den relevanten Ländern, die der App-Nutzer von den nationalen Backend-Servern angefordert hat. Daher empfangen alle nationalen Backend-Server alle Schlüssel, die über das System ausgetauscht werden. Die Nutzer hingegen empfangen nur die Schlüssel aus den relevanten Ländern, die sie angegeben haben. Durch das Exposure Notification Framework der nationalen Apps werden die heruntergeladenen Schlüssel mit den Zufalls-IDs abgeglichen, die das Gerät eines Nutzers von den Geräten anderer Nutzer empfangen hat. Das Ergebnis der Risikoeinschätzung wird dem Nutzer mit entsprechenden Handlungsempfehlungen auf dem Mobilgerät angezeigt.

[14] Coronavirus: new steps towards setting-up of an interoperability solution for mobile tracing and warning apps vom 15. Juli 2020.
[15] Interoperability guidelines vom 13. Mai 2020.
[16] Set of Technical Specifications.
[17] EU Guidelines on Data Protection for Apps.

F. Designentscheidungen

Nachfolgend werden die Designentscheidungen dargestellt, mit denen den Risiken für die Rechte und Freiheiten der von der Datenverarbeitung Betroffenen begegnet wurde. Ebenfalls wird dargestellt, aus welchen Gründen bestimmte Designentscheidungen getroffen wurden.

Die gelb markierten Maßnahmen sind noch nicht umgesetzt.

I. Risiken für den Datenschutz

1. Zweck der Datenverarbeitung

Nachfolgend wird dargestellt, wie die Zweckgebundenheit durch grundsätzliche Designentscheidungen umgesetzt wurde.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-bewertung	Referenz
Zweck: App-Nutzer sollen unabhängig davon, wo sie sich in der EU aufhalten, benachrichtigt werden, wenn sie sich über einen relevanten Zeitraum hinweg in der Nähe eines anderen Nutzers aufgehalten haben, dem die App ein positives COVID-19-Testergebnis übermittelt hatte.	D-1-1	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 2; eHealth Interoperability guidelines, Abschnitt I.4, Definition von Interoperabilität	**Die nationalen Gesundheitsbehörden grenzen den Zweck wie folgt ein** Die App- Nutzer sollten unabhängig davon, wo sie sich in der EU aufhalten, benachrichtigt werden, wenn sie mit einer infizierten Person Kontakt hatten und aufgrund der Dauer des Kontakts und des Abstands zu der Person ein Infektionsrisiko besteht.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-bewertung	Referenz
			✓ Über die nationale App zur Kontaktnachverfolgung sollen den App-Nutzern Informationen zu ihrem Infektionsrisiko sowie Empfehlungen zu Gesundheits- und Infektionsschutzmaßnahmen zur Verfügung gestellt werden, damit Infektionsketten unterbrochen werden können. ✓ Diese Daten dürfen nicht zu anderen Zwecken verarbeitet werden.	
Zweck: Durch die Interoperabilität der Apps zur Kontaktnachverfolgung innerhalb des EWR kann die Wirksamkeit dieser Apps als Ergänzung zu bereits bestehenden Maßnahmen allgemein erhöht werden, da unabhängig von der jeweils genutzten App mehr potenzielle Kontaktnachverfolgungen und Warnungen möglich sind. Dadurch wird die Nutzung insbesondere für Personen in Grenzregionen vereinfacht, die auf Reisen oder	D-1-2	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 6	**Von den Behörden festgelegte Interoperabilitätszwecke** ✓ Erhöhung der Wirksamkeit von Apps zur Kontaktnachverfolgung als Ergänzung zu bereits bestehenden Maßnahmen ✓ Vereinfachung der Nutzung, insbesondere für Personen in Grenzregionen ✓ Vereinfachung der Nutzung, insbesondere für Personen, die beruflich mit Touristen zu tun haben	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-bewertung	Referenz
während der Arbeit (z. B. im Tourismusgewerbe) mit vielen Personen aus anderen Mitgliedstaaten in Kontakt kommen.				
Aufgrund des potenziellen Datenschutzrisikos, das durch die Interoperabilität erhöht wird, sollten die Verantwortlichen **alternative Maßnahmen prüfen**.	D-1-3	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 6	**Analyse von alternativen Maßnahmen** ✓ Im Rahmen des Entwicklungsprozesses zur Anbindung des EFGS an die CWA wurden alternative Lösungen geprüft, Datenschutzrisiken infolge der Anbindung an das EFGS bewertet und in der DSFA beschrieben sowie Designentscheidungen getroffen, die ein durch die Interoperabilität potenziell erhöhtes Datenschutzrisiko minimieren [siehe hierzu z.B. die CWA – Designentscheidungen: D-5.1-8a (Verteilung von Schlüsseln nur mit Verifikation), D-6-2a (Verzicht auf Erhebung von „Countries of Interest“].	CWA-Designentscheidungen, D-1-1a, D-5.1-8a, D-6-2a
Derartige Apps müssten **Teil einer umfassenden Strategie für die öffentliche Gesundheit** zur	D-1-4	EDSA Interoperabilität von	**Strategie für die öffentliche Sicherheit** ⚠ Auszuführen von den Mitgliedstaaten.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-bewertung	Referenz
Bekämpfung der Pandemie sein, die unter anderem Tests und eine anschließende manuelle Kontaktnachverfolgung zur Verbesserung der Wirksamkeit der durchgeführten Maßnahmen vorsieht.		Kontaktnachverfolgungs-Apps, Ziffer 7	✓ Siehe CWA-Designentscheidungen, D-1-1a	
Epidemiologischer Effekt Der Effekt von Apps zur Kontaktnachverfolgung wird von der Wissenschaft derzeit noch diskutiert und erforscht. Wenn mit der App kein epidemiologischer Effekt erzielt wird, kann der Zweck der Datenverarbeitung möglicherweise nicht erreicht werden. Die Zweckmäßigkeit der Verarbeitung von personenbezogenen Daten ist für die Rechtmäßigkeit dieser Datenverarbeitung von entscheidender Bedeutung.	D-1-5		**Forschung zum epidemiologischen Effekt** ✓ Einige Forscher gehen auf Grundlage rein theoretischer Modelle davon aus, dass ein epidemiologischer Effekt erreicht werden kann, wenn 60 Prozent der Bevölkerung die Corona-Warn-App nutzen.[18] Andere wiederum gehen davon aus, dass für die Wirksamkeit von Apps zur Kontaktnachverfolgung eine Nutzungsquote von 60 Prozent nicht erforderlich ist.[19] Wenn Tests erst drei oder mehr Tage nach dem Auftreten von Symptomen durchgeführt werden, würde Wissenschaftlern zufolge selbst die wirksamste Strategie zur	

[18] https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.
[19] https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-bewertung	Referenz
			Kontaktnachverfolgung nicht ausreichen, um die Entstehung einer Infektionskette zu verhindern. Forscher gehen davon aus, dass die Kontaktnachverfolgung eine wirksame Intervention darstellen kann, um die Verbreitung des COVID-19-Virus zu vermeiden, aber nur, wenn der Anteil der rückverfolgten Kontakte hoch ist und die Kontaktrückverfolgung schnell durchgeführt wird.[20]	
	D-1-6	EDSA-Leitlinien für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung, Anhang PUR-2	**Keine Nutzung für die Überwachung von Quarantänemaßnahmen** ✓ Die App wird nicht unter Umgehung ihres primären Verwendungszwecks dazu verwendet, Quarantänemaßnahmen oder Ausgangsbeschränkungen und/oder die Einhaltung von Maßnahmen der sozialen Distanzierung zu überwachen.	
	D-1-7	EDSA-Leitlinien für die Verwendung von Standortdaten und Tools	**Keine Standortbestimmung**	

[20] https://www.thelancet.com/journals/lanpub/article/PIIS2468-2667(20)30157-2/fulltext.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-bewertung	Referenz
		zur Kontaktnachverfolgung, Anhang PUR-3	✓ Die App wird nicht dazu verwendet, Schlüsse über den Standort der App-Nutzer auf der Grundlage ihrer Interaktionen und/oder anderer Kriterien zu ziehen.	
	D-1-8		**Technische Ausstattung der Nutzer** Damit der epidemiologische Zweck der Corona-Warn-App erreicht wird, müssen möglichst viele Personen die App nutzen. Daher ist es erforderlich, dass die App-Nutzer in technischer Hinsicht entsprechend ausgerüstet sind. ⚠ Die einzelstaatlichen Apps wurden für das Betriebssystem iOS von Apple und das Betriebssystem Android von Google entwickelt. Die Entscheidung fiel dabei auf eine Technologie zur Kontaktermittlung, die nicht dem aktuellen Stand der Technik entspricht. Mit der aktuellen Technologie hätten die Kontakte präziser ermittelt werden können. Die Wahl fiel auf die energiesparende Bluetooth-Technologie, da diese auch auf älteren Mobilgeräten verfügbar ist und die App dadurch einem größeren Nutzerkreis zur Verfügung gestellt werden kann.	eHealth NetworkGuidelines Interoperability Specifications, Abschnitt 2.2

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-bewertung	Referenz
			✓ Beim Design des EFGS wurde unter anderem davon ausgegangen, dass die Google/Apple Exposure Notification (GAEN) API von allen teilnehmenden Ländern genutzt wird.	

2. Zweck der App-spezifischen Funktionen

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Zweck der App-spezifischen Funktionen Damit die App ihren Zweck erfüllen kann, muss sie mit geeigneten Funktionen ausgestattet sein.	D-2-1	eHealth Network, Common EU Toolbox for Member States, Anhang I, TF-02, EDSA-Leitlinien für die Verwendung von Standortdaten und Tools zur	**Justierbarkeit der Messalgorithmen** ✓ Siehe CWA-Designentscheidungen D-1-6	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Die tatsächliche physische Nähe sollte exakt erfasst werden. Nur wenn sich ein Mobiltelefon für eine von den nationalen Gesundheitsbehörden gemeinsam vereinbarte „epidemiologisch relevante“ Zeitspanne in „epidemiologisch relevanter“ Nähe zu einem anderen Mobiltelefon befindet, wird die ID der beiden Mobiltelefone in verschlüsselter Form auf dem jeweils anderen Mobiltelefon gespeichert.		Kontaktnachverfolgung, Anhang FUNC-3		
Überwachung der Wirksamkeit der COVID-19-Apps (einschließlich der Interoperabilität) • Technisches Feedback wird auf einzelstaatlicher Ebene und auf EU-Ebene eingeholt. • Die Veröffentlichung/Freigabe des Quellcodes ist ausdrücklich erwünscht. Peer-Review-Verfahren auf nationaler Ebene aber auch zwischen den	D-2-2	eHealth Network, Common EU Toolbox for Member States, Anhang I, SA-03	**Überwachung der Wirksamkeit** ✓ Der offene Quellcode des European Federation Gateway Service (EFGS) ist auf github.com verfügbar. ✓ Unabhängige technische Prüfungen sind möglich. ✓ Die Prüfung wurde von Cybersicherheitsagenturen durchgeführt.	European Federation Gateway Service (EFGS)

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Mitgliedsstaaten mit dem Ziel der Überprüfung der Wirksamkeit und der Funktionsfähigkeit der ausgewählten Mobil-Apps sowie deren Konformität mit den grundrechtlichen Vorgaben sind ausdrücklich erwünscht. Bestandteil dieser Peer-Review-Verfahren sollten unabhängige technische Prüfungen sein, einschließlich eingehender Audits der Apps in Bezug auf die Aspekte Sicherheit, Datenschutz und Barrierefreiheit. Solche unabhängigen Prüfungen können mit den Prüfungen koordiniert werden, die von nationalen Organisationen durchgeführt werden, beispielsweise von Cybersicherheitsagenturen, den einzelstaatlichen Stellen, die mit der Überwachung der Barrierefreiheit von Websites und mobilen Anwendungen im Rahmen der Richtlinie über den barrierefreien Zugang zu Websites betraut sind. Diese Prüfungen werden dazu beitragen, das Vertrauen in die Apps zur Kontaktnachverfolgung zu stärken, eine wesentliche				

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Voraussetzung für die Akzeptanz und den Erfolg dieser Apps.				
Interoperabilitätsrahmen für elektronische Gesundheitsdienste (eHealth Network) Rahmen zur Modellierung der Interoperabilitätslandschaft mit dem Ziel der Beschreibung und Diskussion von Herausforderungen und Lösungen im Bereich der Interoperabilität. Dieser Rahmen wird von dem Netzwerk für elektronische Gesundheitsdienste unterstützt und setzt sich aus folgenden Ebenen zusammen: a) Rechtliche und regulatorische Ebene b) Organisatorische Ebene (Strategie und Pflegeprozess) c) Semantische Ebene (Daten und Informationen) d) Technische Ebene (Anwendungen und Infrastruktur)	D-2-3	eHealth Network, Common EU Toolbox for Member States, Anhang I, IOP-01	**Netzwerk für elektronische Gesundheitsdienste (eHealth Network)** ✓ Das Netzwerk setzt sich aus Mitgliedern aus sämtlichen EU-Mitgliedstaaten sowie aus Norwegen (Beobachterstatus) zusammen. ✓ Es hat die folgenden Leitlinien veröffentlicht: • Durchführungsbeschluss (EU) 2020/1023 der Kommission vom 15. Juli 2020 zur Änderung des Durchführungsbeschlusses (EU) 2019/1765 hinsichtlich des grenzüberschreitenden Datenaustauschs zwischen nationalen Mobil-Apps zur Kontaktnachverfolgung und Warnung zwecks Bekämpfung der COVID-19-Pandemie, ABl. L 227I vom 16. Juli 2020, S. 1-9 • Towards a common approach for the use of anonymised and aggregated mobility data for modelling the diffusion of COVID-19,	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			and optimising the effectiveness of response measures • Mobile applications to support contact tracing in the EU's fight against COVID-19 – progress reporting June 2020 • Coronavirus: Mitgliedstaaten einigen sich auf eine Interoperabilitätslösung für mobile Kontaktnachverfolgungs- und Warn-Apps • eHealth Network Guidelines to the EU Member States and the European Commission on interoperability specifications for cross-border transmission chains between approved applications • Technical specifications for interoperability of contact tracing applications - eHealth Network Guidelines to the EU Member States and the European Commission on Interoperability specifications for cross-border transmission chains between approved apps Die Kommission veröffentlichte folgende Dokumente: • Coronavirus: Kommission gibt Empfehlung zur Unterstützung von Ausstiegsstrategien	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			durch Daten von mobilen Geräten und Mobil-Apps an • EU Toolbox • Coronavirus: Leitlinien zur Gewährleistung der uneingeschränkten Einhaltung der Datenschutzstandards durch Mobil-Apps zur Bekämpfung der Pandemie • Interoperability guidelines for approved contact tracing mobile applications in the EU • Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combating the COVID-19 pandemic, OJ L 227I , 16.7.2020, p. 1–9	
Auf Grundlage epidemiologischer Kriterien muss eine Einigung darüber erzielt werden, wie der Begriff „enger Kontakt“, aus dem ein hohes	D-2-4	eHealth Network, Common EU Toolbox for Member States, Anhang I, IOP-02	**Epidemiologische Kriterien**	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Infektionsrisiko resultiert, zu definieren ist. App-Entwickler und Gesundheitsbehörden sollten sich an den Leitlinien der WHO und des ECDC zu den Bestimmungsfaktoren für die Kontaktnachverfolgung orientieren. Dazu gehört die Definition des Begriffs „enger Kontakt“ (Abstand zur Kontaktperson und Dauer des Kontakts) und eine Einigung darüber, wie lange die Kontaktdaten gespeichert werden.			✓ Das Europäische Zentrum für die Prävention und Kontrolle von Krankheiten (ECDC) hat folgende Dokumente veröffentlicht: Ermittlung von Kontaktpersonen: Umgang des Gesundheitswesens mit Personen (einschließlich Beschäftigten in Gesundheitsberufen), die mit COVID-19-Infizierten in der EU in Kontakt standen Mobile applications in support of contact tracing for COVID-19 - A guidance for EU/EEA Member States Population-wide testing of COVID-19: country experiences and potential approaches in the EU/EEA and the United Kingdom ⚠ Es liegt in der Verantwortung der Mitgliedstaaten, die von den Gesundheitsbehörden festgelegten Verfahren in den jeweiligen einzelstaatlichen Apps zu implementieren. .	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Eine App zur Kontaktnachverfolgung muss in der Lage sein, nahe Kontakte ihrer App-Nutzer mit Nutzern aufzuzeichnen, die andere Apps zur Kontaktnachverfolgung nutzen. Gemäß den vereinbarten epidemiologischen Kriterien müssen die Apps in der Lage sein, einen nahen Kontakt unabhängig von der technologischen Plattform und der Mobil-App der jeweiligen Nutzer zu ermitteln.	D-2-5	eHealth Network, Common EU Toolbox for Member States, Anhang I, IOP-03	**Aufzeichnung der nahen Kontakte der App-Nutzer** ✓ Anhand des Exposure Notification Framework (ENF) von Google und Apple werden die nahen Kontakte des Nutzers aufgezeichnet.	
Backend-Lösungen müssen in der Lage sein, mit anderen Mitgliedstaaten/Regionen über positiv getestete Nutzer zu kommunizieren. Die Gesundheitsbehörden sollten sich auf ein Protokoll für den Datenaustausch von grenzüberschreitenden Kontaktketten einigen, d. h., über ein Protokoll für den Austausch von Daten zu infizierten Personen, die möglicherweise mit	D-2-6	eHealth Network, Common EU Toolbox for Member States, Anhang I, IOP-04	**Protokoll für den grenzüberschreitenden Datenaustausch** ✓ Das Netzwerk für elektronische Gesundheitsdienste (eHealth Network) hat sich auf Übertragungsprotokolle für Downloads, Uploads und Callbacks geeinigt.	eHealth NetworkGuidelines Interoperability Specifications, Abschnitt 5.3.4, 5.4.4, 5.6.4

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Personen aus einem anderen Land in Kontakt waren.				
Benachrichtigungen über den Kontakt mit infizierten Personen Die nationalen Gesundheitsbehörden sollten sich auf das Protokoll verständigen, mit dem Personen darüber informiert werden, dass sie Kontakt mit einer infizierten Person hatten.	D-2-7	eHealth Network, Common EU Toolbox for Member States, Anhang I, IOP-05	**Benachrichtigungen über den Kontakt mit infizierten Personen** ⚠ Es liegt in der Verantwortung der Mitgliedstaaten, die von den Gesundheitsbehörden festgelegten Verfahren in den jeweiligen einzelstaatlichen Apps zu implementieren.	
Die Warnung und die Folgemaßnahmen sollten in Übereinstimmung mit den **von den Gesundheitsbehörden festgelegten Verfahren** erfolgen.	D-2-8	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 3	⚠ Es liegt in der Verantwortung der Mitgliedstaaten, die von den Gesundheitsbehörden festgelegten Verfahren in den jeweiligen einzelstaatlichen Apps zu implementieren.	
	D-2-9	EDSA-Leitlinien für die Verwendung von Standortdaten und Tools zur	**Interoperabilität zwischen den EU-Mitgliedstaaten** ✓ Die App sollte mit anderen in den EU-Mitgliedstaaten entwickelten Apps interoperabel sein,	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
		Kontaktnachverfolgung, Anhang FUNC-5	damit App-Nutzer, die in den Mitgliedstaaten auf Reisen sind, effizient benachrichtigt werden können.	
	D-2-10	eHealth Network Interoperability specifications for cross-border transmission, Abschnitt 3.4.1.1	**Grundlegende Merkmale des Federation Gateway** ✓ Das Gateway wird von einem vertrauenswürdigen Betreiber betrieben. ✓ Das Gateway verfügt über eine standardisierte Schnittstelle, über die die Backend-Server vertrauenswürdiger Länder (in der EU/dem EWR, aber ggf. auch in einem vertrauenswürdigen Drittland) COVID+-Schlüssel (gemeinsam mit den Informationen zu den betreffenden Ländern) hochladen können. ✓ Das Gateway verfügt über eine standardisierte Schnittstelle, über die die Backend-Server vertrauenswürdiger Länder COVID+-Schlüssel (gemeinsam mit den Informationen zu den betreffenden Ländern) herunterladen können. ✓ Die Speicherfrist von Daten auf dem Gateway ist auf das erforderliche Minimum begrenzt,	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			damit die Backend-Server aller vertrauenswürdigen Länder alle relevanten COVID+-Schlüssel herunterladen können. ✓ Über das Gateway können ausschließlich COVID+-Schlüssel verwaltet werden. Damit Datenschutzrisiken vermieden werden, können über das Gateway keine anderen Schlüssel zentral verwaltet werden. ✓ Der Quellcode des Gateway ist offen und überprüfbar.	

2.1 Fehlfunktionen

Durch die folgenden Designentscheidungen/-Bewertungen werden Fehlfunktionen des EFGS vermieden. Damit wird gleichzeitig ein Beitrag zu verschiedenen Grundsätzen des Datenschutzes (z. B. Transparenz und Vertraulichkeit) geleistet.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Offener Quellcode	D-2.1-1	eHealth Network, Common EU Toolbox	**Offener Quellcode**	European Federation

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Die technischen Spezifikationen und der Quellcode der Apps sollten im Sinne einer hohen Wiederverwendung, Interoperabilität, Überprüfbarkeit und Sicherheit veröffentlicht werden.		for Member States, Anhang I, TF-07	✓ Der Quellcode ist in englischer Sprache auf github.com verfügbar. Sicherheitsexperten aus der ganzen Welt haben die Möglichkeit, den Code zu prüfen und Anfragen und Vorschläge einzureichen.	Gateway Service (EFGS)
Sicherheitslücken in quelloffener Software Sicherheitslücken in quelloffenen Softwarekomponenten tragen möglicherweise dazu bei, dass der Zweck der App nicht erreicht werden kann, da sie eine Einschränkung der Funktionalität der Corona-Warn-App zur Folge haben oder dazu führen können, dass das Vertrauen der Nutzer in die App beschädigt wird. Daher ist ein geordnetes Verfahren für den Umgang mit Sicherheitslücken erforderlich.	D-**Fehler! Verweisquelle konnte nicht gefunden werden.**-2	EDSA-Leitlinien für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung, Anhang FUNC-2	**Umgang mit Sicherheitslücken** ✓ Damit das Risiko von Sicherheitslücken in den eingesetzten quelloffenen Softwarekomponenten dauerhaft so gering wie möglich ist, müssen die eingesetzten Komponenten stets auf dem aktuellen Stand sein. Dazu werden die Sicherheitswarnungen von GitHub-Sicherheitswarnungen für Sicherheitslücken in Komponenten, zu denen eine Abhängigkeit besteht („Vulnerable Dependencies“), genutzt.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Unzureichende Wartung und Überprüfung der Software- oder Infrastrukturkomponenten Der Quellcode der App und ihres Backends muss offen sein, und die technischen Spezifikationen müssen veröffentlicht werden, damit jeder Betroffene den Code prüfen und gegebenenfalls zur Verbesserung des Codes, zur Korrektur möglicher Fehler und zur Gewährleistung der Transparenz bei der Verarbeitung personenbezogener Daten beitragen kann.	D-**Fehler! Verweisquelle konnte nicht gefunden werden.**-2	CCC, Ziffer 4 EDSA-Leitlinien für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung, Anhang GEN-3	✓ Das EFGS beruht auf dem Open-Source-Prinzip und ist unter Apache 2.0 lizenziert. ✓ Damit das EFGS und seine Infrastruktur durch Auditoren, Aufsichtsbehörden und die kritische Öffentlichkeit überprüft werden kann, muss der vollständige Quellcode öffentlich verfügbar sein.	Github-Dokumentation

2.2 Unsachgemäße Nutzung

Durch die folgenden Designentscheidungen und -Bewertungen soll das Risiko der Betroffenen infolge einer unsachgemäßen Nutzung der App reduziert werden.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Unterstützung der Mitgliedstaaten Die Kommission muss Unterstützung für sämtliche Federation Gateway Services zur Verfügung stellen.	D-2.2-3	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (10) – (12)	**Die Kommission bietet:** ✓ Support aller Federation Gateway-Services in englischer Sprache rund um die Uhr per Telefon, E-Mail oder Webportal sowie die Annahme von Anrufen von autorisierten Personen, darunter Koordinatoren der Gateway Services und ihre jeweiligen Helpdesks, Projektleiter und designierte Mitarbeiter der Kommission; ✓ Unterstützung der Datenverantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen, soweit dies möglich ist, zwecks Erfüllung ihrer Verpflichtungen dahingehend, Anfragen zur Ausübung der in Abschnitt III DSGVO festgelegten Rechte der betroffenen Person zu bearbeiten. ✓ Support der Datenverantwortlichen durch Bereitstellung von Informationen zum Federation Gateway, um die Verpflichtungen gemäß den Artikeln 32, 35 und 36 DSGVO umzusetzen.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Die zentrale Server-Infrastruktur funktioniert nicht ordnungsgemäß Das Vertrauen in den zentralen Server ist höchstwahrscheinlich begrenzt. Beim Management des zentralen Servers müssen klar definierte Governance-Regeln eingehalten und alle erforderlichen Maßnahmen zur Gewährleistung seiner Sicherheit integriert werden. Seine Positionierung sollte eine effektive Überwachung durch die zuständige Aufsichtsbehörde ermöglichen.	D-2.2-4	EDSA-Richtlinien 04/2020, Kontaktnachverfolgungs-Tools, Anhang PRIV-5	✓ Das Management des EFGS-Servers folgt klar definierten Governance-Regeln und muss alle erforderlichen Maßnahmen zur Gewährleistung seiner Sicherheit integrieren.	Sicherheitsstandards für alle Informationssysteme der Europäischen Kommission

2.3 Verlust des öffentlichen Vertrauens in Kontaktnachverfolgungs-Apps

Da Kontaktnachverfolgungs-Apps von der Freiwilligkeit und Kooperationsbereitschaft eines möglichst großen Teils der Bevölkerung abhängig sind, müssen Designentscheidungen darauf ausgerichtet sein, einen Vertrauensverlust seitens der Bevölkerung zu vermeiden.

Die entsprechenden Designentscheidungen und -Bewertungen sind unten aufgeführt.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Datengenauigkeit: Zur Gewährleistung der Datengenauigkeit implementierte Maßnahmen sind im interoperablen System zu pflegen.	D-2.3-1	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 20	**Audit-Schnittstelle und Integrität** ✓ Die Audit-Schnittstelle bietet Funktionen zur Prüfung von Teilen des Dienstes durch externe Nutzer, um die Integrität des IT-Systems zu überprüfen. ✓ Dieses Audit-Verfahren bietet die Möglichkeit, die Integrität ganzer Datei-Batches zu verifizieren. Dabei werden spezifische Informationen zurückgegeben, zum Beispiel: • Im Batch enthaltene Länder • Batch-Signaturen nach Land • Upload-Infos • Signatur-Infos • Betreibersignaturen All diese Informationen können bei den Zertifizierungsstellen oder über die übertragenen Zertifikatsinformationen (im Fall eines selbstsignierten Zertifikats) geprüft werden. ✓ Der Begriff Integrität bezieht sich hier auf die Anforderung, dass Datenstrukturen und	eHealth Network, Guidelines Interoperability Specifications, Chapter 5.7, 6.1.3 eHealth Network European Interoperability Certificate Governance

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			Inhalte weder versehentlich noch absichtlich beeinträchtigt werden dürfen. Dies lässt sich erreichen, indem man die Client-Identität sowie die hochgeladenen Daten auf ihre Gültigkeit überprüft. Da die vom Roaming-Service gespeicherten Daten bei der Verarbeitung auf der Anwendungsschicht verschlüsselt werden, ist die Gültigkeit der heruntergeladenen Informationen garantiert. ✓ Vertrauen und Integrität lassen sich verbessern, wenn jeder Schlüssel von den nationalen Backend-Systemen signiert wird. Auf diese Weise können hochgeladene Daten von allen Personen validiert werden, die sie herunterladen. Beachten Sie, dass dieser Schritt zu einem gesteigerten Datenverkehr und höheren Validierungsaufwand führt.	
Support der EU-Kommission Die Kommission unterstützt das eHealth-Netzwerk in Bezug auf die Vereinbarung der technischen und organisatorischen Compliance der nationalen Behörden mit den	D-2.3-2	Durchführungsbeschluss (EU) 2020/1023, Artikel 1 (3) (6)	**Notwendige Prüfungen und Audits** ✓ Notwendige Tests werden von der Kommission und den Mitgliedsstaaten durchgeführt, bevor diese am EFGS teilnehmen.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Anforderungen für den grenzüberschreitenden Austausch personenbezogener Daten im Federation Gateway, und zwar durch **Bereitstellung und Durchführung der erforderlichen Tests und Audits**.				
Die Effizienz der **technischen** und **organisatorischen Maßnahmen** zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten innerhalb des Federation Gateways **ist von der Kommission sowie denjenigen nationalen Behörden regelmäßig zu überprüfen und zu bewerten, die Zugang zum Gateway** haben.	D-2.3-3	Durchführungsbeschluss (EU) 2020/1023, Artikel 7a (6)	**Onboarding zum EFGS** ✓ Als Teil des e-Health-Netzwerkprozesses wurde ein Onboarding-Prozess definiert. Antragsteller stellen formal einen Antrag mittels eines Formulars nebst Anlagen. Antragsteller haben eine ausgefüllte Checkliste vorzulegen, die auch datenschutzrechtliche Anforderungen an die Teilnahme am EFGS beinhaltet. Daraufhin entscheiden die Mitgliedstaaten als „Gemeinsame Verantwortliche“ über den Antrag zur Teilnahme am EFGS.	
Definition des Datenfeldes „ReportType“	D-2.3-4	Durchführungsbeschluss (EU) 2020/1023, Artikel 1 (1) (l)	**Selbst gemeldete Testergebnisse** ✗ Es muss geklärt werden, ob selbst gemeldete Testergebnisse wirklich als gültige Daten im	DSFA-Bericht, Abschnitt 14.2.3.1

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Dieses Datenfeld gibt Aufschluss darüber, auf welche Art und Weise die Bestätigung einer Infektion mit COVID-19 erfolgt ist, also, ob dieser Umstand vom App-Nutzer selbst gemeldet oder durch die nationale Gesundheitsbehörde bzw. mit einem Labortest festgestellt wurde. Wenn ein roamender App-Nutzer positiv getestet wird (entweder von einer Gesundheitsbehörde oder einem akkreditierten Testanbieter), hat die zuständige Behörde einen interoperablen und zeitnahen Mechanismus bereitzustellen, um dem Nutzer die Bestätigung der Infektion über seine App zu ermöglichen. Wenn der App-Nutzer das Testergebnis eigenständig und ohne Überprüfung durch eine Regierungsbehörde melden kann, ist das Risiko eines Missbrauchs sehr hoch. Für die Länder, die in der App nur behördlich verifizierte positive Testergebnisse zulassen, würde ein neues Risiko entstehen. Denn der		Im Gegensatz dazu: eHealth Network Interoperability guidelines for approved contact tracing, Chapter III.3	System erfasst werden sollen. Falls ja, muss die Kommission ein Verfahren bereitstellen, um zu überprüfen, welchen Prüfungstyp der jeweilige Mitgliedstaat verwendet und ob dieser die Anforderungen erfüllt. **CWA verteilt nur Testergebnisse mit Attestierung** ✓ Für die CWA ist diese Entscheidung getroffen worden. Der CWA Server verteilt nur Positivschlüssel an die CWA Apps, denen eine Attestierung durch ein Labor oder eine Testeinrichtung zugrunde liegt (CWA-Designentscheidungen, D-5.1-8a). **Verpflichtung zur Überprüfung positiver Testergebnisse durch eine Regierungsbehörde** ✗ Für Teilnehmer des European Federation Gateway Service muss ein sicherer und vertrauenswürdiger Onboarding-Prozess eingerichtet werden. Dieser sollte unter anderem „Regeln“ für den Datenaustausch sowie Mindestanforderungen an die Datenqualität integrieren. Zu den zu vermeidenden Szenarien gehören unter anderem solche, bei denen ein Land den	CWA-Designentscheidungen, D-5.1-8a

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Nutzer einer Kontaktnachverfolgungs-App eines Landes, in der das nichtverifizierte positive Testergebnis veröffentlicht werden kann (Land A), könnte z. B. in ein Land reisen, in dem nur durch ein Labor verifizierte Testergebnisse zulässig sind (Land B) und sich beispielsweise in der Cafeteria eines großen Unternehmens aufhalten. Danach könnte er sich in seiner App als positiv auf Covid-19 getestet melden, obwohl dies nicht der Fall ist. Da er die App des Landes A nutzt, könnte er über die Interoperabilitätsfunktion sein falsches positives Testergebnis durch den Upload seiner Diagnoseschlüssel mit den anderen Mitgliedsstaaten teilen. So würden die App-Nutzer, mit denen er in Land B in der Cafeteria qualifizierten Kontakt hatte, falsch über eine Risikobegegnung durch ihre nationale App informiert werden, was im schlimmsten Fall zu der Empfehlung führen könnte, sich in Quarantäne zu begeben.			Daten eines anderen nicht vertraut und diese deshalb aus seinem System ausschließt. Dies wäre besonders dann fatal, wenn es sich um Nachbarstaaten handelt, da Grenzgänger in diesem Fall nicht entsprechend vorgewarnt werden könnten. Daher sollten für alle teilnehmenden Länder eine Verpflichtung zur Überprüfung positiver Testergebnisse durch eine Regierungsbehörde sowie entsprechende Richtlinien festgelegt werden.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Vermeidung von Sicherheits- und Datenschutzverletzungen Um das Vertrauen der Öffentlichkeit in die Sicherheit der App zu gewinnen/zu stärken und den Datenschutz zu gewährleisten, sind mehrere Öffentlichkeitsmaßnahmen erforderlich. Zur Gewährleistung der Sicherheit der CWA-App in der Zukunft wäre es hilfreich, ein Bug-Bounty-Programm einzurichten. Mit ihm können Sicherheitsexperten Prämien verdienen, wenn sie Schwachstellen unterschiedlicher Kritikalität aufdecken. Diese Maßnahme hat sich beispielsweise sehr positiv auf die Akzeptanz des Passwort-Managers KeePass in der Öffentlichkeit ausgewirkt und sollte daher auch in diesem Fall Früchte tragen. Dazu wird empfohlen, die Abschlussberichte für Penetrationstests zu veröffentlichen. Mit diesen kann der Öffentlichkeit demonstriert werden, dass die zuständige Institution um eine kontinuierliche Sicherheit bemüht ist	D-2.3-5		**Teilnahme am Bug-Bounty-Programm** ⚠ Dieses Programm wird von der für die App verantwortlichen Institution gestartet, um Softwarefehler zu identifizieren, zu korrigieren und zu melden. Den Teilnehmern wird als Belohnung ein materieller oder finanzieller Preis in Aussicht gestellt. Die Implementierung eines solchen Programms würde das Vertrauen der Öffentlichkeit in die Sicherheit des EFGS deutlich stärken helfen. **Regelmäßige Penetrationstests und Berichtsveröffentlichungen** ⚠ Bei den sogenannten Penetrationstests werden Sicherheitsexperten eingesetzt, die im EFGS nach Schwachstellen suchen, so wie das auch Hacker tun. Diese Tests sollten von verschiedenen Anbietern vorgenommen werden, weil jedes Team eigene Fokus- und Schwerpunkte besitzt. Es empfiehlt sich, sie spätestens vor jeder Veröffentlichung einer neuen EFGS-Version durchzuführen. Die Abschlussberichte für die Penetrationstests werden veröffentlicht.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
bzw. nach Schwachstellen sucht und diese behebt.				

3. Rechtsgrundlage

Die aus der Interoperabilität folgende Datenverarbeitung muss eine Rechtsgrundlage haben, da andernfalls die Verarbeitung personenbezogener Daten rechtswidrig ist.

3.1 Freiwillige Verwendung der nationalen App und Einwilligung zur Datenverarbeitung

Im Folgenden werden die mit der Rechtsgrundlage verbundenen Designentscheidungen dargestellt, mit denen folgende Risiken vermieden werden sollen:

- Unwirksame Zustimmung aufgrund einer fehlenden/falschen ausdrücklichen Einwilligungserklärung (technischer Akt der Einwilligung)
- Unwirksame Zustimmung wegen Nichtzugänglichkeit der erforderlichen Informationen (Sprachbarrieren, mangelndes technisches Verständnis)
- Soweit sich das nationale Recht auf ein öffentliches Interesse stützt, müssen ineffektive Vorschriften möglicherweise angepasst werden
- Nicht autorisierte Verwendung der App durch Minderjährige unter 16 Jahren

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Regelungen Die Verarbeitung personenbezogener Daten unter der Verantwortung der Mitgliedstaaten sollte gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung, DSGVO) sowie der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates erfolgen. **Rechtsgrundlage der Mitgliedsstaaten** Jeder Datenverantwortliche hat sicherzustellen, dass er auf nationaler Ebene über eine rechtliche Grundlage für die Datenverarbeitung im Federation Gateway verfügt.	D-3-1	Durchführungsbeschluss der Kommission (EU) 2020/1023, Artikel 7, 10		
Freiwilliger Charakter Die Nutzung der App sollte erlaubnisbasiert sein und vollständige Informationen über die beabsichtigte	D-3-2	eHealth Network, Common EU Toolbox for Member States, Annex I, SG-02	**Freiwilliger Charakter** Es ist in der Verantwortung der Mitgliedstaatesn die festgelegten Verfahren	CWA-Designentscheidungen Kap. 3.1

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Verarbeitung der Daten enthalten oder auf dem freien Willen der betroffenen Person in einem geeigneten gesetzlichen Rahmen beruhen. Der Austausch von Daten über Einzelpersonen, bei denen ein Positiv-Status diagnostiziert oder durch einen Test festgestellt wurde („Infektionsdaten“), sollte mit solchen interoperablen Anwendungen nur durch eine **freiwillige Handlung** des Nutzers ausgelöst werden können. Die betroffenen **Personen** müssen die **Kontrolle über** ihre **Daten** haben.		EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 5	der nationalen Gesundheitsämter in der nationalen App umzusetzen. ✓– Für die Umsetzung in der CWA siehe CWA-Designentscheidungen Kap. 3.1	
Rechtsgrundlage: Soweit sich das nationale Recht auf ein öffentliches Interesse stützt, muss es unter Umständen angepasst werden, um den Datenaustausch mit anderen Ländern zu ermöglichen.	D-3-3	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 12	**Anpassung nationaler Gesetze** Es liegt in der Verantwortung der Mitgliedstaaten, die festgelegten Verfahren der nationalen Gesundheitsbehörden in den nationalen Apps umzusetzen. ✓– Die CWA stützt sich auf die Einwilligung als Rechtsgrundlage der Datenverarbeitung. Eine Anpassung nationaler Gesetze, um	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			Interoperabilität zu ermöglichen, ist daher nicht erforderlich.	
Rechtsgrundlage: Wenn die Zustimmung rechtlich begründet ist, muss eine **zusätzliche Einwilligung** für die im Rahmen der **Interoperabilität erfolgende Verarbeitung** eingeholt werden, die alle Anforderungen an die Wirksamkeit einer Einwilligung erfüllt. Diese muss insbesondere spezifisch und somit ausreichend granular sein.[21] **Rechtsgrundlage**: Soweit es um Gesundheitsdaten geht, findet **Artikel 9 DSGVO** Anwendung und die Verantwortlichen müssen eine der dort aufgeführten Ausnahmebedingungen erfüllen. Die Zustimmung muss die Anforderungen der EDSA-Richtlinien 05/2020 für eine Einwilligung gemäß Verordnung 2016/679 erfüllen.	D-3-4	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 12	**Einwilligung**Es liegt in der Verantwortung der Mitgliedsstaaten die von den Gesundheitsbehörden festgelegten Verfahren in den nationalen Apps umzusetzen. ✓ Die Einholung der Einwilligung wird in den CWA-Designentscheidungen D-3.1-1 beschrieben.	CWA-Designentscheidungen, D-3.1-1

[21] Siehe dazu auch Abschnitt 3.1.3 Granularität der Leitlinien 05/2020 des EDSA über eine Einwilligung im Sinne der Verordnung 2016/679.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Rechtsgrundlage: Wenn sich die für **die** Datenverarbeitung V**erantwortlichen** der Kontaktnachverfolgungs-Apps auf **unterschiedliche Rechtsgrundlagen** stützen, sind unter Umständen zusätzliche Maßnahmen erforderlich, um die Rechte der betroffenen Personen in Bezug auf die betreffende gesetzliche Basis zu implementieren.	D-3-5	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 12	**Zusätzliche Maßnahmen für die Rechtsgrundlage** ✓ Dies ist für die CWA nicht erforderlich.	
Für jede implementierte Maßnahme muss geprüft werden, ob der gleiche Zweck mit einer **weniger einschneidenden Alternative** erfüllt werden kann und diese wirksam und verhältnismäßig ist.	D-3-6	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 22	**Proportionalität** ✓ Im Rahmen des Entwicklungsprozesses zur Anbindung des EFGS an die CWA wurden alternative Lösungen geprüft, Datenschutzrisiken infolge der Anbindung an das EFGS bewertet und in der DSFA beschrieben sowie Designentscheidungen getroffen, die ein durch die Interoperabilität potenziell erhöhtes Datenschutzrisiko minimieren (siehe hierzu die CWA – Designentscheidungen, D-1-1a).	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Prüfung der Rechtmäßigkeit der Rechtsgrundlage Das eHealth-Netzwerk muss die Gesetzmäßigkeit der rechtlichen Grundlage für die Interoperabilitätsverarbeitung bewerten, um Rechtssicherheit und Compliance zu gewährleisten. Wenn einer der Mitgliedstaaten Daten nicht rechtmäßig verarbeitet, kann auch jede nachfolgende Verarbeitung durch andere Mitgliedstaaten rechtswidrig sein. Die Prüfung und Bewertung der Rechtsgrundlage sollte vom **eHealth-Netzwerk sowie den nationalen Behörden durchgeführt werden, die auf den Federation Gateway zugreifen dürfen**.	D-3-7		**Prüfung der Rechtmäßigkeit durch das eHealth-Netzwerk** ✖ Die Rechtsgrundlage des jeweiligen Mitgliedstaates für die mit dem EFGS verbundene Datenverarbeitung muss vom eHealth-Netzwerk geprüft und bewertet werden. ✖ Eine gültige Rechtsgrundlage ist Voraussetzung für den Zugang zum Federation Gateway. Das für die Kommunikation zwischen nationalem Backend- und EFGS-Server erforderliche Zertifikat wird nur ausgestellt, wenn die Rechtsgrundlage vom eHealth-Netzwerk genehmigt wurde. ✖ Dies trifft auch auf die rechtmäßige Nutzung der nationalen App und dementsprechend des EFGS durch unterminierte Nutzer zu.	DSFA-Bericht, Abschnitt 11
Unrechtmäßige Einwilligung Minderjähriger - informierte Entscheidung: Mindestalter	D-3-8		**Einhaltung nationalen und europäischen Rechts** ✓ Die Einhaltung der nationalen Gesetzgebung durch die Einwilligung des einholenden	DSFA-Bericht, Abschnitt 7.4.1.2.3 – informierte Entscheidung: Mindestalter

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Die Bestimmung des Mindest-Einwilligungsalters im Sinne des Datenschutzes bleibt daher der Gerichtsbarkeit der Mitgliedstaaten überlassen. Dies könnte zu folgender Situation führen: Ein Mitgliedstaat holt eine gültige Einwilligung gemäß nationalem Recht ein, die in einem anderen Mitgliedsstaat gegen Gesetze und Vorschriften verstößt.			Mitgliedstaates ist ausreichend, um eine Rechtsgrundlage auch für die Verarbeitung im EFGS und darüber hinaus zu bilden. ✓ Infolgedessen ist jede Einwilligung, die der Gesetzgebung des einholenden Mitgliedstaats entspricht – sofern die Anforderungen geltender europäischer Gesetze erfüllt wurden – eine gültige Rechtsgrundlage für die spätere Verarbeitung durch die anderen am EFGS beteiligten Mitgliedstaaten.	
Fairness: Rechte der betroffenen Person und Widerruf Um die Fairness-Anforderung gemäß Artikel 8 Absatz 2 der Charta zu erfüllen, muss mit der Einwilligung die Souveränität des App-Nutzers als betroffene Person gewahrt werden. Zu diesem Zweck sind Mittel bereitzustellen, die den Widerruf der Einwilligung ebenso einfach machen wie die Gewährung und eine effektive	D-3-9		**Widerruf der Einwilligung** ✓ Artikel 11 Absatz 2, 12 Absatz 2 DSGVO und Artikel 12 Absatz 2, 14 Absatz 2 EU-DVR gestatten dem Datenverantwortlichen, die Verarbeitung personenbezogener Daten so zu gestalten, dass die damit assoziierten natürlichen Personen nicht länger identifizierbar sind. ✓ Das Recht auf Widerruf der Einwilligung entfällt, sobald der Datenverantwortliche nachweisen kann, dass er aufgrund	DSFA-Bericht, Abschnitt 7.4.1.2.5

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Ausübung der Rechte der betroffenen Person.			mangelnder Korrelation zwischen den Verarbeitungsdaten und der Identität hinter den Pseudonymen nicht in der Lage ist, diese Verpflichtungen zu erfüllen. ✓ Das Design der Verarbeitung fokussiert auf der Datenminimierung bzw. Minderung der Korrelation zwischen den gesammelten und verarbeiteten Daten und den dazugehörigen Identitäten. ✓ Folglich gelten die Bestimmungen bezüglich der Rechte der betroffenen Person gemäß Artikel 11 Absatz 2, Artikel 12 Absatz 2 DSGVO und Artikel 12 Absatz 2, Artikel 14 Absatz 2 EU-DVR nicht.	

3.2 Beschränkungen von/zusätzliche Freiheiten bei Nichtnutzung der App bzw. Nutzung der App/erzwungener Einwilligung

Der freiwillige Charakter der Einwilligung der betroffenen Person ist zwingend erforderlich, um eine rechtmäßige Datenverarbeitung zu garantieren. Allerdings besteht ein Risiko dahingehend, dass sich Nutzer aufgrund externen Drucks (Arbeitgeber, Staat, Nachbarn usw.) ggf. gezwungen sehen, die nationale Nachverfolgungs-App zu nutzen.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Einschränkung der Freiheit bei Nichtverwendung der App In bestimmten Situationen kann es vorkommen, dass sich der Nutzer aufgrund von externem Druck oder sogar Zwang dazu veranlasst sieht, die Interoperabilitätsfunktion der App zu verwenden. So könnten Arbeitgeber in Grenzgebieten ihre Mitarbeiter z. B. dazu zwingen, die App zu nutzen und die Interoperabilitätsfunktion zu aktivieren.	D-3.2-1	FifF DSFA, S. 66	✓ Dieses Risiko könnte gemindert werden, indem man die Öffentlichkeit dahingehend sensibilisiert, dass ein jeglicher Zwang zur Nutzung der App eine Straftat darstellt, die mindestens eine Geldstrafe nach sich zieht, und relevante Datenschutzaktivitäten Dritter durch die zuständigen Aufsichtsbehörden der Mitgliedstaaten überwachen lässt. ⚠ Darüber hinaus könnte sich ein solcher Zwang als ineffizient erweisen, wenn betroffene Bürger beispielsweise eine Anwendung installieren, die in ihrem Erscheinungsbild der nationalen App ähnelt, jedoch nur aus Screenshots besteht. Auf diese Weise könnten sie vorgeben, die nationale App zu nutzen und nicht infiziert zu sein.	

3.3 Risiko der Diskriminierung

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Keine Stigmatisierung Das EFGS hat sicherzustellen, dass kein Nutzer die Identität infizierter Menschen oder enger Kontaktpersonen kennt.	D-3.3-1	eHealth Network, Common EU Toolbox for Member States, Annex I, SG-04	**Keine Stigmatisierung** ✓ Das EFGS verwendet ausschließlich stark pseudonymisierte Daten. Eine Identifizierung des Nutzers und folglich die Diskriminierung der betroffenen Person sind nicht möglich.	

3.4 Datenschutz-Folgenabschätzung (DSFA)

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Es müssen mögliche Auswirkungen auf den Datenschutz und die Sicherheit bewertet und angemessene Sicherheitsvorkehrungen getroffen werden.	D-3.4-1	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 3	**Datenschutz-Folgenabschätzung (DSFA)** ✓ Die DSFA umfasst den gesamten Entwicklungsprozess. Darin werden anstehende Datenschutz- und Sicherheitsprobleme diskutiert, bewertet und so weit wie möglich minimiert.	DSFA-Bericht

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Verantwortlichkeit: Eine abschließende Erklärung bezüglich der jeweiligen Rollen der verschiedenen an der Verarbeitung mitwirkenden Akteure ist im Einzelfall auf Grundlage der **tatsächlichen Umstände** der ausgeführten Verarbeitung zu bewerten.	D-3.4-2	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 13	**Durchführung der DSFA** ✓ DSFAs werden im Rahmen der Entwicklung des EFGS ausgeführt.	DSFA-Bericht, Abschnitt 6.2
Verantwortlichkeit: Jeder **Vorgang** oder jede Vorgangsreihe, die der Sicherstellung der Interoperabilität **dient** und **zusätzlich zur Verarbeitung** für die Zwecke der Funktionalität von Anwendungen auf Mitgliedstaatsebene erfolgt, ist **getrennt** von den vorherigen oder anschließenden Verarbeitungsvorgängen zu bewerten, weil es sich um einen **zusätzlichen Zweck** handelt. Diese zusätzliche Verarbeitung sollte daher als gesonderter Vorgang betrachtet werden.	D-3.4-3	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 14	**Zusätzliche DSFA für die Datenverarbeitung im Zusammenhang mit EFGS** ✓ Der DSFA-Entwurf soll als Grundlage für die Datenschutzfolgenabschätzung der Mitgliedsstaaten für die Implementierung des EFGS dienen. ✓ Eine zusätzliche DSFA für die Datenverarbeitung bei Anbindung der CWA an das EFGS wurde durchgeführt.	
Verantwortlichkeit/DSFA: Die gemeinsame Verantwortlichkeit wirkt sich auf den Umfang der DSFA aus. Die DSFA für Datenverarbeitungen als	D-3.4-4	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 15	**Erwägung einer gemeinsamen Verantwortlichkeit**	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
gemeinsame Verantwortliche im Rahmen EFGS ist zusammen mit der DSFA für die Implementierung des EFGS in die nationalen Apps durchzuführen.			✓ Transaktionen vom nationalen Backend- zum EFGS-Server wird in der DSFA Rechnung getragen. ✓ Außerdem wird darin eine Prognose der Auswirkungen vertraglicher Abhängigkeiten vorgenommen. ✓ Die Ausübung der Rechte der betroffenen Person und die Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitungsaktivitäten unter gebührender Berücksichtigung der Verantwortung der Mitgliedstaaten werden ebenfalls in der DSFA behandelt.	
Informationssicherheit/DSFA: In der **Datenschutz-Folgenabschätzung** ist insbesondere auf die mit der Interoperabilität verbundenen Sicherheitsrisiken einzugehen, die **Auswirkungen auf die Rechte und Freiheiten** natürlicher Personen haben.	D-3.4-5	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 18	**Berücksichtigung von Maßnahmen zur Minderung von Sicherheitsrisiken** ✓ In Bezug auf Architektur- und Entwicklungs-Workstreams wurden individuell diskutierte Sicherheitsrisiken angesprochen. Aus diesem Grund fanden tägliche Besprechungen mit Vertretern dieser Workstreams statt.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			✓ Sicherheitsrisiken und Minderungsmaßnahmen sind im DSFA-Bericht nebst Anhängen aufgeführt und beschrieben. ✓ Die Ergebnisse der Beratung durch das DSFA-Team wurden bei der Ausarbeitung der technischen und organisatorischen Maßnahmen der Service-Anbieter berücksichtigt.	
Richtigkeit der Daten: Anbieter, die darüber nachdenken, ihre Anwendungen zur Kontaktnachverfolgung interoperabel zu gestalten, sollten soweit wie möglich sicherstellen, dass dies weder die **Qualität noch die Richtigkeit** der Daten beeinträchtigt. Wo große Abweichungen bestehen, kann die Interoperabilität zu Einbußen bei der Datenqualität (z. B. Falschbeurteilungen, schlechte Risikoeinstufung) und dadurch zu mehr falschen Positivmeldungen führen.	D-3.4-6	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 19	**Risiko einer minderwertigen Datenqualität/-genauigkeit** ✓ Das zunehmende Risiko falscher Positivmeldungen wurde in der DSFA berücksichtigt (z. B. Selbstauskünfte über Testergebnisse).	DSFA-Bericht, Abschnitt 11.2, Tabelle der Risikomatrix
Zusammenarbeit zwischen Datenverantwortlichen	D-3.4-7	Durchführungsbeschluss (EU) 2020/1023, Anhang II, Abschnitt 3	Organisation der Zusammenarbeit von Datenverantwortlichen	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Wenn ein Datenverantwortlicher zur Erfüllung seiner in den Artikeln 35 und 36 DSGVO festgelegten Verpflichtungen Informationen von einem anderen Datenverantwortlichen benötigt, hat er eine spezielle Anfrage an das funktionale Postfach zu senden. Der Empfänger hat sich nach besten Kräften zu bemühen, diese Informationen bereitzustellen.			✓ Es wurde ein gemeinsamer Ausschuss der Datenverantwortlichen innerhalb des eHealth Networks gebildet. Außerdem wurde von jedem teilnehmendem Mitgliedstaat eine funktionale Mailbox eingerichtet.	

4. Transparenz

Die in diesem Abschnitt beschriebenen Designentscheidungen und -Bewertungen dienen in erster Linie der Transparenz. Personenbezogene Daten müssen für die betroffene Person nachvollziehbar erhoben und verarbeitet werden.

Für die verarbeiteten Daten sowie die Funktionalität des EFGS ist in jedem Fall eine größtmögliche Transparenz und Verifizierbarkeit sicherzustellen.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Transparenz und Freiwilligkeit	D-4-1	EDSA-Leitlinien 04/2020, Kontaktnachverfolgungs-	**DSFA, DSK und Entwurfsentscheidungen**	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Die Nutzer müssen über alle erfassten personenbezogenen Daten informiert werden. Diese Daten dürfen nur mit ihrer Einwilligung erhoben werden. Die betroffenen **Personen** sind, wie üblich, über jegliche **zusätzliche Verarbeitung** ihrer personenbezogenen Daten und die daran **beteiligten Parteien** aufzuklären. Für die Nutzer muss stets **klar ersichtlich** sein, was die Benutzung der Anwendung mit sich bringt. Dazu sollten sie stets die **Kontrolle über ihre Daten** behalten. Spätestens zu dem Zeitpunkt, zu dem einer oder alle Datenverantwortlichen personenbezogene Daten erlangt/erlangen, sind der betroffenen Person **klare Informationen** über die zusätzliche Verarbeitung zu geben, die sich durch die Nutzung der Interoperabilität ergibt. Zu diesem Zeitpunkt muss der Nutzer über die		Tools, Anhang, DATA-8, EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffern 9, 10	✓ Die Berichte zu DSFA, Datenschutzkonzept (DSK) und Designentscheidungen werden veröffentlicht, um die Nutzer über alle Verarbeitungsaktivitäten bezüglich ihrer personenbezogenen Daten zu informieren. ✓ Es wird ein Entwurf der Datenschutzrichtlinie bereitgestellt, der alle Verarbeitungsaktivitäten beschreibt.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Bedingungen und den Umfang der Datenverarbeitung informiert werden.				
Transparenz und Bewertung Der **Quellcode** der App und ihres Backends muss **offen** sein, und die technischen Spezifikationen müssen veröffentlicht werden, damit jeder Betroffene den Code prüfen und gegebenenfalls zur Verbesserung des Codes, zur Korrektur möglicher Fehler und zur Gewährleistung der Transparenz bei der Verarbeitung personenbezogener Daten beitragen kann.	D-4-2	EDSA-Leitlinien 04/2020, Kontaktnachverfolgungs-Tools, Anhang, GEN-3	**Offener Quellcode** ✓ Der Quellcode wird veröffentlicht.	European Federation Gateway Service (EFGS)
Datenschutzinformation Jeder Datenverantwortliche stellt den Nutzern seiner nationalen mobilen Nachverfolgungs- und Warn-App („den betroffenen Personen“) Informationen zur Verarbeitung ihrer personenbezogenen Daten im Federation Gateway zur Verfügung, um	D-4-3	Durchführungsbeschluss (EU) 2020/1023, Anhang II, Abschnitt 1, Unterabschnitt 2 (1), EDSA Interoperabilität von Kontaktnachverfolgungs-Apps , Ziffern 11, 19	**Entwurf für Datenschutzinformation** ⚠ Es wird den teilnehmenden Mitgliedsstaaten ein Entwurf der Datenschutzinformation für CWA-Nutzer bereitgestellt, der alle Verarbeitungstätigkeiten umfasst.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
die grenzüberschreitende Interoperabilität dieser nationalen Apps gemäß Artikel 13 und 14 DSGVO zu gewährleisten. Jeder Datenverantwortliche hat den betroffenen Personen den Inhalt von Anhang II des Durchführungsbeschlusses (EU) 2020/1023, einschließlich der in den Punkten 1 und 2 festgelegten Regelungen bereitzustellen. Die Standardregeln für Transparenz gelten weiterhin. Die Informationen sind **klar und deutlich** formuliert bereitzustellen.[22] Dies gilt auch für Informationen dazu, wie die geteilten Daten von den empfangenden Kontaktnachverfolgungs-App anderer Länder verarbeitet werden. Die zusätzlichen Risiken für die Richtigkeit der Daten müssen klar und				

[22] Siehe dazu auch Abschnitt 3.1.3 Granularität der Leitlinien 05/2020 des EDSA über eine Einwilligung im Sinne der Verordnung 2016/679.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
deutlich an die betroffenen Personen kommuniziert werden.				
Übersicht über Verarbeitungstätigkeiten Die Kommission hat die Verarbeitungsaktivitäten zu protokollieren.	D-4-4	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (16)	**Übersicht über Verarbeitungstätigkeiten** ✓ Die Kommission wird eine Übersicht der Verarbeitungstätigkeiten führen, die im Auftrag des Datenverantwortlichen gemäß Artikel 31 (2) der Richtlinie (EU) 2018/1725 durchgeführt werden.	

5. Nicht-Beobachtbarkeit und Vertraulichkeit

Für essenzielle Maßnahmen zur Verknüpfung von Verarbeitungstätigkeiten mit einem bestimmten Zweck werden im Allgemeinen pseudonymisierte und anonymisierte Daten verwendet. Die Anonymisierung personenbezogener Daten erfordert die vollständige Entfernung jeglicher Verweise auf die dazugehörige Identität. Bei pseudonymisierten Daten bleibt die 1:1-Beziehung zur jeweiligen Identität intakt, obwohl sie möglicherweise komplett hinter den personenbezogenen Daten verborgen bleibt. Zu den gängigen Methoden zur Sicherstellung der Pseudonymisierung gehört die Trennung von Daten, Kommunikationsbeziehungen und Teilprozessen einer Verarbeitungstätigkeit von denen einer anderen Verarbeitungstätigkeit.

Gemäß dem Grundsatz der Vertraulichkeit dürfen personenbezogene Daten nur für bestimmte Zwecke an eine befugte Personengruppe weitergegeben werden. Diese Informationen sind vor unbefugter Änderung zu schützen.

5.1 Anonymität/Pseudonymisierung und verschlüsselte Speicherung von Pseudonymen

Unter Pseudonymisierung versteht man die Verarbeitung personenbezogener Daten in einer Weise, durch die diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Dies alles unter der Voraussetzung, dass diese zusätzlichen

Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die die Zuweisung der personenbezogenen Daten einer identifizierten oder identifizierbaren natürlichen Person verhindern (Artikel 4 (5) DSGVO).

Die per Zufallsgenerator auf dem Smartphone im Exposure Notification Framework (ENF) erstellten Zahlen repräsentieren personenbezogene Daten im Sinne der DSGVO, da eine Beziehung zum Gerätebenutzer hergestellt werden kann. Die nachfolgende Datenverarbeitung im Rahmen des ENF ist pseudonymisiert, da eine direkte Identifizierung nur basierend auf diesen zufälligen Zahlen und ohne Bezugnahme auf ein Smartphone deutlich erschwert wird.

Die Designentscheidungen bezüglich der Pseudonymisierung sind nachstehend ausführlicher dargestellt.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Anonymität Die App sollte dem Nutzer nur mitteilen, ob er dem Virus ausgesetzt war und dies (wenn möglich) ohne Informationen zu anderen App-Nutzern, der Häufigkeit der Kontakte und dem Datum der Exposition preiszugeben. Die von der App übermittelten Informationen dürfen es Nutzern nicht ermöglichen, infizierte Anwender oder deren Bewegungen zu identifizieren. Das System muss so konzipiert sein, dass weder beabsichtigte noch unbeabsichtigte Bewegungs- (Standortnachverfolgung) oder Kontaktprofile (Muster häufiger Kontakte,	D-5.1-1	EDSA-Leitlinien 04/2020, Kontaktnachverfolgungs-Tools, Anhang, PRIV-7, PRIV-8	**Anonymität** Es liegt in der Verantwortung der Mitgliedstaaten, die von den Gesundheitsbehörden festgelegten Verfahren in den nationalen Apps zu implementieren. ✓ Die CWA teilt dem CWA-Nutzer nur mit, ob er dem Virus ausgesetzt war ohne Informationen zu anderen App-Nutzern, der Häufigkeit der Kontakte und dem Datum der Exposition preiszugeben. Siehe hierzu auch CWA-Designentscheidungen D-5.1-1	CWA-Designent-scheidungen, D-5.1-1

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
die auf bestimmte Personen rückführbar sind) erstellt werden können.				
Pseudonymität Die folgenden personenbezogenen Daten sind in einem pseudonymisierten Format an den Federation Gateway zu übermitteln: • mit nationalen Kontaktnachverfolgungs- und Warn-Apps für Mobilgeräte hochgeladene Schlüssel bis zu 14 Tage vor dem Datum des Uploads • mit den Schlüsseln assoziierte Daten gemäß dem Protokoll der technischen Spezifikationen, das im Ursprungsland der Schlüssel verwendet wird • die Verifizierung der Infektion • die relevanten Länder und das Ursprungsland der Schlüssel	D-5.1-2	Durchführungsbeschluss (EU) 2020/1023, Artikel 7a (2), (3)	**Pseudonymisierung** ✓ Neu infizierte Nutzer laden für die vergangenen zwei Wochen bis zu 14 Diagnoseschlüssel hoch. ✓ Alle Diagnoseschlüssel basieren auf dem GAEN-Exportdateiformat für Schlüssel in Version 1.5 ✓ Alle Ländercodes basieren auf ISO 3166-1 ✓ Neben dem Diagnoseschlüssel kann jeder App-Nutzer Angaben zu den besuchten Ländern (relevante Länder) an den nationalen Backend-Server übermitteln. Für die CWA wurde dies nicht vollzogen (siehe CWA – Designentscheidungen D-6-26). Mit diesen Informationen kann jeder Server Austauschinformationen für jeden einzelnen Diagnoseschlüssel mit einem Verifikationstyp und einem Ursprungsland in einem Batch an den Federation Gateway Service übertragen.	eHealth Network European Proximity Tracing, Interoperability Architecture, V. 1.3, Chapter 4.1.3 CWA-Designentscheidungen D-6-26

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Kommunikationssicherheit, Verschlüsselung, Kryptographie 1. Die gesamte Netzwerkkommunikation zwischen App und Backend sollte mit gängigen und öffentlich empfohlenen kryptografischen Bibliotheken verschlüsselt werden. Bei der Kommunikation über Mobilfunk- und WiFi-Netze muss für die Daten bei der Übertragung unbedingt die Transportschichtverschlüsselung verwendet werden. 2. Entwickler sollten bestehende gängige und öffentlich empfohlene kryptografische Algorithmen und Protokolle sowie bewährte Implementierungen einsetzen. Dabei sind insbesondere die Anforderungen für eine sichere Verwendung von Algorithmen und Protokollen (z. B. zufälligen Initialisierungsvektoren oder Nonces) zu beachten. 3. Um solche Angriffe zu verhindern, sind Schutzmaßnahmen gegen die Weiter-/Wiedergabe von Kennungen zu implementieren. Will heißen, Nutzer A	D-5.1-3	eHealth Network, Common EU Toolbox for Member States, Annex I, CS-06 EDSA-Leitlinien 04/2020, Kontaktnachverfolgungs-Tools, Anhang, SEC-2, SEC-4	**Sicherheitsmaßnahmen** ✓ • Client-Zertifikate zur Überprüfung der Identität der nationalen Backend-Server • Ein aktiver Vertrauensmechanismus, mit dem Backend-Server dahingehend konfiguriert werden können, wem sie vertrauen (trusted Whitelist) oder auch nicht (Blacklist). • Protokollierung des Datenzugriffs • Unterbindung von Angriffen durch die Nutzung sicherer Übertragungswege zwischen nationalen Backend- und EFGS-Servern: Transitverschlüsselung mit TLS 1.3, um eine Offenlegung von Nachrichten von außen zu verhindern. Die vertrauliche Kommunikation findet nur zwischen nationalem Backend- und EFGS-Server statt. • Verschlüsselung der Verarbeitungsvorgänge in der Anwendungsschicht • Intrusion Detection und Missbrauchsalarme	eHealth Network European Proximity Tracing, Interoperability Architecture, V. 1.3, Chapter 8.2

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
darf nicht in der Lage sein, eine Kennung von Nutzer B aufzuzeichnen und diese anschließend als seine eigene zu senden.				
Verschlüsselung Die App sollte die bestmögliche Verschlüsselung bieten, um Sicherheit und Datenschutz zu verbessern.	D-5.1-4	eHealth Network, Common EU Toolbox for Member States, Annex I, SG-08	**Verschlüsselung** ✓ Eine VPN-Verbindung ist optional, da bereits eine Transitverschlüsselung via TLS 1.3 implementiert wird. ✓ Transitverschlüsselung mit TLS 1.3 ✓ Die Nutzung einer Verschlüsselungs-Middleware in der Anwendungsschicht ist eine Technik, mit der Daten während der Verarbeitung (lesen/speichern) in der Anwendungsschicht chiffriert/dechiffriert werden können. Auf diese Weise lassen sich Informationen auf Attribut Level in Datenbanken verschlüsselt speichern, obwohl diese keine native Verschlüsselung bieten.	Github - feat: DiagnosisKey encryption in database #131
Keine Nachverfolgung Standortdaten sind für Kontaktnachverfolgungs-Apps weder erforderlich noch empfohlen, da das Ziel nicht darin besteht, den Bewegungen einer	D-5.1-5	eHealth Network, Common EU Toolbox for Member	**Standortdaten** ✓ Mit dem EFGS werden keine Standortdaten verarbeitet.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Person zu folgen oder Vorschriften durchzusetzen. Das Erfassen der Bewegungen einer Person im Kontext von Kontaktnachverfolgungs-Apps würde gegen das Prinzip der Datenminimierung verstoßen und erhebliche Sicherheits- und Datenschutzprobleme verursachen.		States, Annex I, SG-03		
Auf dem Gerät gespeicherte Proximity-Daten Um Privatsphäre und Sicherheit zu verbessern, sollten Proximity-Daten (enge Kontakte) nur auf dem Gerät gespeichert und nach dem vom ECDC empfohlenen epidemiologisch relevanten Zeitraum (14-16 Tage) gelöscht werden. Erst nachdem die Infektion eines Nutzers bestätigt wurde, dürfen seine Daten abhängig von dem vom Mitgliedstaat gewählten System auf den zentralen Server und/oder an die zuständigen Gesundheitsbehörden hochgeladen werden.	D-5.1-6	eHealth Network, Common EU Toolbox for Member States, Annex I, SG-05	**Dezentraler Ansatz** ✓ Proximity-Daten (enge Kontakte) werden nur auf dem Gerät gespeichert. Es liegt in der Verantwortung der Mitgliedsstaaten, die von den Gesundheitsbehörden festgelegten Verfahren in den nationalen Apps umzusetzen.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Kontaktnachverfolgungs-Apps verarbeiten **pseudonymisierte** personenbezogene Daten ihrer Nutzer. Dazu gehören Gesundheitsinformationen, beispielsweise wenn eine Gesundheitsfachkraft die Infektion eines App-Nutzers bestätigt oder Expositionsinformationen vom System verarbeitet werden.	D-5.1-7	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 5	**Pseudonymisierte personenbezogene Daten** Es liegt in der Verantwortung der Mitgliedsstaaten, die von den Gesundheitsbehörden festgelegten Verfahren in den nationalen Apps umzusetzen ✓ Die CWA verarbeitet nur **pseudonymisierte** personenbezogene Daten ihrer Nutzer (siehe CWA-Designentscheidungen, Kap. 5.1	CWA-Designentscheidungen Kap. 5.1
Nur Personen, die von den benannten nationalen Behörden oder offiziellen Stellen autorisiert wurden, dürfen auf im Federation Gateway ausgetauschte personenbezogene Daten von Nutzern zugreifen.	D-5.1-8	Durchführungsbeschluss (EU) 2020/1023, Anhang II, Abschnitt 1, Unterabschnitt 1 (6)	**Befugter Zugriff** ✓ Das EFGS wird von der GD DIGIT (Generaldirektion Informatik (innerhalb der Europäischen Kommission)) gehostet. Nur deren Administrator ist berechtigt, auf personenbezogene Daten zuzugreifen.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Anonymität Die App sollte dem Nutzer lediglich mitteilen, ob er dem Virus ausgesetzt war, und wenn möglich, ohne Angaben dazu zu machen, welche Nutzer involviert sind oder wann und wie oft dies geschehen ist. Die von der App übermittelten Informationen dürfen es Nutzern nicht ermöglichen, infizierte Anwender oder deren Bewegungen zu identifizieren. IDs für die „Kontaktnachverfolgung“ per drahtloser Technologie (z. B. Bluetooth oder Ultraschall) sind möglicherweise nicht zu Personen rückverfolgbar und müssen häufig geändert werden. Aus diesem Grund ist es auch untersagt, IDs mit zugehörigen Kommunikationsdaten wie Push-Tokens, Telefonnummern, verwendeten IP-	D-5.1-9	EDSA-Leitlinien 04/2020, Kontaktnachverfolgungs-Tools, Anhang, PRIV-7, PRIV-8 CCC, Nr. 7 und 8 FifF DSFA, S. 75	**Schutz der Pseudonyme** ✓ Es existieren keine serverseitigen Protokolle, mit denen Nutzer erneut identifiziert werden können. Da nur zwischen nationalem Backend- und EFGS-Server eine Verbindung besteht, werden keine persönlichen IP-Adressen verarbeitet. Bei den Diagnoseschlüsseln selbst handelt es sich um pseudonymisierte Daten. Daher ist mit Hilfe des EFGS keine Deanonymisierung von Nutzern möglich. ✓ Die Kommission verarbeitet die Daten nur nach der Authentifizierung nationaler Back-End-Server auf der Grundlage nationaler Back-End-Server-Zertifikate. ✓ Die Kommission stellt sicher, dass Personen, die Zugriff auf das Federation Gateway haben, identifiziert und authentifiziert werden.	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (3) (a) Durchführungsbeschluss (EU) 2020/1023, Anhang III, (6) (f)

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Adressen, Geräte-IDs usw. zu verbinden oder daraus abzuleiten. **Keine Erstellung zentraler Bewegungs- oder Kontaktprofile** Das System muss so konzipiert sein, dass Bewegungs- (Standortverfolgung) oder Kontaktprofile (Muster häufiger Kontakte, die auf bestimmte Personen zurückgeführt werden können) nicht absichtlich oder unbeabsichtigt erstellt werden können. Methoden wie die zentrale GPS-/Standortprotokollierung oder die Verknüpfung der Daten mit Telefonnummern, Social Media-Konten usw. sind daher grundsätzlich abzulehnen.			✓ Die Kommission überprüft die Rechte für den Zugriff auf das Federation Gateway, falls eine Sicherheitsverletzung in Bezug auf diese Infrastruktur eintritt.	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (6) (g)
			✓ Die Kommission setzt technische und organisatorische Sicherheitsmaßnahmen um, um unbefugten Zugriff auf personenbezogene Daten zu verhindern.	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (6) (j)
	D-5.1-10		**Anonymität / Pseudonymität der Nutzer innerhalb der nationalen App** ✓ Nutzer bleiben innerhalb des nationalen App-Systems anonym, solange ihre TEK (Temporary Exposure Keys oder temporäre Expositionsschlüssel) auf ihrem Smartphone verbleiben. Sobald TEKs (im Falle eines positiven Testergebnisses) auf den Server	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			hochgeladen werden, wird aus Anonymität Pseudonymität. Die TEKs der letzten 2 Wochen werden ab dem Zeitpunkt, zu dem das Testergebnis positiv ist, als Diagnoseschlüssel bezeichnet.	
	D-5.1-11		✓ Die Daten zur Exposition einer infizierten Person (Expositionen) verbleiben lokal auf dem Gerät und werden nicht weitergegeben (dezentrale Lösung).	
	D-5.1-12		**Neuidentifizierung positiver Schlüssel nur per Smartphone** ✓ Wenn der hochgeladene positive Schlüssel verfügbar ist, können alle Rolling Proximity Identifiers (RPIs) eines bestimmten Tages einem einzelnen positiven Schlüssel zugewiesen werden. Es ist jedoch nicht möglich, diesen positiven Schlüssel bestimmten Personen zuzuweisen, die die App oder IMEI (International Mobile Equipment Identity) ihres Smartphones verwenden, ohne Zugriff auf den sicheren Speicher des Geräts (Smartphones) zu haben.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
	D-5.1-13	EDSA-Leitlinien 04/2020, Kontaktnachverfolgungs-Tools, Anhang, PRIV-10	**Härtung der Neuidentifizierung durch die Trennung von positivem Schlüssel und Transport-Metadaten** ✓ Wenn der Nutzer seine positiven Schlüssel hochlädt, werden die Transport-Metadaten (z. B. die IP-Adresse) entfernt und an einen bestimmten Akteur namens „Transport Metadata Removal“ verschoben.	
	D-5.1-14		**Härtung der Neuidentifizierung durch die Trennung der IT-Infrastruktur** ✓ Die Testergebnisse werden nicht auf dem EFGS-, sondern nur auf dem nationalen Backend-Server gespeichert.	
	D-5.1-15		✓ Der EFGS-Server wird von separaten Teams betrieben, um Identifizierungs-Angriffe durch Administratoren zu erschweren. ✓ Load Balancer des Administrators: • Verwaltet den Zugriff auf das interne Netzwerk der Generaldirektion für Datenverarbeitung • Verarbeitete Daten: Informationen zum Kundenzertifikat zwecks Systemzugriff ✓ Datenbankadministrator:	DCP, Abschnitt 5.9.1, Rollen für Betreiber der Anwendung

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			• Backup-/Schemaänderungen und Nutzerzuweisung • Verarbeitete Daten: Nutzer, Kennwörter, alle Daten der Datenbank ✓ Webserveradministrator: • Verwaltet die Einrichtung des Webservers • Verarbeitete Daten: Softwarezugriff	

5.2 Grundlegender Datenschutz

Entwurfsentscheidungen zur Gewährleistung einer grundlegenden Privatsphäre sind nachstehend zusammengefasst.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Grundlegender Datenschutz Die gesellschaftliche Akzeptanz kann nur mit einem überzeugenden Konzept erreicht werden, das auf dem Prinzip der Privatsphäre beruht.	D-5.2-1	CCC, Nr. 3 EDSA-Richtlinien, Kontaktnachverfolgungs-	✓ Das EFGS lässt keine direkte Nutzeridentifikation zu.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Gleichzeitig muss die Privatsphäre der Nutzer mit überprüfbaren technischen Maßnahmen wie Kryptografie- und Anonymisierungstechnologien gewährleistet werden. Es reicht nicht aus, sich auf organisatorische Maßnahmen, „Vertrauen“ und Versprechen zu verlassen. Organisatorische oder rechtliche Hürden des Datenzugriffs können im gegenwärtigen sozialen Klima des Notstandsgedanken und als mögliche weitreichende Ausnahmen von Verfassungsrechten durch das Infektionsschutzgesetz nicht als ausreichend angesehen werden. Eine Beteiligung von Unternehmen, die Überwachungstechnologien zum Zwecke des „Covid Washing“ entwickeln, wird abgelehnt. Grundsätzlich sollten Nutzer keiner Person oder Institution ihre Daten „anvertrauen“ müssen, sondern von einer dokumentierten und bewährten technischen Sicherheit profitieren. Es ist möglich, dass eine Identifizierung von Nutzern bei der Nutzung des Service im EFGS nicht zulässig ist.		Tools, Anhang PRIV-2		

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
	D-5.2-2		✓ App Nutzer interagieren nicht mit dem EFGS und müssen sich deshalb auch für keinen Prozess des EFGS identifizieren.	
	D-5.2-3		✓ Die Verbindungen von und zur Datenbank selbst werden nicht verschlüsselt. Um die Vertraulichkeit zu gewährleisten, werden bestimmte Daten durch die Anwendungsschicht verschlüsselt gesichert. ✓ Mit dieser Verschlüsselungs-Middleware können die Daten während der Verarbeitung in der Anwendungsschicht verschlüsselt und entschlüsselt werden. Auf diese Weise lassen sich verschlüsselte Informationen in Datenbanken speichern, die keine native Verschlüsselung bieten.	eHealth Network European Proximity Tracing, Interoperability Architecture, V. 1.3, Chapter 8.2 DSK, Abschnitt 4.5.7.2
	D-5.2-4	EDSA-Richtlinien, Kontaktnachverfolgungs-Tools, Anhang SEC-5	✓ Der EFGS-Server speichert keine Netzwerkverbindungskennungen (z. B. IP-Adressen) von Nutzern, auch nicht von solchen, die positiv getestet wurden und ihre Kontakthistorie oder eigenen Kennungen übertragen haben. Grund dafür ist, dass keine Kommunikation mit dem Nutzer erfolgt, sondern lediglich mit dem nationalen Backend-Server.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
	D-5.2-5		✓ Die auf den EFGS-Server geladenen Diagnoseschlüssel enthalten keine Nutzermetadaten. Dies verringert das Risiko, dass ein Angreifer diese Informationen weiter verknüpfen kann.	
Verarbeitete Protokolldaten Daten in Server-Protokollen müssen minimiert werden und den Datenschutzanforderungen entsprechen.	D-5.2-6	EDSA-Richtlinien, Kontaktnachverfolgungs-Tools, Anhang ID-5	**Protokolldaten** ✓ Die Definition von Protokolldaten lautet wie folgt: „Protokolldaten“ sind eine automatische Aufzeichnung eines Vorgangs im Zusammenhang mit dem Austausch von über das Federation Gateway verarbeiteten Daten und den Zugriff darauf, aus der insbesondere die Art der Verarbeitung, das Datum und die Uhrzeit der Verarbeitung sowie die Kennung der Person, die die Daten verarbeitet, hervorgehen. ✓ Die pseudonymisierten personenbezogenen Daten, die über den Federation Gateway ausgetauscht und verarbeitet werden, dürfen nur folgende Informationen enthalten: Protokolldaten, die den Schlüsseln gemäß dem in ihrem Ursprungsland verwendeten Protokoll für technische Spezifikationen zugeordnet sind. ✓ Um die Audit-Anforderung zu erfüllen, müssen alle Anfragen beim EFGS ein Audit-Modul durchlaufen. Dabei wird ein Prüfbericht mit Protokolldateien,	Durchführungsbeschluss (EU) 2020/1023, Artikel 1 (1) (o), 7a (3) (b) DSK, Abschnitt 5.6.3.2 Daten in der Protokolldatei „webserver“ Github - Softwaredesign European Federation Gateway Service - Audit-Protokollierung

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			Ereignisströmen oder Tabellen in der Datenbank erstellt. Diese Daten können über Standard-Visualisierungstools wie Tableau, Kibana, Splunk, Grafana usw. auf einem Dashboard angezeigt werden. ✓ Bei den in der Webserver-Protokolldatei gespeicherte Daten handelt es sich um das Uploader-Batch-Tag (Upload-Protokollierung) und das Batch-Tag (Batching-Protokollierung). Bei einem „Batch“ handelt es sich um einen Stapel Diagnoseschlüssel.	
	D-5.2-7		✓ In Protokolldateien werden keine persönlichen Daten gespeichert. Die EFGS Software integriert zwei Typen von Protokollen: • Tomcat-Protokoll via Konsole • EFGS-Protokoll via Datei Diese Protokolldateien werden 90 Tage lang beibehalten. Danach werden sie von der Software automatisch gelöscht.	DSK, Abschnitt 4.7.2

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
	D-5.2-8		**Teilung der empfangenen Diagnoseschlüssel** ✓ Die Upload-Schnittstelle besteht aus einem Aufruf zum Hochladen eines Satzes von Diagnoseschlüsseln ✓ Hochladen von Diagnoseschlüsseln, Zweck: Bereitstellung der Diagnoseschlüssel dieses Landes für den EFGS ✓ Aufteilung der empfangenen Stapel mit Diagnoseschlüsseln in einzelne Zeilen in der EFGS-API ✓ Die API speichert Diagnoseschlüssel in der EFGS-Datenbank in einzelnen Zeilen ✓ Technischer Zweck: vermeidet Lücken in der Abfrageleistung, sorgt für Flexibilität, Datenabfrage ist einfacher, Erkennung von doppelt hochgeladenen Schlüsseln, Datennormalisierung ✓ Datenschutzvorteil: Diagnoseschlüssel werden separat verarbeitet und können nicht einzelnen Nutzern zugeordnet werden	DSK, Abschnitt 5.8 Datenverarbeitung

6. Datenminimierung

Im Folgenden werden Entwurfsentscheidungen beschrieben, die der Datenminimierung dienen. Dementsprechend müssen personenbezogene Daten adäquat und zweckdienlich sein und sich auf die Zwecke der Verarbeitung beschränken.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Datenminimierung und Mindestberechtigungen Entwickler sollten die Anwendungsberechtigungen so weit wie möglich einschränken, die verarbeiteten Daten minimieren und wo möglich pseudonymisieren und/oder anonymisieren, jegliche verbleibenden vertraulichen Daten schützen, die von der Anwendung oder dem Backend verarbeitet werden, und diese löschen, wenn sie nicht mehr benötigt werden. Sensible Daten können persönliche Informationen, Gesundheitsinformationen, kritische Sicherheitsdaten, Metadaten usw. umfassen.	D-6-1	eHealth Network, Common EU Toolbox for Member States, Annex I, CS-03	**Kernentitäten** ✓ Diagnoseschlüssel: Ein TEK gemäß GAEN-Format ✓ Batch: Ein Satz von Diagnoseschlüsseln ✓ Upload Tag: Eindeutiger logischer Name für Uploads ✓ Name des Batch Tags: Nur für Downloads relevant ✓ Es werden nur notwendige Daten verarbeitet und so schnell wie möglich gelöscht ✓ Diagnoseschlüssel sind pseudonymisierte personenbezogene Daten, die keine erneute Nutzeridentifizierung zulassen ✓ Es werden keine Metadaten verarbeitet, mit denen der Nutzer erneut identifiziert werden könnte	Github - Software Design European Federation Gateway Service - Core Entities

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Tauschen Sie nur die erforderlichen **Mindestinformationen** aus. Das Ziel der Interoperabilität sollte nicht als Argument dafür verwendet werden, die Erhebung personenbezogener Daten über das Notwendige hinaus zu erweitern. Wenn personenbezogene Daten über den Federation Gateway ausgetauscht werden, beschränkt sich die Verarbeitung auf den Zweck, die Interoperabilität der nationalen mobilen Kontaktnachverfolgungs- und die Warn-Apps innerhalb des Federation Gateways sowie die Kontinuität der Kontaktnachverfolgung in einem grenzüberschreitenden Kontext zu erleichtern.	D-6-2	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps , Ziffern 2, 5; eHealth-Interoperabilitätsleitlinien, Abschnitt I.4., Definition der Interoperabilität; Durchführungsbeschluss (EU) 2020/1023, Artikel 7a (1) EDSA-Richtlinien, Kontaktnachverfolgungs-Tools, Anhang DATA-5, DATA-7	**Nur Mindestinformationen** ✓ Es werden nur Pseudonyme hochgeladen, die nicht auflösbar sind ✓ Die Korrelation zwischen den Diagnoseschlüsseln und der Identität der dazugehörigen natürlichen Person wird so weit wie möglich verborgen ✓ Es werden so wenige Daten wie möglich protokolliert und verarbeitet ✓ Daten werden gelöscht, sobald sie nicht mehr benötigt werden	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Die Bearbeitung durch die Kommission umfasst Folgendes:	D-6-3	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (3)	**Die Bearbeitung durch die Kommission umfasst Folgendes:**	
Authentifizierung Authentifizierung nationaler Backend-Server basierend auf nationalen Backend-Serverzertifikaten.	D-6-4	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (3)	**Nationale Backend-Zertifikate** ✓ **Authentifizierungszertifikat:** Das Zertifikat, das von einem Client (nationales Backend) gesendet wird, wenn gegenseitiges TLS mit dem Federation Gateway Load Balancer ausgeführt wird. Dieses wird zur Authentifizierung des Clients verwendet. ✓ **Unterschriftszertifikat:** Das Zertifikat mit dem öffentlichen Schlüssel, das zur Verifizierung eines Batches mit Diagnoseschlüsseln verwendet wird. Es ist Bestandteil der Batch-Signatur (PKCS#7 Objekt). ✓ **Callback-Zeritifikat/Zertifikat des nationalen Backend-Servers:** Das (Server-) Zertifikat eines nationalen Backends, das für die TLS 1.3-Verbindungen verwendet wird, wenn das nationale Backend Benachrichtigungen (siehe Abschnitt Calback) vom Federation Gateway erhält. Das Zertifikat wird über das Federation Gateway HTTP Proxy verifiziert.	Github - Software Design European Federation Gateway Service - Definitions Github - Software Design European Federation Gateway Service - Client Authentication Github - Software Design European Federation Gateway Service - Certificate Verification during OnBoarding Github - Software Design European Federation Gateway

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			Zertifikat-Daumenabdruck/Fingerabdruck Hash-Wert eines Zertifikats. Wir haben die SHA-256 Hashfunktion zur Berechnung des Fingerabdrucks definiert. In diesem Dokument werden Zertifikat-Hash, Zertifikat-Fingerabdruck und Zertifikat-Daumenabdruck synonym verwendet. **Client-Authentifizierung** ✓ Der Prozess, bei dem ein Client authentifiziert wird (unter Verwendung seines Authentifizierungszertifikats) und die Berechtigung erhält, den Upload/Download eines Diagnoseschlüssels anzufordern. ✓ Der EFGS Load Balancer authentifiziert die Clients (nationale Datenbanken) via mTLS. Danach werden die Client-Anforderungen an das EFGS weitergeleitet, der das Zertifikat der Client-Authentifizierung anhand einer Whitelist in der Datenbank überprüft. Sobald das Zertifikat erfolgreich verifiziert wurde, leitet der Service die Anforderungen an die entsprechenden Endpunkte weiter (z. B. Upload/Download).	Service - Certificate Handling Github - Software Design European Federation Gateway Service - Certificate Requirements

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			Zertifikatverifizierung während des Onboarding-Prozesses ✓ Der gesamte Onboarding-Prozess wird separat als Teil des gesamten e-Health-Netzwerkprozesses definiert.	
Empfang der folgenden von nationalen Backend-Servern hochgeladenen Daten durch Bereitstellung einer API, die den Upload der relevanten Daten über nationale Backend-Server ermöglicht: • mit nationalen Kontaktnachverfolgungs- und Warn-Apps für Mobilgeräte hochgeladene Schlüssel bis zu 14 Tage vor dem Datum des Uploads • mit den Schlüsseln assoziierte Daten gemäß dem Protokoll der technischen Spezifikationen, das im Ursprungsland der Schlüssel verwendet wird • die Verifizierung der Infektion • die relevanten Länder und das Ursprungsland der Schlüssel	D-6-5	Durchführungsbeschluss (EU) 2020/1023, Artikel 7a (3); Anhang III, (3)	**Datenempfang** ✓ Hochgeladene Diagnoseschlüssel werden 14 Tage lang aufbewahrt. Auch wenn eine temporäre Pufferung bei Verwendung der direkten Weiterleitung theoretisch nicht nötig ist, lohnt sie sich doch aus folgenden praktischen Gründen: 1. Pakete gehen verloren und Backends sind ggf. nicht verfügbar. Gespeicherte Daten machen Download-Wiederholungen möglich. 2. Das Timing der Downloads bleibt den Backends überlassen, d. h. es wird kein fester Zeitplan durchgesetzt. 3. Neu integrierte Länder erhalten alle Daten der letzten 14 Tage auf einmal, sodass keine wichtigen Informationen übersehen werden.	eHealth Network European Proximity Tracing, Interoperability Architecture, V. 1.3, Chapter 4.2 eHealth Network European Proximity Tracing, Interoperability Architecture, V. 1.3, Chapter 4.1.3 DSFA-Bericht, Abschnitt 12.2.3, Verarbeitung inakkurater

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			Da neu infizierte Bürger zunächst bis zu 14 Tagesschlüssel einreichen, können gespeicherte Schlüssel bis zu 28 Tage alt sein. **Übertragung von Metadaten für Diagnoseschlüssel** • Den Schlüsseln zugeordneten Protokolldaten gemäß dem Protokoll der technischen Spezifikationen, das im Ursprungsland der Schlüssel verwendet wird; • Die Verifizierung der Infektion; • Relevante Länder und das Ursprungsland der Schlüssel. **Verifizierung der Infektion** Jedes nationale Backend überträgt Austauschinformationen für Diagnoseschlüssel (Schlüssel für Schlüssel) mit einem Verifikationstyp in einem Stapel an den EFGS. Die ReportType-Werte können wie folgt festgelegt werden: UNKNOWN=0; CONFIRMED_TEST=1; CONFIRMED_CLINICAL_DIAGNOSIS=2; SELF_REPORT=3;	personenbezogener Daten Exposure Key export file format and verification

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			RECURSIVE=4; REVOKED=5; ✖ Die selbst gemeldete Verifizierung der Infektion des Nutzers birgt eine hohes Missbrauchsrisiko (siehe oben D-2.3-4). ✓ Für die CWA ist diese Entscheidung getroffen worden. Der CWA Server verteilt nur Positivschlüssel an die CWA Apps, denen eine Attestierung durch ein Labor oder eine Testeinrichtung zugrunde liegt (siehe auch CWA-Designentscheidungen D-5.1-8a). **Relevante Länder und das Ursprungsland der Schlüssel** ✓ Die relevanten oder besuchten Länder müssen von der App mithilfe der Metadaten von Mobilfunkanbietern oder manuellen Nutzereingaben ermittelt werden. ✓ Zusätzlich zum Diagnoseschlüssel kann jeder Nutzer die relevanten Länder an das nationale Backend übermitteln. ✓ Die Werte für das Ursprungsland werden vom nationalen Backend festgelegt. Das Ursprungsland	CWA-Designentscheidungen D-5.1-8a

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			muss bekannt sein, um den Ort des Daten-Downloads zu bestimmen. ✓ Beide Werte werden vom EFGS hochgeladen und verarbeitet. ✓ Die CWA verzichtet auf die Erhebung der relevanten Länder (Siehe auch CWA-Designentscheidungen D-6-2c).	Siehe CWA-Designentscheidungen D-6-2c
Die Bearbeitung durch die Kommission umfasst Folgendes: Speicherung der Daten im Federation Gateway nach dem Empfang von nationalen Backend-Servern.	D-6-6	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (3) (c)	**Sie dazu D-6-5** oben	
Die Bearbeitung durch die Kommission umfasst Folgendes: Verfügbarmachung der Daten durch die nationalen Backend-Server.	D-6-7	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (3) (d)	**Callback-Service** ✓ Das EFGS bietet einen Benachrichtigungs- oder Callback-Service, der die nationalen Backends informiert, wenn ein neuer Batch verfügbar ist. Der Federation Gateway Service sendet die Benachrichtigungen über einen HTTP-Proxy, der mit	Github - Softwaredesign European Federation Gateway Service - Callback eHealth Network European Proximity

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			den nationalen Backends eine gegenseitige Authentifizierung via TLS 1.3 durchführt.	Tracing, Interoperability Architecture, V. 1.3, Chapter 5.6
Die Bearbeitung durch die Kommission umfasst Folgendes: Löschen der Daten nach ihrem Download durch alle teilnehmenden Backend-Server oder 14 Tage nach ihrem Empfang, je nachdem, was zuerst eintritt.	D-6-8	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (3) (e), (f)	**Löschung** ✓ Sie dazu D-6-5 oben ✓ Die Daten bzw. alle dafür vorgesehenen Datensätze werden in einem für alle 6 Stunden geplanten Prozess gelöscht. ✓ Die automatische Löschung von Daten wird durch die Implementierung der Löschroutinen durch einen Cron-Job realisiert. Während des täglichen EFGS-Prozesses erhalten diese Routinen alle zum Löschen erforderlichen Informationen, d. h. alle Daten, die zum Löschen markiert sind. ✓ Das Datenfeld „Created_at“ (Quelle: DFC) wird verwendet, um die zu entfernenden Datensätze auszuwählen. Dieses Feld ist Bestandteil aller Datensätze und wenn der enthaltene Datumswert älter als 14 Tage ist, wird der jeweilige Datensatz vollständig aus dem System gelöscht.	DSK, Abschnitt 4.7

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			✓ Mit dem Ende der Service-Bereitstellung werden alle verbleibenden Daten gelöscht, es sei denn, EU-Recht oder die Gesetzgebung der Mitgliedstaaten verlangt eine fortgesetzte weitere Speicherung der personenbezogenen Daten.	
Um die von der DSGVO geforderte Mindest-Datenteilung bzw. -verarbeitung zu gewährleisten, müssen sich Entwickler von Kontaktnachverfolgungsanwendungen **auf ein gemeinsames Protokoll und kompatible Datenstrukturen einigen**.	D-6-9	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps , Ziffer 8	**Allgemeine Annahmen** ✓ Das eHealth-Netzwerk hat folgende Annahmen vereinbart: • Das typische Datenvolumen pro Land für **neue** Diagnoseschlüssel beträgt zwischen 10 und 20 MB. Nach Schätzungen wird das maximale Volumen weniger als 1 GB pro Tag und Land ausmachen. • Daten werden in Batches alle paar Stunden, **aber nicht in Echtzeit** übertragen • Die **(GAEN)** (Google/Apple Exposure Notification) API wird von allen teilnehmenden Ländern eingesetzt • Für Informationen zu **Diagnoseschlüsseln** wird das GAEN-Format verwendet, inklusive besuchter	eHealth Network European Proximity Tracing, Interoperability Architecture, V. 1.3, Chapter 2.2

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			Länder („relevante Länder“), und zwar für jeden Schlüssel • Länder dürfen Diagnoseschlüssel verarbeiten, verteilen und veröffentlichen. Wenn diese Schlüssel gemäß DSGVO als personenbezogene Daten erachtet werden (rechtliche Überprüfung steht noch aus), muss der Aussteller jedes nationalen Antrags die Einhaltung der DSGVO gewährleisten. • Bürger verwenden die App ihres Heimatlandes • Nationale Apps kommunizieren ausschließlich mit dem jeweiligen nationalen Backend	
Datenhaltung und -minimierung: **Abweichungen** bei den festgelegten **Datenhaltungsfristen** sollten **nicht dazu führen, dass** Daten **länger als unbedingt notwendig** gespeichert werden.[23]	D-6-10	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 17	**Ähnliche Datenhaltungsfristen** ⚠ Mitgliedstaaten sollten, wenn möglich, ähnliche Datenhaltungsfristen verwenden.	

[23] Siehe dazu auch die EDSA-Leitlinien 03/2020 zur Verarbeitung von Gesundheitsdaten zum Zwecke der Forschung im Kontext der COVID-19-Pandemie.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Datenhaltung und -minimierung: Um eine wirksame Anwendung der Datenschutzprinzipien zu fördern, sollten gemeinsame Werte für **Datenminimierung** und **Datenhaltung** angedacht werden.	D-6-11	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 17	**Leitlinien des eHealth-Netzwerks** ✓ eHealth-Netzwerk vereinbart Leitlinien und Architektur für das EFGS ✓ Das eHealth-Netzwerk hat eine gemeinsame Datenhaltungsfrist vereinbart.	eHealth Network European Proximity Tracing, Interoperability Architecture, V. 1.3
Datenhaltung und -minimierung: **Interoperabilität** sollte zu keiner **übermäßigen Informationserfassung** aufgrund eines fehlenden koordinierten Ansatzes führen. Dies muss vor dem Teilend er Daten **klar und deutlich** an die Nutzer kommuniziert werden.	D-6-12	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 17 EDSA-Leitlinien für Tools zur Kontaktnachverfolgung, Anhang PRIV-1	**Verantwortung von Mitgliedsstaaten** ✓ Das eHealth-Netzwerk hat eine gemeinsame Datenhaltungsfrist vereinbart. ⚠ Diese Frist muss von den Mitgliedsstaaten für ihre nationalen Backends implementiert werden. ⚠ Die Speicherung von Daten auf dem EFGS sowie dem nationalen Backend-Server ist in der Datenschutzrichtlinie der nationalen Anwendung transparent zu machen.	
Inkorrekte Entwicklung und Konfiguration	D-6-13	EDSA-Leitlinien für Tools zur	✓ Das EFGS wurde mit größter Sorgfalt entwickelt und konfiguriert, um eine Erfassung unnötiger Daten zu vermeiden.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Anwendung und Server müssen sorgfältig entwickelt und konfiguriert werden, um die Erfassung unnötiger Daten zu vermeiden (z. B. sollten die Serverprotokolle keine Kennungen enthalten usw.).		Kontaktnachverfolgung, Anhang PRIV-17		
Bei Anfragen werden zu viele Informationen vom Server übertragen App-Anfragen an den zentralen Server dürfen keine unnötigen Informationen zum Nutzer enthalten, außer, ggf. und nur bei Bedarf, für ihre pseudonymen Kennungen und Kontaktlisten. Weil keine entsprechenden Verträge vorhanden sind, werden über die Schnittstelle zu viele Daten übertragen, die für ihren Zweck nicht relevant sind.	D-6-14	EDSA-Leitlinien für Tools zur Kontaktnachverfolgung, Anhang PRIV-11, ID-4	✓ Anfragen vom nationalen Backend- an den EFGS-Server dürfen keine unnötigen Informationen über den Nutzer offenlegen. Von der Verarbeitung betroffen sind lediglich ihre pseudonymisierten Kennungen.	
Übertragung von Daten von externen Systemen Das EFGS sollte nur Daten verarbeiten, die von Instanzen der nationalen Backends übermittelt wurden. Es dürfen keine an	D-6-15	EDSA-Leitlinien für Tools zur Kontaktnachverfolgung,	✓ Das EFGS verarbeitet lediglich Daten, die von Instanzen der nationalen Backends übermittelt wurden, aber nicht solche, die an andere Anwendungen und/oder lokalen Kommunikationsgeräte gesendet wurden.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
andere Anwendungen und/oder Geräte der Näherungskommunikation gesendete Daten erfasst werden.		Anhang PRIV-15		
Nachverfolgung der Nutzerbewegungen Es ist möglich, dass der EFGS die Nachverfolgung der Bewegungen von Nutzern nicht zulässt.	D-6-16	EDSA-Leitlinien für Tools zur Kontaktnachverfolgung, Anhang PRIV-3	✓ Das EFGS lässt die Nachverfolgung der Bewegungen von Nutzern nicht zu.	
Standortdaten Mit dem EFGS dürfen zum Zwecke der Kontaktnachverfolgung keine Standortdaten gesammelt werden. Diese dürfen nur zu dem alleinigen Zweck verarbeitet werden, um der App die Interaktion mit ähnlichen Anwendungen in anderen Ländern zu ermöglichen. Dieser Prozess darf dazu nur die zur Zweckerfüllung unbedingt notwendigen Daten verwenden.	D-6-17	EDSA-Leitlinien für Tools zur Kontaktnachverfolgung, Anhang DATA-6	✓ Für die Kontaktnachverfolgung sind keine Standortdaten notwendig, und zwar noch nicht einmal zum Zwecke der Interoperabilität zwischen Mitgliedsstaaten. Es sind lediglich die Werte für das Ursprungsland sowie die relevanten Länder der Diagnoseschlüssel erforderlich.	eHealth Network European Proximity Tracing, Interoperability Architecture, V. 1.3, Chapter 4.1.2

7. Zweckbeschränkung/Unverkettbarkeit

Die folgenden Entwurfsentscheidungen dienen den Schutzzielen der Zweckbeschränkung und der Sicherung der Unverkettbarkeit (siehe CCC, Nr. 9). Personenbezogene Daten dürfen nur für den ursprünglichen Verarbeitungszweck verwendet und nicht mit anderen Daten kombiniert werden. Dementsprechend darf bei der Verarbeitung selbst nur der ursprünglich definierte Zweck verfolgt werden.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Kontaktnachverfolgungs-Apps können im Rahmen einer umfassenden Strategie der öffentlichen Gesundheit zur Bekämpfung der aktuellen Pandemie nur eine **vorübergehende Lösung** sein.	D-7-1	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 22	**Verantwortlichkeit der Mitgliedsstaaten** ⚠ Nationale App und Interoperabilität sollten nur so lange wie nötig zur Bekämpfung der Pandemie verwendet werden.	
Verarbeitungszweck	D-7-2		„Federation Gateway“ bezeichnet einen Netzwerk-Gateway, der von der Kommission mithilfe eines sicheren IT-Tools betrieben wird. Dieses ermöglicht den Empfang, die Speicherung und Bereitstellung eines **Mindestsatzes an personenbezogenen Daten** zwischen den Backend-Servern der Mitgliedstaaten, um die Interoperabilität der nationalen Kontaktnachverfolgungs- und Warn-Apps zu gewährleisten.	Durchführungsbeschluss (EU) 2020/1023, Artikel 1 (1) (j)
Lokale Verarbeitung von Proximity-Daten	D-7-3	EDSA-Richtlinien 04/2020,	✓ Die Proximity-Daten zu einer infizierten Person (Expositionen) verbleiben lokal auf dem Mobilgerät und werden nicht weitergegeben (dezentrale Lösung).	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Die App muss eine Architektur aufweisen, die sich so weit wie möglich auf die Geräte der Nutzer stützt.		Kontaktnachverfolgungs-Tools, Anhang TECH-4	✓ Die von anderen Nutzern über die stromsparende Bluetooth-Schnittstelle empfangenen Rolling Proximity Identifiers (RPI) verbleiben lokal auf dem Mobilgerät im ENF (Exposure Notification Framework) von Apple und Google. Selbst wenn der EFGS-Server gehackt wurde, können diese Informationen nicht zu spezifischen Smartphones rückverfolgt werden. ✓ Die Berechnungen dazu, ob der Kontakt mit einer infizierten Person möglicherweise zu einer Infektion geführt hat, werden lokal auf dem Gerät durchgeführt.	
Gewöhnungseffekt durch Verwendung von nationaler Nachverfolgungs-App und Interoperabilität Diese App darf nicht verwendet werden, um die Gewöhnung an eine dauerhafte Überwachung zu erzielen. Ihre Verwendung muss zeitlich begrenzt sein. Nicht nur ihre Daten, sondern auch die App selbst muss nach einer bestimmten Zeit rückstandslos vom Smartphone entfernt werden (es sei denn, der Nutzer bestätigt ausdrücklich, dass sie beibehalten werden soll).	D-7-4	EDSA-Richtlinien 04/2020, Kontaktnachverfolgungs-Tools, Anhang GEN-1, GEN-2	⚠ Jeder Mitgliedstaat muss ein Verfahren implementieren, um die Erfassung von Kennungen zu unterbinden (allgemeine Deaktivierung der App, Aufforderung zu ihrer Deinstallation, automatische Deinstallation, Einstellung der Interoperabilität usw.) und die Löschung aller erfassten Daten aus allen Datenbanken (mobile Anwendungen und Server) zu veranlassen, sobald die zuständigen Behörden über eine „Rückkehr zur Normalität“ entscheiden.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Die App sollte nur so lange eingesetzt werden, bis die Anzahl der Neuinfektionen ausschließlich mit manuellen Kontaktnachverfolgungstechniken verwaltet werden kann.				
Verhaltensprofilierung und Compliance-Bewertung infizierter Nutzer	D-7-5	FifF DSFA, S. 64	✓ Die Analyse der Kontakte und eine damit verbundene Verhaltensbewertung durch eine zentrale Stelle ist nicht möglich, da die Verarbeitung der Kontakte ausschließlich lokal auf dem Mobilgerät erfolgt. Die Nutzer führen keine Uploads ihres Kontaktverlauf auf den Server hoch.	

8. Intervenierbarkeit

Nach dem Grundsatz der Intervenierbarkeit müssen interessierte Parteien ihre im Rahmen der DSGVO gewährten Rechte uneingeschränkt ausüben können. Die Datenverarbeitung ist so zu gestalten, dass Daten korrigiert und gelöscht werden können. Um diese Rechte in Anspruch nehmen zu können, muss der Nutzer identifizierbar sein. Im Folgenden wird gezeigt, dass die Ausübung der Rechte der betroffenen Person aufgrund der mangelnden Zuordnung zwischen personenbezogenen Daten und Identität unmöglich ist.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Ausübung der Rechte der betroffenen Person: Jede interoperable Lösung muss es der betroffenen Person ermöglichen, ihre Rechte auszuüben. **Ausübung der Rechte der betroffenen Person:** Wenn die Ausübung von Rechten möglich ist, sollte den betroffenen Personen dies so einfach wie möglich gemacht werden. Dazu muss **klar sein, an wen** sie sich bezüglich der **Ausübung ihrer Rechte** wenden müssen.	D-8-1	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 16 EDSA-Richtlinien 04/2020, Kontaktnachverfolgungs-Tools, Anhang PRIV-13	**Respekt für die Rechte der betroffenen Person** ✓ Die betroffenen Personen werden über ihre Rechte und deren Ausübung in Form der Datenschutzerklärung in der nationalen App aufgeklärt.	DSFA-Bericht, Abschnitt 11.10
Ausübung der Rechte der betroffenen Person: Einschränkungen der Ausübung der Rechte von betroffenen Personen sind im Rahmen der in den **Artikeln 11 und 23 DSGVO** festgelegten Ausnahmen möglich.	D-8-2	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 16	**Keine Korrelation mit Identitäten** ✓ Die im EFGS stattfindende sowie die anschließende Verarbeitung betreffen Pseudonyme, die nicht mehr länger mit Identitäten korreliert sind. ✓ Dies führt dazu, dass die Datenverantwortlichen nicht in der Lage sind, die Rechtmäßigkeit eines Anspruchs in Bezug auf die Rechte der betroffenen Person oder den Widerruf einer Einwilligung festzustellen.	DSFA-Bericht, Abschnitt 11.10.1

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Rechte der betroffenen Person Die in den Artikeln 15 bis 20 der DSGVO genannten Rechte gelten daher möglicherweise nicht, wenn die Bedingungen gemäß Artikel 11 dieser Verordnung erfüllt sind.	D-8-3	Kommission Durchführungsbeschluss (EU) 2020/1023, Artikel 13	**Artikel 11 DSGVO** ✓ Dementsprechend gelten gemäß Artikel 11 Absatz 2, Artikel 12 Absatz 2 DSGVO und Artikel 12 Absatz 2, Artikel 14 Absatz 2 EU-DVR die Bestimmungen über die Rechte der betroffenen Person nicht und die Datenverantwortlichen sind berechtigt, Ansprüche bezüglich solcher Rechte abzulehnen.	
Verantwortung für Anfragen von betroffenen Personen Jeder Datenverantwortliche fungiert als Kontaktstelle für die Nutzer seiner nationalen mobilen Kontaktnachverfolgungs- und Warn-App und bearbeitet alle Anfragen im Zusammenhang mit der Ausübung der Rechte von betroffenen Personen gemäß DSGVO, die von diesen Nutzer oder ihren Vertretern eingereicht werden. Jeder Datenverantwortliche benennt eine spezifische Kontaktstelle für Anfragen von betroffenen Personen.	D-8-4	Durchführungsbeschluss (EU) 2020/1023, Anhang II, Abschnitt 1, Unterabschnitt 2 (2)	**Verantwortung als gemeinsame Datenverantwortliche** ✓ Die gemeinsamen Datenverantwortlichen haben ihre jeweiligen Verantwortlichkeiten gemäß Durchführungsbeschluss (EU) 2020/1023 geregelt. ✓ Die Verteilung der Zuständigkeiten auf die gemeinsamen Datenverantwortlichen hat aufgrund der Verbindlichkeit des Durchführungsbeschlusses (EU) 2020/1023 und seiner Veröffentlichung öffentlichen Charakter. ✓ Wenn ein gemeinsamer Datenverantwortlicher eine Anfrage von einer betroffenen Person erhält, die nicht in seine Verantwortung fällt, leitet er diese unverzüglich an den zuständigen Datenverantwortlichen weiter.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			✓ Auf Wunsch unterstützen sich die gemeinsamen Datenverantwortlichen gegenseitig bei der Bearbeitung der Anfragen von betroffenen Personen und antworten einander unverzüglich und spätestens 15 Tage nach Eingang einer Bitte um Unterstützung.	
Respekt für die Rechte der betroffenen Person Der Schutz der Rechte von betroffenen Personen könnte gefährdet sein, wenn die Vertragspartner im Zuge dessen, z. B. Offenlegungspflichten, nicht zusammenarbeiten.	D-8-5		**Vertragliche Bestimmungen** ✓ Die beauftragte Datenverarbeitungsvereinbarung (Artikel 28 DSGVO) mit den Subunternehmern enthält Bestimmungen, nach denen die Vertragsparteien zur Zusammenarbeit verpflichtet sind.	
Datenschutzmanagementsystem (DMS) Erstellung eines DMS zur Überwachung des EFGS-Betriebs gemäß Datenschutz.	D-8-6		**Datenschutz während des Betriebs des EFGS** ✓ Für die Ausführung der App wird ein Datenschutzmanagementsystem eingerichtet.	
Zugang oder Beschlagnahme durch staatliche Behörden	D-8-7		**Stark pseudonymisierte Daten**	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Regierungsstellen wie Geheimdienste oder Strafverfolgungsbehörden können Zugang zu den einzelnen Komponenten der EFGS-Architektur erhalten, Datenbestände beschlagnahmen und durch Kombination der ihnen zur Verfügung stehenden Informationen persönliche Referenzen erstellen.			✓ Da Diagnoseschlüssel stark pseudonymisiert sind und keine direkte Verbindung zwischen betroffener Person und EFGS, sondern nur dem nationalen Backend besteht, können Identitäten nicht mithilfe von Daten hergestellt werden. Die verarbeiteten personenbezogenen Daten sind daher nur für eine statistische Auswertung nützlich, für Regierungsstellen wie Ermittlungsbehörden oder Geheimdienste jedoch nicht.	

9. Löschung/Speicherbegrenzung

Entsprechend dem Datenschutzziel der Datenminimierung dürfen personenbezogene Daten nur so lange verarbeitet werden, wie dies zur Erreichung des Zwecks erforderlich ist. Entwurfsentscheidungen zur Implementierung der Speicherbeschränkung sind unten dargestellt.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Designentscheidung/-bewertung	Referenz
Löschung	D-9-1	Durchführungsbeschluss	**sieh dazu auch D-6-8** oben	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Designentscheidung/-bewertung	Referenz
Löschung der Daten nach abgeschlossenem Download durch die teilnehmenden Backend-Server oder 14 Tage nach Erhalt, je nachdem, was früher eintritt.		(EU) 2020/1023, Anhang III, (3) (e)		

10. Implementierung der Trennung

Im folgenden Kapitel werden Entwurfsentscheidungen detailliert beschrieben, die dem Zweck der Trennungskontrolle dienen. Die Trennungskontrolle dient auch dem Schutzziel der Zweckbeschränkung/Nichtverkettbarkeit.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Implementierung der Trennung Mit diesen Maßnahmen soll sichergestellt werden, dass für verschiedene Zwecke gesammelte Daten separat verarbeitet werden können. Dies kann beispielsweise durch die logische oder physikalische Trennung der Daten erreicht werden.	D-10-1		✓ Bei jeder Softwareentwicklung werden die Funktionen der Test- und Produktionsumgebung getrennt.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
	D-10-2		✓ Es dürfen nur relevante Daten gesammelt, gespeichert oder verarbeitet werden, die direkt dem eigentlichen Zweck dienen oder für die Erfüllung der Aufgabe oder die Ausführung des Prozesses erforderlich sind. Dieser Zweck darf sich auch nach Übermittlung der personenbezogenen Daten in keinem der weiteren Verarbeitungsschritte ändern.	
	D-10-3		✓ Vorschriften und Maßnahmen zur Gewährleistung einer getrennten Verarbeitung (Speicherung, Änderung, Löschung und Übermittlung usw.) und/oder Speicherung von Daten und/oder Datenträgern mit unterschiedlichen vertraglichen Zwecken sind zu dokumentieren und anzuwenden.	
	D-10-4		✓ Vorschriften und Maßnahmen zur Gewährleistung einer getrennten Verarbeitung (Speicherung, Änderung, Löschung und Übermittlung usw.) und / oder Speicherung von Daten und / oder Datenträgern mit unterschiedlichen vertraglichen Zwecken sind zu dokumentieren und anzuwenden.	

11. Vertragsbeziehungen

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Designentscheidung/-bewertung	Referenz
Gesamtkoordination Die zugrunde liegenden Richtlinien, Anforderungen und Kontrollen müssen von den zuständigen nationalen Gesundheitsbehörden koordiniert aufeinander abgestimmt und umgesetzt werden	D-11-1	eHealth Network, Common EU Toolbox for Member States, Annex I, GA01	**Unterstützung der Applikation** ✓ Die Gesundheitsbehörden sind für die App verantwortlich und verwenden die Toolbox zu ihrer Bewertung/Unterstützung. ✓ In Bezug auf die Bewertung der Qualität und Zuverlässigkeit der Apps haben die Mitgliedstaaten die Prinzipien der laufenden CEN TC251-Konsultationen einzuhalten, die einen gemeinsamen integrierten Rahmen für alle EU-Mitgliedstaaten bieten	eHealth Network, Common EU Toolbox for Member States, Annex I, GA04
	D-11-2		**Zusammenarbeit innerhalb der EU** ✓ Die Mitgliedstaaten, die von der Kommission unterstützt werden, sollten zusammenarbeiten, um die Kriterien zu definieren, die eine grenzüberschreitende Interoperabilität ermöglichen würden; diese Kriterien werden in der Toolbox aufgeführt, die in einem iterativen Prozess aktualisiert werden kann.	eHealth Network, Common EU Toolbox for Member States, Annex I, GA04

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Designentscheidung/-bewertung	Referenz
			✓ Grenzüberschreitende Zusammenarbeit zum Austausch von Informationen über infizierte Patienten und ihre Kontakte zur Ergänzung der Maßnahmen, die im Rahmens des Beschlusses Nr. 1082/2013 des Europäischen Parlaments und des Rates ergriffen wurden.	
Verantwortlichkeit: Hinsichtlich dieses gesonderten Verarbeitungsvorgangs können die Parteien jeweils einzeln oder gemeinsam für die Verarbeitung Verantwortliche sein; sie können auch Auftragsverarbeiter einschalten.	D-11-3	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 14	**Die Mitgliedstaaten sind gemeinsam für die Verarbeitung Verantwortliche, Artikel 26 DSGVO** ✓ Die teilnehmenden Mitgliedstaaten sind gemeinsam für die Verarbeitung Verantwortliche. Gemäß Artikel 26 der Datenschutz-Grundverordnung sind die gemeinsam für die Verarbeitung personenbezogener Daten Verantwortlichen dazu verpflichtet, in einer Vereinbarung in transparenter Form festzulegen, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt.	Durchführungsbeschluss (EU) 2020/1023 der Kommission, Ziffer 10, Artikel 7a Absatz 4

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Designentscheidung/-bewertung	Referenz
	D-11-4	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 14	**Anschließende Verarbeitungsvorgänge** ✓ Jede **nach dem Austausch der Kennungen** erfolgende Verarbeitung (Expositionsberechnung, Versenden von Warnmeldungen an festgestellte Kontaktpersonen usw.) fände **unter der gesonderten Verantwortung des App-Anbieters statt, der die Daten empfängt**.	
	D-11-5	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 15	**Verantwortlichkeit/Transparenz** ✓ Die jeweiligen Rollen, Beziehungen und Verantwortlichkeiten **der gemeinsam für die Verarbeitung Verantwortlichen** gegenüber der betroffenen Person sind festzulegen, und diese **Informationen** sollten dann **der betroffenen Personen mitgeteilt werden**.	
	D-11-6	EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 15	**Mit der Verarbeitung betraute Auftragsverarbeiter** ✓ Mit der Verarbeitung zum **Zwecke der Sicherstellung der Interoperabilität** kann ein Auftragsverarbeiter betraut werden, der die in **Artikel 28 DSGVO** genannten Voraussetzungen erfüllt.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Designentscheidung/-bewertung	Referenz
	D-11-7	Durchführungsbeschluss (EU) 2020/1023 der Kommission, Ziffer 11, Artikel 7a Absatz 5	**Die Kommission als Auftragsverarbeiter, Artikel 28 DSGVO** ✓ Die Kommission, die technische und organisatorische Lösungen für das Federation Gateway bereitstellt, verarbeitet im Namen der am Federation Gateway als gemeinsam Verantwortliche teilnehmenden Mitgliedstaaten pseudonymisierte personenbezogene Daten und ist daher Auftragsverarbeiter. Gemäß Artikel 28 der Datenschutz-Grundverordnung und Artikel 29 der Verordnung (EU) 2018/1725 erfolgt die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines Rechtsinstruments nach dem Recht der Union oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und die Verarbeitung regelt. Dieser Beschluss enthält Vorschriften für die Verarbeitung durch die Kommission als Auftragsverarbeiter.	

II. Bedrohungen durch Hacker, Trolle, Stalker und Einzelpersonen

Nachfolgend wird auszugsweise erläutert, welche Sicherheitsbedrohungen bei der Entwicklung des EFGS erkannt wurden und mit welchen Designentscheidungen den Sicherheitsrisiken begegnet wurde. Schutzziele der IT-Sicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Durch die Vertraulichkeit wird sichergestellt, dass nur autorisierte Personen Zugriff auf die Daten haben. Durch die Authentizität und Integrität wird garantiert, dass der Empfänger sicher sein kann, dass die Informationen tatsächlich von dem Sender stammen, von dem er glaubt, sie erhalten zu haben (Authentizität, z. B. gesendete E-Mail oder gespeicherte Datei), und dass die Daten nicht zwischenzeitlich durch einen Dritten verändert wurden (Integrität). Durch die Verfügbarkeit wird sichergestellt, dass jederzeit auf die Daten zugegriffen werden kann.

Dieses Kapitel ist nach der STRIDE-Methode zur Bedrohungsmodellierung („Threat Modelling“) aufgebaut. Die Bedrohungsmodellierung ist eine Methode, mit der potenzielle Bedrohungen, wie z. B. strukturelle Schwachstellen oder das Fehlen geeigneter Schutzmaßnahmen, erkannt und beschrieben und mit der Priorität für Abhilfemaßnahmen festgelegt werden können. Durch eine Bedrohungsmodellierung können beispielsweise die folgenden Fragen beantwortet werden: „Wo bin ich am anfälligsten für Angriffe? Was sind die wichtigsten Bedrohungen? Was muss ich tun, um mich gegen diese Bedrohungen zu schützen?“

Eine Methode zur Bedrohungsmodellierung ist der sogenannte STRIDE-Ansatz. Nach diesem Ansatz werden die Bedrohungen in sechs verschiedene Kategorien eingeordnet. Dabei steht jeder Buchstabe des Ansatzes für eine Bedrohung:

S – Spoofing (Angreifer verschleiert seine Identität; Schutzziel: Authentizität)

T – Tampering (Manipulation, Angreifer verändert Daten; Schutzziel: Integrität)

R – Repudiation (Nichtanerkennung, Angreifer bestreitet Identität; Schutzziel: Nichtabstreitbarkeit)

I – Information Disclosure (Veröffentlichung von Informationen, Angreifer verursacht Datenleck; Schutzziel: Vertraulichkeit)

D – Denial of Service (Angreifer überlastet das System mutwillig; Schutzziel: Verfügbarkeit)

E – Elevation of Privilege (Rechteerweiterungen, Angreifer erweitert seine Rechte; Schutzziel: Authentizität)

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Sicherheitstests und unabhängige Überprüfung	T-II-1	eHealth Network, Common EU Toolbox for Member States, Anhang I, CS-02	**Steuerung von Sicherheitsrisiken** ⚠ 1. Die nationalen Behörden sollten sicherstellen, dass die Sicherheit der App und des Backends vor der Bereitstellung und nach jeder Änderung von unabhängigen Sachverständigen überprüft und getestet wird. ⚠ 2. Um das Vertrauen der Bevölkerung in die Sicherheit der App zu gewinnen und um die Transparenz zu fördern, sollten die nationalen Behörden sicherstellen, dass die Architektur und der Code der App (die App und das Backend) unabhängigen technischen Experten zur Überprüfung bereitgestellt werden. Die Veröffentlichung des Quellcodes zur unabhängigen Überprüfung ist ebenso wichtig wie die Bereitstellung einer bekannten Anlaufstelle, damit potenzielle Sicherheitsrisiken aufgezeigt werden können. ⚠ 3. Es ist wichtig, dass Sicherheitsforscher, Experten, Bürger und Organisationen dem/den Projektteam(s) Fehler und/oder Schwachstellen melden können. ⚠ 4. Die Entwickler sollten über Verfahren zur Behandlung von Schwachstellen verfügen und geeignete Richtlinien für die Offenlegung von Sicherheitslücken vorgeben.	Security standards applying to all European Commission information systems

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			⚠ Um das Vertrauen in die Apps zu stärken, können die nationalen Behörden auch weitere Maßnahmen, wie z. B. ein Bug-Bounty-Programm, in Betracht ziehen.	
Nationale Risikobewertung, Informationsaustausch, Reaktion auf Sicherheitsvorfälle	T-II-2	eHealth Network, Common EU Toolbox for Member States, Anhang I, CS-01 EDSA Interoperabilität von Kontaktnachverfolgungs-Apps, Ziffer 18	**Nationale Risikobewertung** ⚠ Die nationalen Behörden sollten eine Gesamtrisikobewertung vornehmen, in der die potenziellen Cybersicherheitsrisiken von Corona-Apps untersucht und bekannte Sicherheitslücken in den zugrunde liegenden Plattformen und Kommunikationsprotokollen sowie die jüngsten Sicherheitsvorfälle und -bedrohungen berücksichtigt werden. Die relevanten Ergebnisse dieser nationalen Risikobewertung sollten dem/den mit der Entwicklung der App betrauten Projektteam(s) zur Verfügung gestellt werden. ⚠ Im Hinblick auf die Cybersicherheit und das Schwachstellenmanagement sollte ein Informationsaustausch und eine Zusammenarbeit zwischen dem/den Projektteam(s) und den zuständigen nationalen Behörden und Stellen, einschließlich der nationalen CSIRT, den	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			Cybersicherheitsbehörden, der zuständigen CSIRTs für medizinische Produkte usw. etabliert werden. Regelmäßige Briefings zu Sicherheitsbedrohungen sind ein wichtiges Instrument, um das/die Projektteams(s) auf allen Ebenen für die Cybersicherheitsbedrohungen zu sensibilisieren. Es ist wichtig, Pläne für das Management von Störfällen und Schwachstellen zu haben; dazu zählen angemessene Verfahren für die Benachrichtigung und Einbeziehung der nationalen CSIRTs und der für Cybersicherheit und Datenschutz zuständigen Behörden. ⚠ **Informationssicherheit:** Die Interoperabilität sollte **keine Beeinträchtigung** der **Datensicherheit** und des Schutzes personenbezogener Daten bewirken. ⚠ **Informationssicherheit:** Anbieter von Anwendungen zur Kontaktnachverfolgung sollten **jede Erhöhung der Risiken in Bezug auf die Informationssicherheit**, die sich durch die zusätzliche Verarbeitung und die Mitwirkung zusätzlicher Akteure ergibt, berücksichtigen. Dies betrifft vor allem die Sicherheit der Daten im Transit wegen der möglichen **Kopplung von Backend-Servern**.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
	T-II-3	Durchführungsbeschluss (EU) 2020/1023, Anhang II, Abschnitt 1, Unterabschnitt 1 (3)	**Anlaufstelle mit einem Funktionspostfach** ⚠ Jeder Verantwortliche richtet eine Anlaufstelle mit einem Funktionspostfach ein, das der Kommunikation zwischen den gemeinsam Verantwortlichen und zwischen den gemeinsam Verantwortlichen und dem Auftragsverarbeiter dient.	
Management von Sicherheitsvorfällen, einschließlich Verletzungen des Schutzes personenbezogener Daten Die gemeinsam Verantwortlichen unterstützen sich gegenseitig bei der Ermittlung und Behandlung von Sicherheitsvorfällen, einschließlich Verletzungen des Schutzes personenbezogener Daten, im Zusammenhang mit der Verarbeitung im Federation Gateway.	T-II-4	Durchführungsbeschluss (EU) 2020/1023, Anhang II, Abschnitt 2	**Gemeinsam Verantwortliche unterstützen sich gegenseitig** ⚠ Insbesondere teilen die gemeinsam Verantwortlichen einander Folgendes mit: • Potenzielle oder tatsächliche Risiken für die Verfügbarkeit, Vertraulichkeit und/oder Integrität der personenbezogenen Daten, die im Federation Gateway verarbeitet werden; • Sicherheitsvorfälle, die mit der Verarbeitung im Federation Gateway in Verbindung stehen; • Jede Verletzung des Schutzes personenbezogener Daten, die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und die Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen sowie alle Maßnahmen, die ergriffen wurden, um gegen die Verletzung des	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			Schutzes personenbezogener Daten vorzugehen und das Risiko für die Rechte und Freiheiten natürlicher Personen zu mindern; • Jeden Verstoß gegen die technischen und/oder organisatorischen Vorkehrungen für die Verarbeitungsvorgänge im Federation Gateway. ⚠ Die gemeinsam Verantwortlichen unterrichten die Kommission, die zuständigen Aufsichtsbehörden und, falls erforderlich, die betroffenen Personen im Einklang mit den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder nach Mitteilung der Kommission über jegliche Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung im Federation Gateway.	
Sicherheitsmaßnahmen Die Kommission trifft alle organisatorischen, physischen und logischen Sicherheitsmaßnahmen auf Grundlage des aktuellen Stands der Technik, um das Federation Gateway aufrechtzuerhalten.	T-II-5	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (4)	**Sicherheitsmaßnahmen der Kommission** ⚠ Die Kommission benennt eine für das Sicherheitsmanagement beim Federation Gateway zuständige Stelle, teilt den Verantwortlichen deren Kontaktdaten mit und gewährleistet deren Verfügbarkeit zur Reaktion auf Sicherheitsbedrohungen.	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (4)

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			⚠ Ihre Verantwortung für die Sicherheit des Federation Gateway wird vermutet, ⚠ Stellt sicher, dass alle Personen, denen der Zugriff auf das Federation Gateway gewährt wird, vertraglichen, beruflichen oder gesetzlichen Vertraulichkeitsverpflichtungen unterliegen.	
Sicherheitsmaßnahmen für nationale Backend-Server Die Kommission muss alle erforderlichen Sicherheitsmaßnahmen treffen, damit das reibungslose Funktionieren der nationalen Backend-Server nicht beeinträchtigt wird. Zu diesem Zweck richtet die Kommission besondere Verfahren für den Anschluss der Backend-Server an das Federation Gateway ein.	T-II-6	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (5)	**Sicherheitsmaßnahmen für nationale Backend-Server** ⚠ Die Kommission legt ein Verfahren zur Risikobewertung fest, um potenzielle Bedrohungen des Systems zu ermitteln und abzuschätzen ⚠ Audit- und Überprüfungsverfahren sollen aufgebaut werden: • Zur Überprüfung der Übereinstimmung der umgesetzten Sicherheitsmaßnahmen mit den geltenden Sicherheitsvorgaben; • Zur regelmäßigen Kontrolle der Integrität der Systemdateien, der Sicherheitsparameter und der erteilten Genehmigungen;	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (5) (a), (b)

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			• Zur Überwachung zwecks Feststellung von Sicherheitsverstößen und von unbefugtem Eindringen; • Zur Umsetzung von Änderungen zur Behebung bestehender Sicherheitslücken; • Zur Ermöglichung — auch auf Anfrage der Verantwortlichen — und zur Mitwirkung an der Durchführung unabhängiger Audits, einschließlich Inspektionen, sowie von Überprüfungen von Sicherheitsmaßnahmen im Einklang mit den Bedingungen des Protokolls (Nr. 7) zum AEUV über die Vorrechte und Befreiungen der Europäischen Union[24]; ⚠ Die Kommission richtet ein Änderungskontrollverfahren ein, um die Auswirkungen einer Änderung vor ihrer Umsetzung zu dokumentieren und abzuschätzen und die Verantwortlichen über alle Änderungen auf dem Laufenden zu halten, die sich auf die Kommunikation mit ihren Infrastrukturen und/oder deren Sicherheit auswirken können; ⚠ Die Kommission legt ein Wartungs- und Reparaturverfahren mit Regeln und Bedingungen für	

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1023&from=EN#ntr2-LI2020227EN.01000801-E0001.

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			die Wartung und/oder Reparatur von Einrichtungen fest; ⚠ Die Kommission richtet ein Verfahren ein in Bezug auf Sicherheitsvorfälle zur Festlegung des Melde- und Eskalationsprogramms, zur unverzüglichen Unterrichtung der Verantwortlichen sowie des Europäischen Datenschutzbeauftragten über jegliche Verletzung des Schutzes personenbezogener Daten sowie zur Festlegung eines Disziplinarverfahrens, um gegen Sicherheitsverletzungen vorzugehen.	
TOMs für die Flächen, auf denen die Einrichtungen für das Federation Gateway untergebracht sind Die Kommission muss physische und/oder logische Sicherheitsmaßnahmen auf Grundlage des aktuellen Stands der Technik für die Flächen ergreifen, in denen die Einrichtungen für das Federation Gateway untergebracht sind, und für die Kontrollen der logischen Daten und der Zugriffssicherheit.	T-II-7	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (6)	**Zur Umsetzung der Sicherheitsmaßnahmen wird die Kommission:** ✓ die physische Sicherheit durchsetzen, um abgegrenzte Sicherheitsbereiche einzurichten und das Erkennen von Verstößen zu ermöglichen; ✓ den Zugang zum Betriebsgelände / zu den Räumlichkeitenkontrollieren und ein Besucherregister für Rückverfolgungszwecke führen; ✓ sicherstellen, dass die externen Personen, denen Zugang zu den Räumlichkeiten gewährt wird, von	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (6) Security standards applying to all European Commission information systems

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			entsprechend bevollmächtigten Mitarbeitern begleitet werden; ✓ sicherstellen, dass Ausrüstung ohne Vorabgenehmigung durch die benannten zuständigen Stellen nicht ergänzt, ersetzt oder entfernt werden können; ✓ den beiderseitigen Zugriff auf nationale Backend-Server und das Federation Gateway kontrollieren; ✓ sicherstellen, dass Personen, die Zugriff auf das Federation Gateway haben, identifiziert und authentifiziert werden; ✓ die Rechte für den Zugriff auf das Federation Gateway überprüfen, falls eine Sicherheitsverletzung in Bezug auf diese Infrastruktur eintritt; ✓ die Integrität der über das Federation Gateway übermittelten Informationen wahren; ✓ technische und organisatorische Sicherheitsmaßnahmen umsetzen, um unbefugten Zugriff auf personenbezogene Daten zu verhindern;	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
			✓ bei Bedarf Maßnahmen zur Verhinderung des unbefugten Zugriffs auf das Federation Gateway von der Netzdomäne der nationalen Behörden aus ergreifen (d. h. Sperrung eines Standorts/einer IP-Adresse);	
Überwachung des Betriebs Die Kommission muss im Falle einer erheblichen Abweichung von den Qualitäts- oder Sicherheitsgrundsätzen und -konzepten alle Betriebsprozesse überwachen;	T-II-8	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (7) – (9)	**Die Kommission überwacht den Betrieb folgendermaßen:** ✓ Die Kommission ergreift Maßnahmen zum Schutz ihrer Netzdomäne, einschließlich der Trennung von Anschlüssen, im Falle einer erheblichen Abweichung von den Qualitäts- oder Sicherheitsgrundsätzen und -konzepten; ✓ führt einen Risikomanagement-Plan in Bezug auf ihren Zuständigkeitsbereich; ✓ überwacht – in Echtzeit – die Leistung aller Dienstkomponenten ihres Federation Gateways, erstellt regelmäßige Statistiken und führt Aufzeichnungen.	Security standards applying to all European Commission information systems, Logging and Monitoring security standard.pdf
Zugriffskontrolle	T-II-9	Durchführungsbeschluss	**Die Kommission stellt die Zugriffskontrolle folgendermaßen sicher:**	Security standards applying to all

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Die Kommission muss die Zugriffskontrolle sicherstellen.		(EU) 2020/1023, Anhang III, (13) – (14)	✓ Die Kommission stellt sicher, dass die im Federation Gateway verarbeiteten Daten für Personen, die nicht zugriffsbefugt sind, unverständlich sind; ✓ Die Kommission ergreift alle erforderlichen Maßnahmen, damit die Betreiber des Federation Gateways keinen unbefugten Zugriff auf übermittelte Daten haben;	European Commission information systems, Access Control & Authentication security standard.pdf

1. Spoofing (Identitätsverschleierung)

Beschreibung	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Quelle
Authentifizierung EFGS/nationale Backend-Server	T-1-1	EDSA-Leitlinien 04/2020 Tools zur	**Signatur der Daten** Zur Authentifizierung des Kommunikationspartners nutzen das EFGS und die nationalen Backend-Server spezielle	Github – Software Design European Federation Gateway

Beschreibung	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Quelle
Ein Angreifer könnte versuchen, sich als nationaler Backend-Server auszugeben und Daten an das EFGS zu übertragen. Ebenfalls wäre es möglich, dass der Angreifer sich als EFGS ausgibt und versucht, Daten an die nationalen Backend-Server zu übertragen.		Kontaktnachverfolgung, Anhang SEC-6, SEC-7, SEC-9	Mechanismen, mit denen die Herkunft der Daten überprüft werden kann. Das EFGS signiert die Daten mit einem privaten Schlüssel und die nationalen Backend-Server validieren die Signatur anhand des öffentlichen Schlüssels. Umgekehrt gilt dasselbe.	Service – Batch Signature
Vortäuschen der Identität des Backend-Servers Ein Angreifer könnte versuchen, die nationalen Backend-Server anhand von DNS-Spoofing oder Man-in-the-Middle-Angriffen davon zu überzeugen, statt mit dem echten EFGS mit einem von dem Angreifer bestimmten Server zu kommunizieren. Ein solcher Angriff könnte auch von einem böswillig eingesetzten Backend-Server gegen das EFGS ausgehen. Außerdem könnte der Angreifer versuchen, ungültige oder gefälschte Daten an das EFGS zu senden. Ziel eines solchen Angriffs ist es, die EFGS-Datenbank zu manipulieren oder	T-1-2	EDSA-Leitlinien 04/2020 Tools zur Kontaktnachverfolgung, Anhang SEC-6, SEC-7, SEC-9	**HTTP Public Key Pinning** Damit solche Angriffe vermieden werden, arbeitet das System mit einer strengen TLS-Verifizierung sowie mit Pinning-Mechanismen zur Validierung der eingehenden Daten. **Authentifizierung des nationalen Backend-Servers/EFGS** Zur Authentifizierung des Kommunikationspartners (EFGS/nationaler Backend-Server) nutzt das System eine digitale Signatur. Damit wird die Identität des jeweils anderen Kommunikationspartners verifiziert.	eHealth Network European Proximity Tracing, Interoperability Architecture, V. 1.3, Anhang (A), Authentication

Beschreibung	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Quelle
das System durch einen Denial-of-Service-Angriff zu einer Abschaltung zu zwingen.				
Netzwerk-Sniffing Ein Angreifer könnte den Datenverkehr zwischen den nationalen Backend-Servern und dem EFGS abhören und dabei Daten sammeln, speichern oder auswerten.	T-1-3	EDSA-Leitlinien 04/2020 Tools zur Kontaktnachverfolgung, Anhang SEC-4	**Schutzmaßnahmen gegen Network-Sniffing** Um einen solchen Angriff zu vermeiden, wird die Kommunikation zwischen dem EFGS und den nationalen Backend-Servern anhand hochmoderner kryptographischer Techniken, d. h. TLS (1.3), verschlüsselt. Dank dieser Techniken ist ein sicherer Datenaustausch zwischen den nationalen Backend-Servern und dem EFGS möglich.	eHealth Network European Proximity Tracing, Interoperability Architecture, V. 1.3, Abschnitt 3.1.3
Spamming von Diagnoseschlüsseln Dieses Risiko kann insbesondere durch Länder verursacht werden, die nur über schwache Mechanismen zur Überprüfung	T-1-4	EDSA-Leitlinien 04/2020 Tools zur Kontaktnachv	**Schlüssel-Filterung** Bei dieser Art von Angriff werden falsche Warnungen vor einem positiven Testergebnis ausgegeben, die eine hohe Zahl von Kontaktwarnungen zur Folge haben können.	

Beschreibung	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Quelle
des Status von Nutzern verfügen, die in der App ein positives COVID-19-Testergebnis melden, z. B. durch Bereitstellung eines Einmalcodes, der von einer Teststation oder einer Fachkraft im Gesundheitswesen stammt. Wenn nicht auf sicherem Wege eine Bestätigung eingeholt werden kann, dürfen die Daten nicht verarbeitet werden.		erfolgung, Anhang SEC-1	Damit derartige Angriffe vermieden werden, unterscheidet das EFGS anhand von Metadaten zwischen verschiedenen Arten von Validierungsmechanismen. Anhand dieser Metadaten können die nationalen Backend-Server die von ihnen empfangenen Diagnoseschlüssel filtern.	

2. Manipulation (Veränderung von Daten)

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Einspeisung falsch-positiver Testergebnisse Ein oder mehrere Angreifer könnten ihre Schlüssel für ein positives Testergebnis auf den Server hochladen und behaupten, infiziert zu sein. Dadurch könnte das System gestört werden.	T-2-1	eHealth Network, Common EU Toolbox for Member States, Anhang I, EF-05	**Wahrung der Integrität der verarbeiteten Daten** ✓ Die Kommission trifft die zur Wahrung der Integrität der verarbeiteten Daten erforderlichen Maßnahmen.	Durchführungsbeschluss (EU) 2020/1023, Anhang III, (3)

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Nur autorisierte Gesundheitsbehörden oder andere autorisierte Stellen, wie z. B. Labore, sollten dazu berechtigt sein, Infektionen zu bestätigen und Warnungen auszulösen, z. B. durch die Bereitstellung eines (QR-)Codes/die Versendung einer Benachrichtigung, damit der Nutzer eine Warnung auslösen kann; alternativ sollten die autorisierten Gesundheitsbehörden oder andere autorisierte Stellen, wie z. B. Labore, selbst dazu befugt sein, eine Warnung auszulösen.			⚠ Diese Anforderung sollte für alle Mitgliedstaaten gelten.	
Von einer Gesundheitsbehörde zur Bestätigung von COVID-19-Fällen erstellter QR-Code Der von der zuständigen nationalen Gesundheitsbehörde erstellte Code sollte pseudozufällig generiert werden und zur einmaligen Nutzung vorgesehen sein. So wird sichergestellt, dass der Code nicht von böswilligen Personen zur Kontamination der auf dem Server gesammelten Daten genutzt werden kann. Der Code sollte möglichst benutzerfreundlich sein (z. B. ein QR-Code),	T-2-2	eHealth Network, Common EU Toolbox for Member States, Anhang I, TF-04	**Verifizierung des Testergebnisses** ⚠ Der Code sollte pseudozufällig generiert werden und zur einmaligen Nutzung vorgesehen sein. ✖ Alle teilnehmenden Mitgliedstaaten sollten das Testergebnis durch eine Regierungsstelle überprüfen lassen, siehe D-6-5 oben. ✓ Der CWA Server verteilt nur Positivschlüssel an die CWA Apps, denen eine Attestierung durch ein Labor oder eine Testeinrichtung zugrunde liegt (CWA-Designentscheidungen D-6-2c).	EFGS-DSFA-Bericht, Abschnitt 14.2.3.1, Verarbeitung inakkurater personenbezogener Daten CWA-Designentscheidungen D-6-2c

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
damit das Risiko einer fehlerhaften Eingabe durch den Nutzer reduziert wird.				
Böswillige Nutzung eines nationalen Backend-Servers Ein Angreifer, der sich Zugang zu einem der nationalen Backend-Server verschafft hat, könnte Diagnoseschlüssel in die EFGS-Datenbank einspeisen. Das EFGS kann in diesem Fall nicht erkennen, ob der nationale Backend-Server in böswilliger Absicht genutzt wird.	T-2-3		**Sicherheitsstandard/Filterung** Das EFGS kann nicht feststellen, ob ein nationaler Backend-Server von einem Angreifer übernommen wurde. Die nationalen Backends müssen sicherstellen, dass sie die erforderlichen Sicherheitsstandards einhalten. Andere nationale Backends können jedoch beschließen, alle Diagnoseschlüssel, die von einem potenziell in böswilliger Absicht genutzten nationalen Backend-Server übertragen werden, zu ignorieren, indem sie die Daten in den nationalen Backends filtern.	
EFGS-Datenbankadministrator Eine böswillige Absicht der EFGS-Datenbankadministratoren vorausgesetzt, könnten sie die EFGS-Datenbank modifizieren oder beschädigen, da sie uneingeschränkten Zugriff auf die Datenbank haben. Sie können die Metadaten der Datenbank verändern, da	T-2-4		**Autorisierte Mitarbeiter** Damit solche Insider-Angriffe verhindert werden können, muss darauf geachtet werden, dass der Zugriff ausschließlich autorisierten und vertrauenswürdigen Mitarbeitern gewährt wird. ✓ Das EFGS wird von der GD DIGIT (Generaldirektion Informatik (innerhalb der Europäischen Kommission))	DSK, Abschnitt 5.9.1, Rollen für App-Betreiber

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
die Metadaten zum jetzigen Zeitpunkt von keiner Behörde signiert wurden.			gehostet. Nur der Administrator der GD DIGIT hat Zugriff auf personenbezogene Daten. ✓ Der EFGS-Server wird von separaten Teams betreut, um Neuidentifizierungs-Angriffe auf Administratoren zu erschweren.	
Schutz vor dem Import böswilliger Datenpakete Bei dieser Art von Angriff werden Daten von einem beliebigen Ort auf der Welt an das EFGS gesendet, mit dem Ziel, Daten zu verändern oder Zugang zu dem System zu erhalten.	T-2-5	EDSA-Leitlinien 04/2020 Tools zur Kontaktnachverfolgung, Anhang SEC-3, SEC-6	**Digitale Signatur** ✓ Um das EFGS von dem Verteilen nichtautorisierter Daten zu schützen, werden die von den jeweiligen nationalen Backend-Servern übertragenen Daten vor der Übertragung mit einem Herkunftsvermerk signiert. Unberechtigte Imports in die Datenbank von anderen naionalen Backends können so erkannt werden. Der EFGS Server überprüft ebenfalls anhand der Zertifikate die Gültigkeit der Daten innerhalb des Pakets.	Github – Software Design European Federation Gateway Service – Batch Signature

3. Nichtanerkennung

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Missbräuchliche Nutzung von Systemressourcen Ein Hacker könnte die zur Verfügung stehenden Systemressourcen (d. h. die Rechenleistung) für missbräuchliche Aktivitäten (z. B. für das Schürfen von Kryptowährungen) nutzen. Um seine Entdeckung zu erschweren, wird der Hacker versuchen, alle seine Änderungen und Aktivitäten zu verbergen, indem er sämtliche Logs, Spuren usw. entfernt.	T-3-1	EDSA-Leitlinien 04/2020 Tools zur Kontaktnachverfolgung, Anhang SEC-11	**Die Kommission überwacht den Betrieb folgendermaßen:** ✓ Die Kommission ergreift Maßnahmen zum Schutz ihrer Netzdomäne, einschließlich der Trennung von Anschlüssen, im Falle einer erheblichen Abweichung von den Qualitäts- oder Sicherheitsgrundsätzen und -konzepten; ✓ führt einen Risikomanagement-Plan in Bezug auf ihren Zuständigkeitsbereich; ✓ überwacht – in Echtzeit – die Leistung aller Dienstkomponenten ihres Federation Gateways, erstellt regelmäßige Statistiken und führt Aufzeichnungen. ✓ Alle sicherheitsrelevanten Änderungen und Anpassungen müssen in einem speziellen (auditsicheren) und geschützten Sicherheitsaudit-Protokoll gespeichert werden.	Security standards applying to all European Commission information systems, Logging and Monitoring security standard.pdf
Implementierung von Hintertüren Ein Hacker mit Zugang zu dem System (z. B. ein Bediener) könnte die	T-3-2	EDSA-Leitlinien 04/2020 Tools zur	Wie oben	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Sicherheitskonfigurationen so ändern, dass Hintertüren geöffnet werden. Um seine Entdeckung zu erschweren, wird der Hacker versuchen, alle seine Änderungen und Aktivitäten zu verbergen, indem er sämtliche Logs, Spuren usw. entfernt.		Kontaktnachverfolgung, Anhang SEC-11		

4. Veröffentlichung von Informationen (Datenleck)

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Zugriff auf die EFGS-Datenbank Im Falle eines Sicherheitsproblems könnte ein Angreifer Zugriff auf die Datenbank erlangen und die darin gespeicherten Daten lesen.	T-4-1		**Sicherheitsstandards** ✓ Damit ein nichtautorisierter Zugriff auf die Datenbank vermieden wird, arbeitet der EFGS-Server mit verschiedenen Sicherheitsmechanismen.	Security standards applying to all European Commission information systems

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Kommunikation zwischen dem nationalen Backend-Server und dem EFGS Ein Angreifer kann die Kommunikation zwischen dem EFGS und dem nationalen Backend-Server abhören. Ziel dieses Angriffs ist es, Zugriff auf Informationen aus dem System zu erlangen.	T-4-2	EDSA-Leitlinien 04/2020 Tools zur Kontaktnachverfolgung, Anhang SEC-3, SEC-9	**Sichere Kommunikation** ✓ Die Kommunikation zwischen dem EFGS und den nationalen Backend-Servern wird anhand hochmoderner kryptographischer Techniken (TLS 1.3) verschlüsselt. Dank dieser Techniken ist ein sicherer Datenaustausch zwischen den nationalen Backend-Servern und dem EFGS möglich.	eHealth Network European Proximity Tracing, Interoperability Architecture, V. 1.3, Abschnitt 3.1.3
Falsche Datenübertragung durch die nationalen Backend-Server Die nationalen Backend-Server könnten Daten an einen Server übertragen, bei dem es sich nicht um das EFGS handelt.	T-4-3	EDSA-Leitlinien 04/2020 Tools zur Kontaktnachverfolgung, Anhang SEC-9	**Sichere Kommunikation** ✓ Bei der Kommunikation zwischen den Backend-Servern und dem EFGS werden die übertragenen Daten durch Kryptoverfahren verschlüsselt.	eHealth Network European Proximity Tracing, Interoperability Architecture, V. 1.3, Abschnitt 8.2
Falsche Datenübertragung durch das EFGS Das EFGS könnte Daten statt an den vorgesehenen nationalen Backend-Server an einen falschen Zielort übertragen.	T-4-4	EDSA-Leitlinien 04/2020 Tools zur Kontaktnachverfolgung, Anhang SEC-2, SEC-4	**Sichere Kommunikation** ✓ Das EFGS überträgt die Daten nicht aktiv, sondern stellt sie lediglich zum Download zur Verfügung.	

5. Denial of Service (mutwillige Überlastung)

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Verfügbarkeit	T-5-1		Das von den einzelnen Backend-Servern hochgeladene Datenvolumen ist mit schätzungsweise max. 20-30 MB pro Tag vergleichsweise gering. Außerdem ist die Anzahl der Teilnehmer begrenzt, da jedes Land nur einen Backend-Server betreibt. Darüber hinaus genügt ein kleiner Webdienst, der im Sinne einer Hochverfügbarkeit mit einfachem Load Balancer und repliziertem Datenspeicher ausgestattet ist, um den Bedarf selbst in den kritischsten Pandemie-Szenarien zu decken.	eHealth Network Guidelines, Intop Specs, Abschnitt, S. 12
Missbräuchliche Nutzung der von den nationalen Corona-Warn-App-Servern genutzten EFGS-APIs, um eine große Zahl gefälschter Schlüssel hochzuladen Ein Angreifer könnte die implementierten EFGS-APIs, über die Daten hochgeladen werden können, missbrauchen, um eine große Zahl von gefälschten Schlüsseln an den	T-5-2	EDSA-Leitlinien 04/2020 Tools zur Kontaktnachverfolgung, Anhang SEC-7	✓ Die Upload-APIs müssen vor diesem Angriffsmuster geschützt werden und zwar durch die Implementierung einer geeigneten Überwachung der relevanten Systemparameter (Ressourcenverbrauch der App, Netzwerk usw.), die eine dynamische Netzwerk- und/oder API-Drosselung ermöglicht. Zusätzlich sollte ein Betrugserkennungssystem implementiert werden, mit dem Missbrauchsversuche identifiziert werden können.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
EFGS-Server zu übertragen. Dies könnte eine hohe Auslastung des EFGS-Servers und damit eine Verringerung der verfügbaren Netzwerkkapazität zur Folge haben. Durch beide Aspekte könnte die Verfügbarkeit des EFGS-Backend-Servers gefährdet werden. Die Daten des EFGS werden automatisch mit den nationalen Corona-Warn-App-Servern ausgetauscht. Daher kann der Angreifer möglicherweise auch die Verfügbarkeit der nationalen Corona-Warn-App-Server gefährden. Da diese Schlüssel mit den mobilen Corona-Warn-Apps ausgetauscht werden, kann dies die Verfügbarkeit und Leistung der Mobilgeräte beeinträchtigen, auf denen die Nutzer die Corona-Warn-App installiert haben.				
Missbräuchliche Nutzung der von den nationalen Corona-Warn-App-Servern genutzten EFGS-APIs, um Schlüssel herunterzuladen	T-5-3		✓ Die Upload-APIs müssen vor diesem Angriffsmuster geschützt werden und zwar durch die Implementierung einer geeigneten Überwachung der relevanten Systemparameter (Ressourcenverbrauch der App, Netzwerk usw.), die eine dynamische	Security standards applying to all European Commission information

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Ein Angreifer könnte die APIs der Corona-Warn-App-Server missbrauchen, um darüber regelmäßig und mit steigender Frequenz Schlüsselpakete herunterzuladen. Ein solcher Angriff hat möglicherweise Verfügbarkeitsprobleme des EFGS-Servers sowie eine Reduzierung der verfügbaren Netzwerkkapazität des EFGS-Servers zur Folge.			Netzwerk- und/oder API-Drosselung ermöglicht. Zusätzlich sollte ein Betrugserkennungssystem implementiert werden, mit dem Missbrauchsversuche identifiziert werden können.	systems, Logging and Monitoring security standard.pdf
DDoS-API-Angriffe Ein Angreifer könnte versuchen, anhand eines Botnets einen Brute-Force-Angriff gegen die Autorisierungs- und Authentifizierungskonzepte des EFGS-Servers in die Wege zu leiten. Infolge eines solchen Angriffs könnte der EFGS-Server nicht mehr verfügbar sein oder es könnte zu einem Systemabsturz kommen.	T-5-4		✓ Die EFGS-Serverarchitektur muss mit einer Technologie ausgestattet sein, die einen ausreichenden Schutz gegen DDoS-Angriffe bietet. ✓ Die EFGS-Serverarchitektur muss skalierbar sein, damit die Verfügbarkeit auch bei (potenziell dauerhaft) hoher Auslastung sichergestellt ist. ✓ Durch eine ordnungsgemäß implementierte Netzwerk-/Systemüberwachung könnte der ordnungsgemäße Zustand der EFGS-Lösung sichergestellt werden.	

6. Erhöhung/Ausweitung von Berechtigungen

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Unbefugter Zugriff auf das EFGS-System Es besteht das Risiko, dass aufgrund fehlender oder falscher Benutzer-/Rollenberechtigungen eine nichtautorisierte Person Zugriff auf den EFGS-Server erhält.	T-6-1	EDSA-Leitlinien 04/2020 Tools zur Kontaktnachverfolgung, Anhang SEC-10	✓ Es muss ein konsistentes Autorisierungskonzept implementiert werden. Durch das Konzept muss Folgendes sichergestellt werden: • eine klare Trennung der Zuständigkeiten • die Einhaltung des Prinzips der geringsten Zugriffsrechte • eine klare Trennung der Pflichten ✓ Durch die Architektur muss ein strikter Ansatz zur System-/Mandantentrennung sichergestellt werden.	Security standards applying to all European Commission information systems
Nichtautorisierter Zugriff auf Daten, die im EFGS gespeichert sind Aufgrund von unzureichenden Zugriffskontrollen könnte ein nichtautorisierter Nutzer Zugriff auf vertrauliche Informationen erlangen oder zugriffsbeschränkte Operationen durchführen.	T-6-2		**Sicherheitsstandards** ✓ Damit ein nichtautorisierter Zugriff auf die Datenbank verhindert wird, arbeitet der EFGS-Server mit verschiedenen Sicherheitsmechanismen.	

Beschreibung der Anforderung/des Risikos	ID	Quelle der Anforderung	Design-Entscheidung/-Bewertung	Referenz
Nichtautorisierter Zugriff zwecks Änderung sicherheitsrelevanter Konfigurationen im EFGS Aufgrund eines unzureichendes Autorisierungskonzepts könnte ein Angreifer Sicherheitskonfigurationen in einer solchen Weise ändern, dass dadurch die Sicherheit des gesamten EFGS-Servers gefährdet wird.	T-6-3		**Sicherheitsstandards** ✓ Damit ein nichtautorisierter Zugriff auf die Datenbank verhindert wird, arbeitet der EFGS-Server mit verschiedenen Sicherheitsmechanismen. ✓ Im EFGS ist eine „Trust-Anchor-Liste“ implementiert, über die der Zugang zum System geregelt wird. Diese Liste muss offline mit dem privaten Schlüssel der EFGS-Betreiber signiert werden. Ohne diesen privaten Schlüssel kann ein potenzieller Angreifer die EFGS-Zugangsliste nicht verändern.	Security standards applying to all European Commission information systems
Fehlende System-/Mandantentrennung Aufgrund einer fehlenden System-/Mandantentrennung innerhalb des EFGS könnte ein Angreifer Zugriff auf bestimmte Ressourcen erlangen.	T-6-4			Security standards applying to all European Commission information systems

G. Abkürzungsverzeichnis

Begriff	Beschreibung

API	Application Programming Interface (Anwendungsprogrammierschnittstelle)
BLE	Bluetooth Low Energy
CCC	Chaos Computer Club
CDN	Content Delivery Network
DSFA	Datenschutzfolgenabschätzung
DSK	Datenschutzkonzept
ECDC	European Centre for Disease Prevention and Control (Europäisches Zentrum für die Prävention und Kontrolle von Krankheiten)
EDSA	Europäischer Datenschutzausschuss
EWR	Europäischer Wirtschaftsraum
EFGS	European Federation Gateway Service
ENF	Exposure Notification Framework
GAEN	Google/Apple Exposure Notification API
DSGVO	Datenschutzgrundverordnung
GUID	Globally Unique Identifier
RPI	Rolling-Proximity-Identifier
TAN	Transaktionsnummer
TEK	Temporary Exposure Key