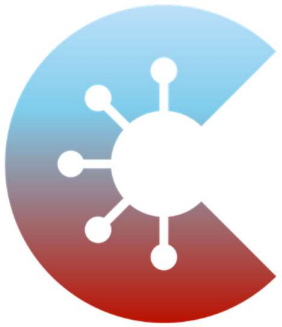

EXTERNAL

Designentscheidungen bei der Entwicklung der Corona-Warn-App der Bundesrepublik Deutschland

Version 1.2

A. Vorwort

Die Corona-Warn-App der Bundesrepublik Deutschland wurde in einer durch die Corona-Pandemie bedingten kurzen Zeit erstellt und veröffentlicht.

Mit diesem Dokument soll für die Öffentlichkeit nachvollziehbar dargestellt werden, welche Designentscheidungen getroffen wurden, um die Corona-Warn-App grundrechtsschonend auszugestalten. Die Erkenntnisse aus der ständig begleitenden Datenschutzfolgenabschätzung sind in den Entwicklungsprozess als Designentscheidungen eingeflossen.

Aufgrund der schnelllebigen neuen Erkenntnisgewinnung, wird neben der Corona-Warn-App, auch dieses Dokument eine regelmäßige Aktualisierung erfahren. Dem entsprechend handelt es sich um ein „lebendiges Dokument“, welches regelmäßig in Bearbeitung ist.

Der Datenschutz muss ganzheitlich, integrativ und kreativ in Technologien, Abläufe und Informationsarchitekturen eingebettet werden. Ganzheitlich, weil immer zusätzliche, breitere Kontexte berücksichtigt werden müssen. Integrativ, weil alle Beteiligten und Interessen konsultiert werden sollten. Kreativ, weil die Einbettung des Datenschutzes manchmal bedeutet, bestehende Entscheidungen neu zu erfinden, weil die Alternativen inakzeptabel sind. Das Ergebnis ist, dass der Datenschutz zu einem wesentlichen Bestandteil der bereitgestellten Kernfunktionalität wird. Der Datenschutz ist integraler Bestandteil des Systems, ohne die Funktionalität zu beeinträchtigen.

Zur Erreichung dieser Ziele und Vermeidung von Risiken für den Datenschutz wurden bei der Entwicklung der Corona-Warn-App und ihrer Infrastruktur die in diesem Dokument aufgeführten Designentscheidungen getroffen.

In diesem Dokument wird – ausschließlich zum Zweck der besseren Lesbarkeit – auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen in diesem Dokument sind somit geschlechtsneutral zu verstehen.

B. Inhaltsverzeichnis

C. Quellenverzeichnis

Bei den Designentscheidungen der Corona-Warn-App → (CWA) der Bundesregierung Deutschland wurden insbesondere die folgenden Veröffentlichungen von Behörden und Nichtregierungsorganisationen berücksichtigt:

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[1]

Chaos Computer Club → (CCC), *10 Prüfsteine für die Beurteilung von „Contact Tracing"-Apps* vom 6. April 2020[2]

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. → (FifF), *Datenschutz-Folgenabschätzung → (DSFA) für eine Corona-App*, Version 1.6 vom 29. April2020[3]

Digitalcourage e.V., *Einordung zur geplanten „Corona-Kontakt-Tracing-App" des →RKI*, Stand 4. Mai 2020[4]

Öffentliche Quellen für die hier gemachten Angaben sind insbesondere die folgenden Dokumentationen zu den einzelnen Komponenten der CWA App, zu finden auf den Websites von github.com zur CWA App, sowie die Dokumentationen von Apple und Google. Die Dokumentationen auf github.com, die auf Englisch vorliegen, werden regelmäßig aktualisiert und sind den deutschen Übersetzungen in Hinblick auf die Aktualität deshalb vorzuziehen:

T/SAP Dokumentation, Scoping Document[5]

T/SAP Dokumentation, CWA User Interface Screens[6]

T/SAP Dokumentation, Solution Architecture[7]

---

[1] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_de.pdf
[2] https://www.ccc.de/de/updates/2020/contact-tracing-requirements
[3] https://www.fiff.de/dsfa-corona
[4] https://digitalcourage.de/blog/2020/corona-app-einordnung-digitalcourage
[5] https://github.com/corona-warn-app/cwa-documentation/blob/master/scoping_document.md
[6] https://github.com/corona-warn-app/cwa-documentation/blob/master/ui_screens.md
[7] https://github.com/corona-warn-app/cwa-documentation/blob/master/solution_architecture.md

T/SAP Dokumentation, Sicherheit[8]

T/SAP Dokumentation, CWA Verification Server[9]

T/SAP Dokumentation, Software Design Verification Server[10]

T/SAP Dokumentation, CWA App[11]

T/SAP Dokumentation, CWA Server[12]

T/SAP Dokumentation, CWA Portal Server[13]

T/SAP Dokumentation, CWA Test Result Server[14]

T/SAP Dokumentation, Criteria for the Evaluation of Contact Tracing Apps (Prüfsteine CCC)[15]

Google/Apple, Exposure Notification - Bluetooth Specification[16]

[8] https://github.com/corona-warn-app/cwa-documentation/blob/master/overview-security.md
[9] https://github.com/corona-warn-app/cwa-verification-server
[10] https://github.com/corona-warn-app/cwa-verification-server/blob/master/docs/architecture-overview.md
[11] https://github.com/corona-warn-app/cwa-documentation
[12] https://github.com/corona-warn-app/cwa-server
[13] https://github.com/corona-warn-app/cwa-verification-portal/blob/master/README.md
[14] https://github.com/corona-warn-app/cwa-testresult-server/blob/master/README.md
[15] https://github.com/corona-warn-app/cwa-documentation/blob/master/pruefsteine.md
[16] https://blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf

D. Ziele des Dokuments

Mit diesem Dokument soll für die Öffentlichkeit nachvollziehbar dargestellt werden, welche Designentscheidungen getroffen wurden, um die Corona-Warn-App grundrechtsschonend auszugestalten.

Zur laufenden Verbesserung und Berücksichtigung der Datenschutzanforderungen wurde während des gesamten Entwicklungsverlaufs der Corona-Warn-App eine Datenschutzfolgenabschätzung (DSFA) durchgeführt. Eine Datenschutzfolgenabschätzung ist eine Risikoanalyse und -bewertung für die Verarbeitung personenbezogener Daten. Es wird abgeschätzt, welche Gefährdungen für die Rechte und Freiheiten der Benutzer der App durch die Datenverarbeitungen bestehen und wie wahrscheinlich es ist, dass diese Gefährdungen eintreten. Die Erkenntnisse aus der ständig begleitenden Datenschutzfolgenabschätzung sind in den Entwicklungsprozess als Designentscheidungen eingeflossen.

Inhaltlich wurde bei der Datenschutzfolgenabschätzung die Perspektive des von der Datenverarbeitung Betroffenen – also des Benutzers der CWA App – in den Fokus der Risikobetrachtungen genommen. Damit wurde einer Grundanforderung Rechnung getragen, die auch der „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V." (FifF) in seiner Datenschutzfolgenabschätzung [17] formuliert. Insbesondere wurden Risiken für die sogenannten immateriellen Schäden der Benutzer betrachtet, also drohende gesellschaftliche und soziale Nachteile, Diskriminierungen, Einschüchterungseffekte und die (selbstauferlegte) Einschränkung von Grundrechten. Weiterführende Informationen finden sich in dem ausführlichen Bericht zur Datenschutzfolgenabschätzung für die Corona-Warn-App.

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 ausdrücklich erwünscht, um die Prozesse weiter zu verbessern.

[17] FifF DSFA, S. 11.

E. Beschreibung der CWA App

Zur besseren Lesbarkeit des Dokumentes wird an dieser Stelle die Funktionsweise der Corona-Warn-App aus Nutzersicht dargestellt.

Durch die Corona-Pandemie kam es zu dem weltweiten Ausbruch der neuen Atemwegserkrankung COVID-19 („Corona“). Verursacht wird die Erkrankung durch eine Infektion mit dem bis 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. Zur Unterstützung der frühestmöglichen Unterbrechung der Infektionsketten wurde die Corona-Warn-App entwickelt. Hierzu sollen die Benutzer durch die CWA App über den Kontakt zu einer infizierten Person möglichst früh gewarnt und bei dem Erhalt ihres Testergebnisses unterstützt werden.

Das Erfassen der möglichen Begegnungen mit infizierten Personen erfolgt durch die sog. Annäherungsverfolgung (Tracing). Ziel der Annäherungsverfolgung ist es, Benutzer darüber zu informieren, dass sie in körperlicher Nähe zu einer infizierten Person standen, ohne 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 von denen der Benutzer deshalb nicht erfahren kann, dass sie infiziert waren. Solche Kontakte können in öffentlichen Verkehrsmitteln, Supermärkten usw. stattfinden. Voraussetzung für die Annäherungsverfolgung ist, dass der Benutzer sein mobiles Gerät bei sich trägt, die CWA App installiert ist und er die Bluetooth Schnittstelle aktiviert hat. Denn über die Bluetooth Schnittstelle sendet der Benutzer Zufalls-IDs und empfängt die Zufalls-IDs anderer Benutzer. Durch ein von Google und Apple bereitgestelltes Framework, auf das die CWA App zugreifen kann, wird berechnet, ob bei einem der Kontakte ein besonderes Risiko für eine Ansteckung bestand. Die Algorithmen für die Berechnungen werden von dem Robert Koch Institut (RKI) zur Verfügung gestellt und entsprechen den neusten wissenschaftlichen Erkenntnissen. Das Ergebnis der Risikoeinschätzung wird dem Benutzer mit entsprechenden Handlungsempfehlungen auf dem mobilen Gerät angezeigt.

Im Detail durchläuft der Benutzer die folgenden Phasen:

I. Phase Idee

In dieser Phase entscheidet sich der Benutzer dafür, sich über die CWA App zu informieren. Er hat ggf. Fragestellungen zu der Nutzung und Funktionsweis der App sowie zu der Gewährleistung des Datenschutzes. Hierzu kann er bereits vor dem Download unterschiedliche Quellen nutzen, wie die Websites des RKI oder des Bundesministeriums für Gesundheit sowie das Google Play Store oder Apple App Store.

II. Phase Installation

Die →CWA App wird in den App-Stores der Betriebssysteme →Android von →Google (Play Store) und →iOS von→ Apple (App Store) angeboten.

Soweit sich der Benutzer für die Installation/den Download entscheidet, werden gemäß den Nutzungsbedingungen der Stores Nutzungsdaten der Benutzer übermittelt (z.B. →IP-Adressen). Nach der technischen Installation wird der Benutzer beim erstmaligen Öffnen der CWA App durch eine Einführung begleitet. Mit der Einführung erhält der Benutzer eine Übersicht über die Funktionsweise, die Nutzungsbedingungen, die Datenschutzbestimmungen sowie die erforderlichen Einwilligungen für Berechtigungen und Benachrichtigungen.

Von dem Benutzer werden folgende Berechtigungen eingeholt:

- Internetkommunikation

  Die CWA App benötigt für die Funktionen der Risikoermittlung, Testergebnisse erhalten und Testergebnis übermitteln eine Internetverbindung, um mit den Serversystemen der CWA App kommunizieren zu können.

- Bluetooth

  Die Bluetooth-Schnittstelle des mobilen Geräts muss aktiviert sein, damit das Gerät Zufalls-IDs senden und die Zufalls-IDs von anderen Smartphones erfassen und im Kontaktprotokoll des Geräts speichern kann. Hierfür wird das →Exposure Notification Framework (ENF) von Google und Apple verwendet. Die Exposure Notification ist ein Bluetooth Low Energy-Dienst. Er wurde von Google und Apple entwickelt, um die Annäherungserkennung zwischen Geräten zur Berechnung eines Ansteckungsrisikos zu ermöglichen.

- Kamera

  Bei der Durchführung eines Corona-Tests wird dem Benutzer ein QR-Code übergeben, den er mit der CWA App einscannen kann, um mobil sein Testergebnis abrufen zu können. Für den Scan des QR-Codes benötigt das mobile Gerät den Zugriff auf die Kamera.

- Hintergrundaktivität

  Die CWA App nutzt den Hintergrundbetrieb, um das Risiko einer Ansteckung automatisch zu ermitteln und den Status eines registrierten Tests abzufragen. Wenn der Hintergrundbetrieb im Betriebssystem deaktiviert wird, muss der Benutzer alle Aktionen in der CWA App manuell starten.

- Lokale Benachrichtigungen

  Der Benutzer wird lokal über Ansteckungsrisiken und vorhandene Testergebnisse benachrichtigt

Die CWA App führt eine Erkennung der eingestellten Systemsprache durch, um dem Benutzer die Informationen über die Nutzung der CWA App in der für ihn verständlichen Sprache bereitzustellen. Wenn die erkannte Systemsprache nicht von dem Umfang der CWA App umfasst ist, wird Englisch als Sprache ausgewählt.

III. Phase der Anwendung

Folgend wird die Anwendungsphase in vier Phasen unterteilt:

1. Anwendungsphase: App läuft im Hintergrund

Im Ruhezustand (Idle Mode) des mobilen Geräts läuft die CWA App im Hintergrund. Der Benutzer bekommt zur Pseudonymisierung jeden Tag eine neue Zufalls-ID, also einen Tagesschlüssel (in den Dokumentationen wird dieser →Temporary Exposure Key (TEK) genannt). Aus diesem Tagesschlüssel werden aller 10 bis 20 Minuten neue Zufalls-IDs zur weiteren Pseudonymisierung berechnet (diese werden in den Dokumentationen → Rolling Proximity Identifier (RPI) genannt). Die kurzlebigen Zufalls-IDs sendet das mobile Gerät permanent an seine Umgebung. Außerdem speichert das Gerät automatisiert und verschlüsselt die kurzlebigen Zufalls-IDs, die von in der Nähe befindlichen Geräten gesendet werden, einschließlich definierter Parameter über die Entfernung und Dauer des Kontakts der Geräte. Zur sprachlichen Klarstellung und Unterscheidung werden die Tagesschlüssel eines Benutzers, sobald dieser positiv auf das Corona Virus getestet wurde, als Positivschlüssel bezeichnet. In regelmäßigen Abständen lädt die CWA App das aktuelle Paket der Positivschlüssel der Benutzer vom Systemserver, die sich freiwillig als infiziert gemeldet und ihre Tagesschlüssel mit der Gemeinschaft geteilt haben. Aus den Positivschlüsseln, die ja Tagesschlüssel sind, können die gesendeten kurzlebigen Zufalls-IDs (RPI) durch Berechnungen rekonstruiert und mit den gespeicherten Zufalls-IDs im Gerät verglichen werden, um einen möglichen Kontakt zu ermitteln. Diese Berechnungen werden nicht durch die CWA App selbst, sondern durch das von Google und Apple zur Verfügung gestellte Framework (ENF) durchgeführt. Die CWA App wird durch das Framework im Fall eines risikobehafteten Kontakts informiert und kann die Benachrichtigung an den Benutzer weitergeben.

2. Anwendungsphase: Kontaktfall

Im festgestellten Kontaktfall zu infizierten Personen erhält der Benutzer jeweils automatisch eine Benachrichtigung und verhaltensbezogene Empfehlungen. Hier kann zum Beispiel die Kontaktaufnahme mit dem Hausarzt, dem zuständigen Gesundheitsamt und/oder die freiwillige häusliche Isolation empfohlen werden.

3. Anwendungsphase: Testinformationsprozess

Im Fall eines durchgeführten Corona-Tests kann der Benutzer über die CWA App den digitalen Testinformationsprozess starten und so durch die App über das Testergebnis benachrichtigt werden.

Wenn der Benutzer einen Corona-Test durchführt, wird ihm ein →QR-Code übergeben. Der QR-Code enthält eine ID (in den Dokumentationen →Globally Unique Identifier (GUID) genannt). Vereinfacht gesagt, handelt es sich hierbei um eine lange Nummer, die zur Pseudonymisierung eingesetzt wird. Denn so muss der Benutzer später in der CWA App nicht seinen Namen angeben. Außerdem wird das Testergebnis nicht gemeinsam mit dem Namen des Benutzers auf dem Server gespeichert, sondern mit der GUID. Auch das Labor bekommt den QR-Code mit der Probe des Benutzers, so dass es später das Testergebnis mit der GUID pseudonymisiert auf den Server laden kann.

Nachdem der Benutzer den QR-Code mit der CWA App gescannt hat, verbindet sich das mobile Gerät mit dem sogenannten Verification Server. Dieser Server ist für den Verifikationsprozess verantwortlich. Der Verification Server speichert die in dem QR-Code enthaltene GUID und gibt an die CWA App eine neue ID zurück, den Registration Token. Die weitere Kommunikation zwischen dem Verification Server und der CWA App findet nur noch über den Austausch des Registration Token statt. Damit soll erreicht werden, dass der QR-Code nur für ein mobiles Gerät verwendet werden kann. Damit kann auch das Testergebnis nur von diesem mobilen Gerät abgefragt werden.

Soweit der Benutzer es wünscht, fragt die CWA App das Testergebnis regelmäßig automatisch ab. Hierzu verbindet sie sich mit dem Verification Server unter Mitteilung des Registration Token. Der Verification Server fragt dann bei dem Test Result Server an, ob ein Testergebnis für die GUID des Benutzers vorliegt. Der Test Result Server antwortet, mit „positiv“, „negativ“, „ausstehend“ oder „ungültig“. Der Verification Server leitet diese Information an die CWA App weiter, speichert sie aber nicht. Das Ergebnis wird dann in der App angezeigt.

Der Benutzer muss den digitalen Testinformationsprozess nicht nutzen. Er kann nach wie vor auf analogem Weg von seinem Arzt oder dem Gesundheitsamt benachrichtigt werden.

4. Anwendungsphase: Infektfall/ Verbreitung positiver Infektionsstatus

Im Fall eines positiven Corona-Tests kann der Benutzer freiwillig die in dem Framework (ENF) von Google und Apple gespeicherten, täglich an ihn vergebenen Zufalls-IDs der letzten 2 Wochen veröffentlichen. Weil der Benutzer selbst infiziert ist, heißen diese Tagesschlüssel von nun an Positivschlüssel.

Wenn der Benutzer sein positives Testergebnis mit der CWA App abgerufen hat, wird er gefragt, ob er seine Positivschlüssel auf den Server laden möchte, um anderen mitzuteilen, dass sie sich angesteckt haben könnten. Wenn der Benutzer zustimmt, generiert der Verification Server eine TAN und sendet diese an die CWA App. Die TAN wird als Autorisierung und Beweis dafür, dass ein positives Testergebnis vorliegt, mit den Positivschlüsseln der letzten 2 Wochen auf einen anderen Server des Systems, den CWA Server, geladen. Der CWA Server nimmt die TAN und fragt bei dem Verification Server an, ob die TAN valide ist. Dieser antwortet entsprechend. Nur, wenn eine positive Bestätigung durch den Verification Server vorliegt, speichert der CWA Server die Positivschlüssel in der Datenbank. Falls der Upload fehlschlägt, erhält der Benutzer eine entsprechende Rückmeldung, dass die Daten erneut eingereicht werden müssen.

Es gibt verschiedene Szenarien, in denen der Benutzer die CWA App zwar schon zur Kontaktverfolgung nutzte und auch ein positives Testergebnis vorliegt, der Benutzer aber keinen QR-Code besitzt und damit keine Möglichkeit hat, eine TAN generieren zu lassen und die Positivschlüssel hochzuladen. Das betrifft die Fälle, in denen das Labor mangels technischer Ausstattung nicht an das System angebunden ist und das Testergebnis deshalb nicht gemeinsam mit der GUID auf den Test Result Server geladen werden kann. Außerdem sind die Fälle betroffen, in denen der Benutzer von dem Arzt oder Gesundheitsamt keinen QR-Code erhalten hat oder der QR-Code verlorenen gegangen ist oder beschädigt wurde.

Um seine Positivschlüssel dennoch mit der Gemeinschaft teilen zu können, kann der Benutzer die →Verifikationshotline anrufen und eine →teleTAN erfragen. Die teleTAN ist eine TAN, die zur Plausibilisierung des Vorliegens eines positiven Testergebnisses generiert wird. Weil sie telefonisch übermittelt wird, heißt sie zur sprachlichen Unterscheidung teleTAN. Wenn der Benutzer die Verifikationshotline anruft, um eine teleTAN zu erfragen, muss er einen Plausibilitätstest durchlaufen. Es ist zu erwarten, dass sich der Benutzer zu Beginn des Telefonats namentlich vorstellt. Der Mitarbeiter der Hotline darf den Namen des Benutzers bei Bedarf auf einen Zettel schreiben, um ihn während des Telefonats namentlich ansprechen zu können. Der Mitarbeiter stellt sodann die Plausibilitätsfragen. Die Antworten auf diese Fragen werden in keiner Form festgehalten oder gespeichert, weder in einem System noch auf Papier. Das Stellen der Fragen dient lediglich der Prüfung durch den Mitarbeiter, ob der Benutzer so sicher und schlüssig antwortet, dass der Mitarbeiter mit großer Sicherheit davon ausgehen kann, dass ein positives Testergebnis des Benutzers vorliegt. Der Mitarbeiter erfragt sodann die Telefonnummer des Benutzers. Diese schreibt er auf einen Zettel, um den Benutzer zurückrufen und ihm die teleTAN telefonisch übermitteln zu können. Der Mitarbeiter meldet sich sodann über eine Weboberfläche bei dem Portal Server an, um eine teleTAN zu generieren. Der Portal Server erfragt beim Verification Server eine teleTAN. Der Verification Server sendet die generierte teleTAN an den Portal Server und speichert sie. Nachdem der Portal Server die teleTAN erhalten hat, wird sie dem Mitarbeiter auf der Weboberfläche angezeigt. Er ruft den Benutzer zurück und übermittelt die teleTAN. Die Telefonnummer und ggf. der Name des Benutzers werden allein für den Zweck des Rückrufs verwendet. Der Zettel wird spätestens eine Stunde nach erfolgtem Rückruf durch einen Reißwolf datenschutzgerecht zerstört. Die teleTAN ist nur eine Stunde gültig. Der Benutzer gibt die teleTAN in die CWA App ein. Diese verbindet sich mit dem Verification Server. Der Verification Server prüft, ob die teleTAN valide ist und sendet für die weitere Kommunikation mit der CWA App einen Registration Token. Außerdem sendet er an die CWA App eine TAN, so dass der Benutzer die Positivschlüssel nun auf den CWA Server laden kann.

IV. Phase Deinstallation

Der Nutzer kann die CWA App jederzeit deinstallieren. Alle in der CWA App gespeicherten Daten werden dadurch gelöscht.

F. Designentscheidungen

Nachfolgend werden die Designentscheidungen dargestellt, mit denen den Bedrohungen für die Rechte und Freiheiten der Benutzer der CWA App begegnet wurde. Ebenfalls wird dargestellt, aus welchen Gründen bestimmte Designentscheidungen getroffen wurden.

gelbe Markierungen sind noch nicht umgesetzt

I. Bedrohungen für den Datenschutz

1. Zweckgebundenheit & Epidemiologischer Sinn

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

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
Zweckgebundenheit & Epidemiologischer Sinn Die Verarbeitung von personenbezogenen Daten ist immer an einen Zweck gebunden. Dieser muss vor der Datenverarbeitung ganz konkret festgelegt werden und kann nicht beliebig ausgetauscht werden.	D-1-1	CCC, Nr. 1 EDSA, Rn. 36 ff., Anhang PUR-1	**Das Robert Koch Institut (RKI) hat für den Einsatz der App die folgenden Zwecke verbindlich festgelegt:** ✓ Der Benutzer soll automatisch darüber informiert werden, ob er Kontakt zu einer infizierten Person hatte und ob wegen der Dauer des Kontakts und des Abstands zu der Person ein Infektionsrisiko besteht.	DSK Rahmendokument, Kapitel 7

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
Außerdem muss der Zweck auch erreichbar sein. Die Datenverarbeitung darf also nicht mit einem utopischen Ziel gerechtfertigt werden. Deshalb ist es notwendig, dass wissenschaftlich festgestellt wird, ob die CWA App überhaupt geeignet ist und eine epidemiologisch signifikante Wirksamkeit entfaltet.			✓ Dem Benutzer sollen durch die CWA App (auf Basis der aktuellen Empfehlungen des RKI) Informationen zu seinem Infektionsrisiko und Empfehlungen zu Gesundheits- und Infektionsschutzmaßnahmen bereitgestellt werden, um Infektionsketten zu unterbrechen. ✓ Soweit der Benutzer es wünscht, sollen er durch die CWA App möglichst schnell und direkt über sein Testergebnis informiert werden, so dass er ohne Zeitverlust Maßnahmen zur eigenen Gesundheitsfürsorge und zur Reduzierung des Ansteckungsrisikos für andere Personen ergreifen kann. ✓ Soweit der Benutzer es wünscht, kann er sein positives Testergebnis für die Gemeinschaft verfügbar machen, so dass andere darüber informiert werden können, dass sie sich in unmittelbarer Nähe zu einer infizierten Person aufgehalten haben. ✓ Zu anderen Zwecken dürfen die Daten nicht verarbeitet werden.	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
Ein epidemiologischer Effekt kann nach bisher rein theoretischen Modellierungen dann angenommen werden, wenn 60 Prozent der Bevölkerung die CWA App nutzen.	D-1-2	FifF DSFA, S. 63	**Wissenschaftliche Erkenntnisse zur Zweckerreichung** ⚠ Es ist aktuell nicht abschätzbar, ob dieses Ziel erreicht werden kann. Mit den Designentscheidungen soll die Akzeptanz in der Bevölkerung erhöht und eine breite Nutzung gefördert werden.	
	D-1-3	EDSA, Anhang PUR-2	**Kein Einsatz für Überwachung von Quarantänemaßnahmen** ✓ Die App wird nicht unter Umgehung ihres primären Verwendungszwecks für die Überwachung von Quarantänemaßnahmen oder Ausgangsbeschränkungen und/oder der Einhaltung von Maßnahmen der sozialen Distanzierung eingesetzt.	DSK Rahmenkonzept 10.2
	D-1-4	EDSA, Anhang PUR-3	**Keine Standortbestimmung** ✓ Die App wird nicht dazu verwendet, Schlüsse über den Standort der Benutzer auf der Grundlage ihrer Interaktionen und/oder anderer Kriterien zu ziehen.	DSK Rahmenkonzept 10.2

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
	D-1-5		**Geräteausstattung der Benutzer** Um den epidemiologischen Zweck der CWA App erreichen zu können, müssen möglichst viele Personen die App nutzen. Hierfür ist es notwendig, dass die Benutzer technisch entsprechend ausgerüstet sind. ⚠ Die CWA App wurde für Apple's iOS and Google's Android entwickelt. Die Entscheidung für die Auswahl der Technologie für die Kontaktberechnung ist nicht zugunsten der neusten Technologie ausgefallen, die den Kontakt hätte genauer bestimmen können. Es wurde sich für die Bluetooth Low Energy Technologie entschieden, da diese auch in älteren mobilen Geräten vorhanden ist und so ein größerer Benutzerkreis mit der CWA App versorgt werden kann. ✓ Das für das Scannen der Umgebung nach vorhanden Bluetooth Signalen notwendige Exposure Notification Framework (ENF) wird ab der Apple OS Version 13.5 (Release: 20.05.2020) verfügbar sein. ✓ Für Android Geräte wird das Feature in das Google Play Store integriert, so dass nur die Google Play Anwendung aktualisiert werden muss. Geräte ab der Android Version 6.0 (Release: 05.10.2015) werden das Framework nutzen können.	Solution Architecture.md – GitHub

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
	D-1-6	EDSA Anhang FUNC-3	**Falsche Ergebnisse der Kontaktberechnungen in der CWA App** Die Berechnung des Risikos des Kontakts mit Infizierten findet ausschließlich lokal auf dem mobilen Gerät statt. Um den Zweck der CWA App zu erreichen, sollten einerseits die Benutzer nicht unnötig alarmiert werden und andererseits aber auch möglichst keine Kontakte übersehen werden, bei denen es zu einer Übertragung des Virus gekommen ist. ✓ Die Gleichung, mit der die gefährdenden Kontakte berechnet werden, wird durch das RKI vorgegeben. In der Gleichung gibt es eine ganze Anzahl von Faktoren (sog. Parameter und Gewichte), die angepasst werden können. Die Berechnung der Kontakte kann so immer wieder neu konfiguriert werden. Auf diese Weise können die neuesten wissenschaftlichen Erkenntnisse und die aktuelle Pandemielage stets berücksichtigt werden. ✓ Die Parameter und Gewichte werden über den CWA Server an die Mobilgeräte der Benutzer verteilt und kommen so unmittelbar zur Anwendung. Auf diese Weise kann die CWA App stets nachjustiert werden und mit der Zeit immer akkurater arbeiten.	DSK CWA App, 5.4.1 Scoping document.md - Github E07.01

2. Zweckerfüllende Funktionalität der App

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Zweckentsprechende Funktionalität der CWA App Um ihren Zweck erfüllen zu können, muss die CWA App auch die entsprechende Funktionalität aufweisen.	D-2-1	EDSA Anhang FUNC-1	**Funktion: Information an Benutzer** ✓ Die App informiert den Benutzer darüber, dass er einem Infektionsrisiko ausgesetzt war. Diese Information beruht auf den Berechnungen, die das mobile Gerät anhand der zuvor festgelegten Parameter lokal durchgeführt hat. Das Framework, das diese Berechnungen vornimmt, heißt Exposure Notification Framework (ENF) und wird von Google und Apple im Betriebssystem bereitgestellt. Die CWA App selbst nimmt die Berechnungen nicht vor und erhält nur das Ergebnis. Die Parameter für die Berechnung, ob es zu einer Ansteckung gekommen sein kann, sind die räumliche Nähe zu einem infizierten Benutzer innerhalb eines Zeitfensters von 2 Wochen vor dessen positivem Testergebnis (der Wert für das Zeitfenster wird von den Gesundheitsbehörden festgelegt).	Scoping_document.md - Github E04.01
	D-2-2	EDSA Anhang FUNC-2	**Handlungsempfehlungen für den Benutzer**	Scoping_document.md - Github E04.02

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			✓ Die App gibt dem Benutzer Empfehlungen, wenn berechnet wurde, dass er einem Infektionsrisiko ausgesetzt war. Neben den Empfehlungen bekommt der Benutzer Informationen darüber, wie er weiteren Rat einholen kann.	
	D-2-3	EDSA Anhang FUNC-3	**Justierbarkeit des Algorithmus** ✓ Der Algorithmus, der das Infektionsrisiko unter Berücksichtigung von Abstands- und Zeitfaktoren misst und somit bestimmt, wann ein Kontakt in die Kontaktnachverfolgungsliste aufzunehmen ist, ist justierbar, um die neuesten Erkenntnisse über die Ausbreitung des Virus berücksichtigen zu können.	Scoping document.md - Github E10.01 in der initialen Version nur durch ein Update der App möglich Scoping document.md - Github E07.01
	D-2-4	EDSA Anhang FUNC-4	**Benutzerinformation innerhalb der Inkubationszeit** ✓ Die Benutzer werden innerhalb der Inkubationszeit des Virus informiert, wenn sie dem Virus ausgesetzt waren.	Scoping document.md - Github E04.01
	D-2-5	EDSA Anhang FUNC-5	**Interoperabilität der CWA App innerhalb der EU** ✗ Die CWA App kann derzeit nicht mit den App-Systemen anderer Mitgliedsstaaten zur Bekämpfung der Corona Pandemie zusammenarbeiten.	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
	D-2-5	EDSA Anhang DATA-1, TECH-1	**Bluetooth Low Energy zur Kontaktverfolgung** ✓ Die App ist in der Lage, Daten über Nahkommunikationstechnologien wie Bluetooth Low Energy Daten zu senden und zu empfangen, damit Kontakte nachverfolgt werden können.	Scoping_document.md - Github E01.04
Anbindung mehrere Bluetooth Geräte gleichzeitig Die CWA App funktioniert reibungslos, selbst wenn mehrere Bluetooth Geräte eingebunden sind.	D-2-6		**Bluetooth Low Energy zur Kontaktverfolgung** Bluetooth erlaubt die gleichzeitige Verbindung zu mehr als 7 Geräten. Die Bluetooth Verbindungen laufen über dieselben Antennen und teilen sich das ISM Spektrum. Bluetooth ist in der Lage, einzelne Kanäle für die Kommunikation zu favorisieren und kann so diejenigen auswählen, in denen keine weiteren drahtlosen Geräte funken. Auch die zur Verfügung stehende Bluetooth Bandbreite ist ausreichend (2000 kb/s), um mehrere Bluetooth Geräte gleichzeitig parallel zu bedienen (Kopfhörer, Tastatur, andere BLE Geräte wie Wearables, usw.).	Bluetooth Core Specification, Version 5.2 | Vol 2, Part B Kap 1. General Description, Seite 414
Erfassung von Hindernissen (Wand) zwischen den Benutzern Bluetooth Low Energy kann keinen Unterschied machen, ob eine Wand oder	D-2-7		**Erfassung der gesendeten Signalstärke** Derzeit wird der Berechnung für die räumliche Distanz der Kontakte die empfangene Signalstärke zugrunde gelegt. Wenn ein Signal mit unter 50 dB empfangen wird, wird	Exposure Notification Bluetooth Specification, S. 4 Advertising Payload

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
ein Glass zwischen den Benutzern vorliegt. Das kann zu falschen Berechnungsergebnissen führen.			davon ausgegangen, dass die Personen unter 2 Metern voneinander entfernt waren. Das Exposure Notification Framework (ENF) von Google und Apple sendet zusätzlich durch die Metadaten des Bluetooth-Pakets die gemessene abgestrahlte Sendeleistung von den Bluetooth Nachrichten. Damit kann empfängerseitig miterfasst werden, mit welcher Signalstärke der Sender das Signal gesendet hat, um die Entfernung mit der tatsächlichen empfangenen Signalstärke zu berechnen. ⚠ Je nach Umgebung, findet man diverse Materialien (Beton, Glass, Spanplatte usw.), die sich zwischen Personen befinden und eine unterschiedliche Auswirkung auf die Dämpfung des Bluetooth Signals ausüben können. Es wird daran geforscht, diese Hindernisse in der Berechnung zu berücksichtigen.	Bluetooth Core Specification Version 5.2 | Vol 6, Part A

2.1 Fehlfunktion

Folgende Designentscheidungen/ Bewertungen dienen verschiedenen Datenschutzschutzzielen (Transparenz, Vertraulichkeit…) durch die Vermeidung von Fehlfunktionen der CWA.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Zweckentsprechende Funktionalität der CWA App Die CWA App könnte durch eine Fehlfunktion eine große Menge an Alarmen auslösen, die dann für alle Kontaktpersonen eine 14-tägige Quarantäne bedeuten würde. Falls ein solcher Fehler mehrfach auftreten würde, bestünde die Gefahr, dass die Benutzer nicht mehr bereit sind, den Empfehlungen - beispielsweise zur Selbstisolation – nachzukommen.	D-2.1-1	FifF DSFA S. 70	**Ständige Weiterentwicklung des Algorithmus** ✓ In dem Algorithmus für die Berechnung des Ansteckungsrisikos lässt sich ein minimaler Risikowert einstellen, ab dem Kontakte überhaupt erst berücksichtigt werden und außerdem zwei Wertebereiche (Ranges) für die Bewertung des Ansteckungsrisikos. All diese Parameter und Gewichte können von Experten des RKI auf der Grundlage mathematischer Modelle unter Berücksichtigung beispielsweise der Anzahl durchgeführter Tests und des Verhältnisses positiver zu negativer Testergebnisse immer wieder neu festgelegt werden. Der neue Algorithmus wird über den CWA Server an die Mobilgeräte der Benutzer verteilt und kommt so unmittelbar zur Anwendung.	DSK CWA App, 5.4.1
Sicherheitslücken Open Source Komponenten Sicherheitslücken in Open Source Software Komponenten können, soweit sie die Funktionalität der CWA App einschränken oder das Vertrauen der Benutzer in die Sicherheit der App beschädigen dazu beitragen, dass der Zweck der App nicht	D-2.1-2	EDSA Anhang FUNC-2	**Umgang mit Sicherheitslücken** ✓ Um das Risiko durch Sicherheitslücken in verwendeten Open Source Software Komponenten möglichst gering zu halten, werden die eingesetzten Komponenten stets auf dem neuesten Stand gehalten. Dabei wird auf die GitHub Security Alerts for Vulnerable Dependencies zurückgegriffen.	DSK CWA Server, 5.3.7

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
erreicht werden kann. Deshalb ist es wichtig, dass ein geordneter Prozess für den Umgang mit Sicherheitslücken besteht.			Zusätzlich kommen die Werkzeuge WhiteSource und Vulas in einer SAP-internen Pipeline zum Einsatz.	

2.2 Fehlgebrauch

Nachfolgend werden Designentscheidungen und Bewertungen aufgeführt, die Risiken für Betroffene infolge Fehlgebrauch der CWA App minimieren sollen.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
Beeinträchtigung der Funktionalität durch fehlerhafte Einstellungen Durch fehlerhafte Einstellungen in der CWA App beispielsweise, wenn der Benutzer der App nachträglich Berechtigungen entzieht oder die Bluetooth Schnittstelle deaktiviert, kann die Zweckerreichung der App vereitelt werden.	D-2.2-1	FifF DSFA S. 70	**Warnung über fehlerhafte Einstellungen** ✓ Um eine Beeinträchtigung der Funktionalität der App durch unbeabsichtigte, fehlerhafte Einstellungen oder Manipulation Dritter (z.B. bei ungesichert liegen gelassenem Mobilgerät) zu vermeiden, wird der Benutzer der App darüber in Kenntnis gehalten, wenn aktuelle Einstellungen der App ihre Funktionalität beeinträchtigen.	DSK CWA App, 5.4.6
Unsachgemäße Verwendung des Mobilgeräts	D-2.2-2	EDSA Anhang FUNC-2	**Aufklärung der Benutzer über unsachgemäße Verwendung des Mobilgeräts**	DSK CWA App, 5.5.5

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
Die CWA App kann das mobile Gerät nicht einer bestimmten Person zuordnen. Es kann auch nicht sichergestellt werden, dass der Benutzer das mobile Gerät jederzeit bei sich führt. Zudem kann nicht ausgeschlossen werden, dass ein Benutzer zwei Geräte verwendet und er eines bei sich trägt, das die pseudonymisierten IDs der Kontakte gespeichert, er mit der App eines anderen Geräts aber den QR-Code scannt, der mit dem positiven Testergebnis verknüpft ist. Der Benutzer kann auch nicht daran gehindert werden, auf ein ihm zugängliches Mobilgerät einer anderen Person zurückzugreifen. Darüber hinaus kann ein Benutzer sein Mobilgerät mit anderen Personen, zum Beispiel aber nicht nur mit den Angehörigen seines Haushalts, teilen.			⚠ Die Benutzer können durch geeignete Werbe- und Aufklärungskampagnen zu einer ordnungsgemäßen Nutzung aufgefordert und angeleitet werden.	
Verspäteter Scan des QR-Codes Wenn der Benutzer einen Corona-Test durchführt, wird ihm ein QR-Code übergeben. Der QR-Code enthält eine ID, vereinfacht gesagt, eine lange Nummer,	D-2.2-3		**Umgang mit Sicherheitslücken** ⚠ Diesem Problem könnte nur durch die Ausübung eines entsprechenden Zwangs begegnet werden, nämlich indem der Benutzer direkt bei der Durchführung des Tests zum Scan des QR-Codes gezwungen werden	DSK CWA App, 5.5.6 DSK CWA App, 5.5.7

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
damit der Benutzer später in der App nicht seinen Namen angeben muss und das Testergebnis nicht gemeinsam mit dem Namen des Benutzers auf dem Server gespeichert wird. Auch das Labor bekommt den QR-Code mit der Probe des Benutzers und lädt später das Testergebnis mit der ID auf den Server. So kann der Benutzer über die CWA App sein Testergebnis abrufen und wenn er möchte, in einem weiteren Schritt mit der Gemeinschaft teilen. Wenn der Benutzer keinen QR-Code erhalten oder ihn verloren hat, ihm aber bereits ein positives Testergebnis vorliegt und er dieses gern mit der Gemeinschaft teilen möchte, kann er bei der Verifikationshotline anrufen und eine teleTAN erfragen. Diese Nummer plausibilisiert das Vorliegen eines positiven Testergebnisses und dass der Benutzer andere Benutzer infiziert haben könnte. Der Benutzer kann nun unter Eingabe der teleTAN, seine IDs, die die App täglich für ihn generiert und an andere mobile Geräte in der Umgebung gesendet hat, auf den Server laden, um andere zu warnen.			würde. Bei der Einführung der CWA App in Deutschland wird in allen Belangen auf die Freiwilligkeit des Benutzers gesetzt. Es soll gerade kein Zwang entstehen. Der Benutzer kann sich in allen Phasen der App entscheiden, in welchem Umfang er die App nutzen möchte. So ist er auch nicht gezwungen, nach der Durchführung des Tests das Ergebnis des Tests über die App abzurufen oder gar mit der Gemeinschaft zu teilen. Er kann sich genauso gut dafür entscheiden, die App ausschließlich für die Warnung über den Kontakt mit infizierten Personen zu nutzen. Die Benutzer können grundsätzlich durch geeignete Werbe- und Aufklärungskampagnen zu einer ordnungsgemäßen Nutzung, insbesondere dem Unterlassen der Weitergabe des QR-Codes, aufgefordert und angeleitet werden. Es bleibt jedoch an dieser Stelle nur, auf die Kooperation der Benutzer zu vertrauen.	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
Problematisch ist, wenn ein Benutzer seinen QR-Code nicht unmittelbar bei Erhalt mit seinem mobilen Gerät scannt bzw. die teleTAN nicht in das Gerät eingibt, sondern an eine andere Person zur erstmaligen Verwendung weitergibt, die eigentlich nicht infiziert ist. Bei einem solchen Fehlgebrauch kann der Zweck der App nicht erreicht werden.				

2.3 Vertrauensverlust der Bevölkerung in Vertrauenswürdigkeit der App

Da die CWA auf der Freiwilligkeit und Kooperationsbereitschaft möglichst eines Großteils der Bevölkerung beruht, müssen die Designentscheidungen dem Ziel dienen, einen Vertrauensverlust der Bevölkerung zu vermeiden.

Nachfolgend sind die entsprechenden Designentscheidungen und Bewertungen aufgeführt.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Vermeiden von Sicherheitslücken und Datenschutzvorfällen Um das Vertrauen der Bevölkerung in die Sicherheit der App und die Gewährleistung des Datenschutzes nicht zu verlieren bzw. zu gewinnen, sind eine Reihe von öffentlichkeitswirksamen Maßnahmen notwendig. Insbesondere ist es hilfreich, wenn die CWA App einschließlich ihrer Infrastruktur von unabhängigen Sicherheitsforschern überprüft werden kann. Diese können gegenüber der Presse und in eigenen Veröffentlichungen zudem belegen, dass tatsächlich nur die notwendigsten Datenverarbeitungen vorgenommen werden und es beispielsweise zu keiner zentralen Profilbildung kommt. Um die Sicherheit der CWA App auch zukünftig zu gewährleisten, ist es sinnvoll, an einem Bug-Bounty-Programm teilzunehmen. Hier können sich Sicherheitsforscher eine Belohnung verdienen, wenn sie Schwachstellen verschiedener Kritikalitätsstufen aufdecken. Sehr gut hat sich dies beispielsweise auf das Vertrauen der Bevölkerung in den Passwortmanager KeePass ausgewirkt, so	D-2.3-1	FifF DSFA S. 70	**Open-Source** ✓ Alle Komponenten sind Open-Source. Die Community kann so an der Sicherheit der App mitarbeiten und ihre Funktionsweise prüfen.	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
dass auch hier mit sehr positiven Effekten zu rechnen ist. Außerdem sollten die Abschlussberichte der Penetration-Tests veröffentlicht werden. Denn so wird der Öffentlichkeit gezeigt, dass sich der Verantwortliche ständig um die Sicherheit kümmert, Sicherheitslücken sucht, sieht und sie behebt.				
	D-2.3-2	EDSA Anhang FUNC-2	**Teilnahme an Bug-Bounty-Programm** ⚠ Ein Bug-Bounty-Programm (sinngemäß „Kopfgeld-Programm für Programmfehler“) wird von den Verantwortlichen für die Applikation gestartet, um Fehler in der Software zu identifizieren, zu beheben und bekanntzumachen. Den Entdeckern wird als Belohnung ein Sach- oder Geldpreis versprochen. Die Initiierung eines Bug-Bounty-Programms würde das Vertrauen der Bevölkerung in die Sicherheit der CWA App deutlich erhöhen.	
	D-2.3-3		**Update der Open Source Komponenten** ✓ Um das Risiko durch Sicherheitslücken in verwendeten Open Source Software Komponenten möglichst gering zu halten, werden die eingesetzten Komponenten	DSK CWA App, 5.4.12

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			stets auf dem neuesten Stand gehalten. Dabei wird auf die GitHub Security Alerts for Vulnerable Dependencies zurückgegriffen.	
	D-2.3-4		**Regelmäßige Penetration Tests und Veröffentlichung der Berichte** ⚠ Für sogenannte Penetration Tests sind Sicherheitsforscher engagiert, die wie ein Hacker nach Sicherheitslücken in der CWA App suchen. Die Penetration Tests sollten durch verschiedene Anbieter durchgeführt werden, da jedes Team bei der Durchführung der Tests einen eigenen Fokus und Schwerpunkt hat. Die Penetration Tests werden mindestens vor jedem Release einer neuen Version der CWA App durchgeführt. Die Abschlussberichte der Tests werden veröffentlicht	

3. Rechtmäßigkeit der Verarbeitung

Die Datenverarbeitungen durch die Nutzung und den Betrieb der CWA App müssen auf eine Rechtsgrundlage gestützt werden können, andernfalls ist die Datenverarbeitung personenbezogener Daten rechtswidrig.

Da kein Gesetz die Nutzung der CWA vorschreibt und die Datenverarbeitung regelt, wird die Datenverarbeitung in ihren verschiedenen Phasen ausdrücklich auf die Einwilligung der Nutzer gestützt. Die Nutzung der CWA App und die damit zusammenhängenden Datenverarbeitungen sollen nur aufgrund der Einwilligung des Einzelnen möglich sein. Eine Einwilligung ist nur dann wirksam, wenn sie hinreichend informiert und freiwillig erfolgt.

3.1 Freiwilligkeit der Nutzung der CWA-App und der Einwilligungen in die Datenverarbeitung

Im Folgenden werden die Designentscheidungen dargestellt, die im Zusammenhang mit der Einwilligung stehen, um folgenden Risiken zu begegnen:

- Unwirksame Einwilligung aufgrund fehlender / fehlerhafter ausdrückliche Einwilligungserklärung (technischer Einwilligungs-Akt)
- Unwirksame Einwilligung aufgrund Nichterreichbarkeit der notwendigen Informationen (sprachliche Barrieren, fehlendes Technikverständnis)
- Unbefugte Nutzung der App durch Minderjährige unter 16 Jahre

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Verbot mit Erlaubnisvorbehalt Im Datenschutz besteht der Grundsatz des Verbots der Datenverarbeitung mit Erlaubnisvorbehalt. Die Datenverarbeitungen durch die Nutzung und den Betrieb der App müssen also auf eine Rechtsgrundlage gestützt werden können. Dazu erklärt der Benutzer seine Einwilligung für die verschiedenen	D-3.1-1	CCC, Nr. 2, EDSA, Rn. 43, 46 EDSA Anhang DATA-8	**Einholung und Erteilung der Einwilligung bei Installation der CWA App** ✓ Beim erstmaligen Start der CWA App wird der Benutzer über die Funktionsweise der App informiert und es werden ihm die Nutzungsbedingungen und Datenschutzbestimmungen angezeigt. Mit Nutzung der App akzeptiert der Benutzer die Nutzungsbedingungen und Datenschutzbestimmungen.	Scoping document.md - Github E01.01 und E01.02 Scoping document.md - Github E01.03 und E01.04 CWA App Screens

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Verarbeitungstätigkeiten im Zusammenhang mit der CWA App. Die Einwilligung muss informiert erfolgen und freiwillig sein.			✓ Bei der Installation der App wird die Einwilligung des Benutzers für die Datenverarbeitungen durch die CWA App eingeholt. Der Benutzer wird ausdrücklich um seine Einwilligung für die Risikoermittlung einer Ansteckungsgefahr gebeten (dezentrale Kontaktnachverfolgung). Die Erteilung dieser Einwilligungen ist Voraussetzung für die Nutzung der App.	
	D-3.1-2		**Unbefugte Nutzung der App durch Minderjährige unter 16 Jahre** ⚠ Eine Gewährleistung und Dokumentation der Einwilligung von Erziehungsberechtigten für Kinder- und Jugendliche unter 16 Jahren ist nicht möglich, ohne dafür personenbezogene Daten zu erheben. Sowohl in den Nutzungsbedingungen als auch in der Datenschutzerklärung wird daher klargestellt, dass die Nutzung der CWA App für Personen ab 16 Jahre vorgesehen ist. Außerdem werden die Jugendschutzmöglichkeiten des Google Play Store und Apple App Store genutzt. ⚠ Für das Folge-Release der CWA App soll außerdem ein Popup-Fenster implementiert werden, mit dem sinngemäßen Inhalt: „Wenn Du unter 16 Jahre alt	Jugendschutzeinstellungen bei Google Play, Kindersicherung auf dem iPhone, App Store Vorschau Altersfreigaben

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			bist, dann besprich bitte die Nutzung der App mit Deinen Eltern." ⚠ Für die CWA App ist es nicht möglich, die unbefugte Nutzung durch Kinder und Jugendliche unter 16 Jahren und damit auch die (unbefugte) Datenverarbeitung (technisch oder organisatorisch) auszuschließen. Infolge dieser unbefugten Datenverarbeitung können auch Schäden für die Rechte und Freiheiten der Benutzergruppe entstehen. ✓ Erziehungsberechtigte können dies verhindern, wenn sie auf den mobilen Geräten ihrer Kinder unter 16 Jahren Jugendschutzeinstellungen vornehmen, die eine Nutzung der CWA App ausschließen.	
	D-3.1-3		**Erreichbarkeit/ Lesbarkeit der Informationen in der Sprache der Benutzer** ✓ Bei der erstmaligen Nutzung der App wird die Systemsprache ausgelesen, so dass dem Benutzer die Informationen und Texte für die Einwilligungen in seiner Sprache angezeigt werden können. Wenn die erkannte Systemsprache nicht im Content	Scoping document.md - Github E01.06 Scoping document.md - Github E01.07, E09.01 - E09.03

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			hinterlegt ist, wird im Default Englisch ausgewählt. Die App ist zudem barrierefrei programmiert.	
	D-3.1-4		**Datenschutzfreundliche Voreinstellungen** ✓ Die Benachrichtigungen in der App sind per Voreinstellungen ausgeschaltet. Der Benutzer muss sie aktiv einschalten und kann ihr Verhalten individuell gestalten (z.B. durch Auswahl eines individuellen oder auch eines allgemeinüblichen Benachrichtigungstons). ✓ Auch alle weiteren Berechtigungen, wie für die Internetkommunikation, Bluetooth-Aktivierung, Nutzung der Kamera und Hintergrundaktivität werden eingeholt.	DSK CWA App 5.4.5 Scoping document.md - Github E01.05
	D-3.1-5	EDSA Anhang PRIV-9	**Einholung und Erteilung der Einwilligung für die Abfrage der Testergebnisse** ✓ Für die Abfrage und den Erhalt von Testergebnissen muss der Benutzer seine Einwilligung erklären. Für den Fall, dass der Benutzer nicht durch die App über das Testergebnis informiert werden möchte, ist ein alternativer Prozess etabliert.	Solution Architecture.md – GitHub Scoping document.md - Github E06.03, E06.04; DSK Verifikation und Testergebnis, 6.4.1.1.2

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
	D-3.1-6	EDSA Anhang PRIV-9, ID-1	**Einholung und Erteilung der Einwilligung für den Upload der Positivschlüssel** ✓ Nach dem Erhalt des positiven Testergebnisses muss der Benutzer seine Einwilligung für den Upload seiner Positivschlüssel der letzten 2 Wochen erklären.	CWA App Screens
	D-3.1-7	EDSA Anhang PRIV-9, ID-2	**Keine zentrale Speicherung der Kontakthistorie** ✓ Der CWA Server erhält die Kontakthistorie der mit dem Virus infizierten Benutzer nicht.	Exposure Notification Bluetooth Specification

3.2 Freiheitsbeschränkungen bei Nicht-Nutzung der App oder Freiheitsgewinne bei Nutzung der App / Erzwungene Einwilligung

Die Freiwilligkeit der Einwilligung des Betroffenen ist zwingend, damit die Datenverarbeitung rechtmäßig ist. Es besteht jedoch die Gefahr, dass sich Benutzer durch Druck von außen (Arbeitgeber, Staat, Nachbarn o.ä.) zum Einsatz der CWA App gezwungen sehen.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Erzwungene Einwilligung Es ist möglich, dass der Benutzer in einzelnen Situationen durch die Anwendung von äußerem Druck oder gar Gewalt zum Einsatz der App genötigt wird. Knüpfen die Besitzer oder Betreiber im allgemeinen öffentlich zugänglicher Einrichtungen wie z.B. Restaurants, Bars, Ladengeschäfte, Kinos oder Kultureinrichtungen oder gar Behörden den Zugang zu ihrer Einrichtung an das Vorweisen der auf einem Mobilgerät installierten App, wird damit die Freiwilligkeit der Nutzung der App de facto außer Kraft gesetzt. (Quelle: DSK CWA App, 5.5.16)	D-3.2-1	FifF DSFA S. 72	⚠ Die Anzeige in der CWA App kann nicht so gestaltet werden, dass sie keinen Nutzen für den Benutzer hat. Somit kann technisch nicht ausgeschlossen werden, dass die Anzeige durch Benutzer mit Dritten geteilt wird. ✓ Durch Sensibilisierung, dass es sich bei der Nutzung zu solchen Zwecken, um einen bußgeldbewerten Verstoß handelt, sowie Kontrolltätigkeiten der Datenschutzaufsichtsbehörden der Länder könnte diesem Risiko begegnet werden. ✓ Zudem könnte dieser Zwang ins Leere laufen, wenn sich betroffene Bürger beispielsweise eine App installieren, die der CWA App nach ihrem äußeren Erscheinungsbild ähnelt, aber nur aus Screenshots besteht. So könnten die Bürger vortäuschen, dass sie die CWA App nutzen und nicht infiziert sind.	DSK CWA App, 5.4.5 DSK CWA App, 5.5.16

3.3 Gefahr der Diskriminierung

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Unbeobachtbarkeit der Kommunikation Auch wenn die Übermittlung einer Nachricht im System beobachtet wird (z. B. über die Metadaten der Kommunikation), darf daraus nicht geschlossen werden können, dass eine Person selbst infiziert ist oder Kontakt zu Infizierten hatte. Dies ist sowohl gegenüber anderen Benutzern als auch gegenüber Infrastruktur- und Netzbetreibern oder Angreifern, die Einblick in diese Systeme erlangen, sicherzustellen.	D-3.3-1	CCC, Nr. 10	**Benachrichtigungsfunktion für den CWA App Benutzer und andere Benutzer** ⚠ Falls ein Benutzer durch eine visuelle, textuelle oder auch akustische Benachrichtigung von der App über einen möglichen Kontakt mit einem Infizierten oder das Vorliegen eines Testergebnisses informiert wird, kann dies je nach situativem Kontext den Grund der Benachrichtigung der aktuellen Umgebung des Benutzers anzeigen. Liegt das Mobilgerät etwa in einem Zugabteil offen auf einer Ablage, kann der auf dem Display erscheinende Nachrichtentext oder die Visualisierung der Nachricht für Mitreisende sichtbar sein. Erfolgt die Benachrichtigung mit einem für die App typischen Klingelton, kann dies von Personen in unmittelbarer Umgebung des Benutzers wahrgenommen werden. **Datenschutzfreundliche Voreinstellungen** ✓ Deshalb sind Benachrichtigungen in der App per Voreinstellung ausgeschaltet. Der Benutzer muss sie aktiv einschalten und kann ihr Verhalten individuell gestalten (z.B. durch Auswahl eines individuellen oder auch eines allgemeinüblichen Benachrichtigungstons).	DSK CWA App, 5.4.5

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			✓ Gegenüber Infrastruktur- und Netzbetreibern oder Angreifern, die Einblick in diese Systeme haben sind die Daten der Benutzer insbesondere durch die Maßnahme zur Pseudonymisierung (siehe unten 5.1) und zur Trennungskontrolle (siehe unten 10.) geschützt.	

4. Transparenz

Designentscheidungen und Bewertungen in diesem Kapitel dienen vor allem dem Schutzziel der Transparenz. Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise erhoben und verarbeitet werden.

Gefahren der Intransparenz und fehlenden Prüfbarkeit der verarbeiteten Daten und Funktionsweise der CWA App soll begegnet werden.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Transparenz und Prüfbarkeit Um eine Prüfbarkeit der CWA App und Infrastruktur durch Auditoren, Aufsichtsbehörden und die kritische	D-4-1	CCC, Nr. 4 EDSA Anhang GEN-3	**Veröffentlichung des vollständigen Quelltextes** ✓ Die App und die Backend-Infrastruktur folgen dem Open-Source-Prinzip - lizenziert unter Apache 2.0.	Github Dokumentation, README.de.md unter „Über dieses Projekt“

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Öffentlichkeit zu ermöglichen, muss der vollständige Quelltext zur Verfügung stehen.				
Durchführung einer Datenschutzfolgen-abschätzung Die mit der Datenverarbeitung verbundenen Risiken für Rechte und Freiheiten der von der Datenverarbeitung Betroffenen werden in einem strukturierten Verfahren zur Risikoabschätzung erfasst und bewertet. Es werden Gegenmaßnahmen festgelegt, Restrisiken bestimmt und die Ergebnisse öffentlich gemacht.	D-4-2	EDSA, Rn. 39	**Durchführung einer Datenschutzfolgenabschätzung** ✓ Es wird eine Datenschutz-Folgenabschätzung (DSFA) vor der Einführung der App durchgeführt, da die Verarbeitungen als mit einem hohen Risiko behaftet eingestuft werden (Gesundheitsdaten, voraussichtliche flächendeckende Einführung, systematische Überwachung, Einsatz neuer technologischer Lösungen).	DSFA Bericht
	D-4-2a		**Einholung des Standpunktes der Betroffenen** ✓ In Vorbereitung und während der Durchführung der DSFA wurden explizit die Standpunkte von CCC, FifF berücksichtigt. Dies wird mit diesem Dokument nachgewiesen. ✓ Kommentare zu den auf Github veröffentlichten Dokumenten sind in die Diskussionen um Designentscheidungen und die Bewertung mit eingeflossen.	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
	D-4-3	EDSA, Rn. 39, Anhang PRIV-6	**Veröffentlichung der Datenschutzfolgenabschätzung** ✓ Die Datenschutzfolgenabschätzung wird veröffentlicht.	

5. Verdecktheit/ Unbeobachtbarkeit und Vertraulichkeit

Wesentliche Maßnahmen zur Sicherstellung der Bindung der Verarbeitungstätigkeiten für einen ausgewiesenen Zweck besteht im Allgemeinen darin, pseudonymisierte und anonymisierte Daten, bei denen der Personenbezug so weit wie möglich aufgehoben oder unter Bedingungen gestellt ist, zu verwenden und die Datenbestände, Kommunikationsbeziehungen und Teilprozesse dieser Verarbeitungstätigkeit von anderen Verarbeitungstätigkeiten zu trennen[18].

Dem Grundsatz der Vertraulichkeit folgend, dürfen personenbezogene Daten nur einem berechtigten Personenkreis für bestimmte Zwecke offenbar werden. Sie sind vor unbefugter Veränderung zu schützen.

5.1 Anonymität/Pseudonymität und verschlüsselte Speicherung der Pseudonyme

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Art. 4 Nr. 5 DSGVO).

Bei den Zufallszahlen, die auf dem Smartphone kreiert werden, und für die CWA erforderlich sind, handelt es sich um personenbezogene Daten im Sinne der DSGVO, da ein Personenbezug mit dem Gerätenutzer herstellbar ist. Die nachfolgende Datenverarbeitung im Rahmen der CWA erfolgt pseudonymisiert, da unmittelbare Identifizierung allein aufgrund der Zufallszahlen und ohne Bezug zu einem Smartphone erschwert wird.

[18] FifF DSFA, S. 43

Im Nachfolgenden sind die Designentscheidungen bezüglich der Pseudonymisierung genauer dargestellt. Es wird dabei auch beschrieben, welche Anforderung damit adressiert wird bzw. erklärt, aus welchen Gründen von Anforderungen abgewichen wurde.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
Anonymität Daten, die jedes Gerät über andere Geräte sammelt, dürfen zur De-Anonymisierung ihrer Benutzer nicht geeignet sein. Die Daten, die jede Person ggf. über sich weitergibt, dürfen nicht zur De-Anonymisierung der Person selbst geeignet sein. Das System muss so beschaffen sein, dass weder absichtlich noch unabsichtlich Bewegungsprofile (Standortverfolgung) oder Kontakt-Profile (auf konkrete Menschen zurückführbare Muster von häufigen Kontakten) aufgebaut werden können.	D-5.1-1	CCC, Nr. 7 und 8 FifF DSFA S. 83 EDSA, Rn. 41, Anhang PRIV-7, PRIV-8	**Keine Identifizierung von Kontaktpersonen durch den Benutzer der CWA App** ✓ Benutzer der App können nicht auf die gespeicherten Rolling Proximity Identifier (RPI) der Personen zugreifen, mit denen sie in Kontakt getreten sind, da diese lokal in einem sicheren Bereich des Geräts (Smartphone) in dem Framework, das von Google und Apple bereitgestellt wird, gespeichert sind. Dieses Framework von Google/ Apple ist das Exposure Notification Framework (ENF). Auf diesen Speicherbereich kann nur durch das ENF zugegriffen werden.	Solution Architecture.md – GitHub
Es MUSS unmöglich sein, verschiedene temporäre IDs der gleichen Benutzer in Zusammenhang zu setzen. Sie dürfen beispielsweise nicht auf einem mathematischen Seed basieren, der eine spätere Verkettung ermöglicht.	D-5.1-2		**Kontaktnachverfolgung mittels ENF** ✓ In dem Exposure Notification Framework von Google und Apple sind Expositionen (risikobehaftete Kontakte) definiert als eine Zusammenfassung aller Begegnungen mit einer anderen Person an einem einzigen Kalendertag. Aus Datenschutzgründen ist es nicht möglich, Begegnungen mit anderen Personen	Solution Architecture.md – GitHub

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
			über mehrere Tage hinweg zu verfolgen, auch wenn die Daten dafür vorliegen. Wenn der Benutzer also über mehrere Tage hinweg mit derselben infizierten Person in Kontakt war, wird dies durch die Berechnungen des Frameworks nicht erfasst.	
	D-5.1-3		**Anonymität/ Pseudonymität der Benutzer innerhalb der CWA** ✓ Benutzer bleiben innerhalb des Corona-Warn-App-Systems anonym, solange ihre Temporary Exposure Keys (TEK) auf ihrem Smartphone verbleiben. Sobald TEKs (im Falle eines positive Testergebnisses) auf den Server hochgeladen werden, wird aus Anonymität Pseudonymität. Die Temporary Exposure Keys der letzten 2 Wochen werden ab dem Zeitpunkt des positiven Testergebnisses Positivschlüssel genannt.	Github - Prüfsteine für die Beurteilung von „Contact Tracing“-Apps
	D-5.1-4		✓ Die Begegnungsdaten mit einer infizierten Person (exposures) verbleiben lokal auf dem Gerät und werden nicht geteilt (dezentrale Lösung).	DSK CWA App 4.2.2, 5.4.7
	D-5.1-5		**Re-Identifikation von Positivschlüsseln nur über Smartphone**	Github - Prüfsteine für die Beurteilung

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
			✓ Wenn der hochgeladene Positivschlüssel verfügbar ist, können alle RPIs eines bestimmten Tages einem einzelnen Positivschlüssel zugeordnet werden. Es ist jedoch nicht möglich, diesen Positivschlüssel konkreten, die App nutzenden Personen oder der International Mobile Equipment Identity (IMEI) von deren Smartphone zuzuordnen, ohne Zugang zum gesicherten Speicher des Geräts (Smartphones) zu haben.	von „Contact Tracing“-Apps
	D-5.1-6		**Verschlüsselte Speicherung von Daten anderer CWA-App Benutzer** ✓ Die gespeicherten Rolling Proximity Identifiers (RPI), die der Benutzer von anderen App Benutzern empfangen hat, enthalten Metadaten z.B. über die Signalstärke, durch die auf die Entfernung der Personen geschlossen werden kann. Diese Metadaten werden verschlüsselt abgelegt.	Solution Architecture.md – GitHub
	D-5.1-7		⚠ Das Exposure Notification Framework von Google und Apple nicht dazu konzipiert, ununterbrochen die Bluetooth-Signale der Umgebung aufzufangen und zu speichern. Stattdessen lauscht das Framework nur alle	Solution Architecture.md – GitHub DSK CWA App, 5.5.2

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
			fünf Minuten für jeweils 20 Sekunden an der Umgebung, um dazwischen für 280 Sekunden inaktiv zu werden. Es werden also nur Kontakte erkannt und festgehalten, die innerhalb des kurzen aktiven Zeitfensters oder über einen längeren Zeitraum hinweg stattfinden. Insgesamt können durch die beschriebenen Effekte sowohl Kontakte mit Infizierten registriert werden, die epidemiologisch nicht relevant sind, als auch solche übersehen werden, die möglicherweise für eine Ansteckung von Bedeutung sein könnten. Da sich das Empfangen der Bluetooth-Signale merklich auf den Energieverbrauch auswirkt, mussten Google und Apple hier eine Abwägung treffen und haben sich für die beschriebene Lösung entschieden.	
	D-5.1-8	EDSA Anhang PRIV-10	**Verification erfolgt mittels Verification Server und nicht durch den CWA-Server** ✓ Die Anfragen der App an den zentralen Server (CWA-Backend) enthalten keine Hinweise auf den Status als infizierte Person. Um die Herstellung einer Verbindung zwischen einem bestimmten Gerät und der GUID/teleTAN zu verhindern, erhält der Benutzer, wenn er mit der App	Solution Architecture.md – GitHub DSK Verifikation und Testergebnis, 6.1.3.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
			sein Testergebnis abfragt oder einen TAN zum Upload seiner Daten erhalten möchte, einen Registration Token (Sitzungs-ID). Der Registration Token identifiziert eine Langzeit Session zwischen der App und dem Verification Server. Auf diese Weise müssen keine personenbezogenen Daten im CWA-Backend gespeichert werden. Der Registration Token hat eine Länge von 128 Bit. Hashing des Registration Token: SHA-256, no salt, no pepper	
	D-5.1-9	EDSA Anhang PRIV-10	**Erschwerung der Re-Identifizierung durch Trennung von Positivschlüssel und Transportmetadaten** ✓ Wenn der Benutzer seine Positivschlüssel hochlädt, werden die Transportmetadaten (wie die IP-Adresse) entfernt und in einen dafür vorgesehenen Akteur verschoben, der „Transport Metadata Removal“ heißt.	Solution Architecture.md – GitHub
	D-5.1-10	EDSA Anhang SEC-2	**Erschwerung von Angriffen durch sicheren Transportweg zwischen CWA-Server und Verification Server** ✓ Die an den Verification Server und CWA Server gesendeten Daten werden über einen sicheren Kanal übermittelt.	DSK Verifikation und Testergebnis 6.1.5.1 DSK CWA Server 4.3.1, 5.3.5

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
	D-5.1-11	EDSA Anhang SEC-4	**Allgemein: Einsatz von Verschlüsselungstechnologie** ✓ Es werden hochmoderne kryptografische Techniken eingesetzt, um den Austausch zwischen der App und dem Server sowie zwischen Anwendungen zu sichern und um generell die in den Apps und auf dem Server gespeicherten Informationen zu schützen. Etablierte Verschlüsselungsmechanismen wie HTTP over TLS (HTTPS) stellen sicher, dass Nachrichten von außen nicht lesbar sind. Um das Risiko von Man-in-the-Middle-Angriffen weiter zu reduzieren, wird durch HTTP Public Key Pinning sichergestellt, dass vertrauliche Kommunikation nur zwischen der CWA App und dem Server stattfindet. **Verschlüsselte Speicherung auf dem TestresultServer** ✓ Die auf dem Test Result Server liegenden Daten (Ergebnisse des Corona-Tests: Hashed GUID, Testergebnis, Datum des Imports) werden mit TLS 1.2 verschlüsselt, Kommunikation ist verschlüsselt, auf Client OS Crypto SDK implementiert.	Github - Prüfsteine für die Beurteilung von „Contact Tracing“-Apps Solution Architecture.md – GitHub DSK Verifikation und Testergebnis 6.2.5.1, 6.2.5.3 DSK CWA Server 4.3.1
Von EDSA genannte Maßnahmen, die durch andere Maßnahmen ersetzt wurden	D-5.1-11a		✓ Dieses Protokoll ist bei der vorliegenden Architektur allenfalls für den Abruf des Testergebnisses relevant.	DSK Rahmenkonzept 9.5.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
Von EDSA Anhang SEC-4 vorgeschlagenes Protokoll „Private Membership Test mit Bloom Filter" Hierbei handelt es sich um eine True/False Anfrage an die Datenbank, ob sich ein bestimmter Eintrag in der Datenbank befindet. Dabei sollte der Betreiber der Datenbank keine Informationen über die Identität des Clients (hier das mobile Gerät) erhalten.			Es wird nicht angewandt, weil sich der Benutzer nicht mit einem Klarnamen gegenüber den Servern identifizieren muss. Der Benutzer hat mit dem Covid19-Test einen QR-Code erhalten, den er mit seinem mobilen Gerät einscannt. Diesen QR-Code bekommt außerdem das Labor mit der Probe des Benutzers. Nachdem der Benutzer den QR-Code scannt, wird die darin enthaltene GUID (Global Unique Identifier) gehasht und an den Verification Server übertragen. Der Verification Server vergibt für die App des Benutzers eine weitere ID, den Registration Token. Der Registration Token dient fortan dem Austausch zwischen dem Verification Server und dem mobilen Gerät. So kann sich die App gegenüber dem Verification Server authentifizieren und es wird sichergestellt, dass eine GUID nur einem Gerät zugeordnet ist. Die GUID und der Registration Token werden gehasht auf dem Verification Server gespeichert. Für den Abruf des Testergebnisses fragt der Verification Server dann mit der gehashten GUID bei dem Test Result Server an, ob ein Testergebnis für die GUID vorliegt. Denn sobald dem Labor das Testergebnis bekannt ist, lädt es das Testergebnis ebenfalls mit der gehashten GUID (über das Laboratory Information System (LIS)) auf den Test	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
			Result Server. Auch dort wird die GUID ausschließlich gehasht gespeichert. Die Antwort, die der Verification Server von dem Test Result Server bekommt, wird unter Verwendung des Registration Token an die App ausgeliefert. Es werden also zu keiner Zeit personenbezogene Daten verarbeitet, die den Benutzer direkt (ohne Zusatzwissen) identifizieren könnten.	
Von EDSA genannte Maßnahmen, die durch andere Maßnahmen ersetzt wurden Von EDSA Anhang SEC-4 vorgeschlagenes Protokoll „Private Set Intersection" (PSI) (Intersection = hier Schnittmenge) PSI ist ein Protokoll zur Berechnung von Schnittmengen von Datensätzen. Dabei sollen nur die Daten ausgetauscht werden, die der Schnittmenge entsprechen. Dieses Protokoll wäre relevant, wenn für die Berechnung der Kontakte mit infizierten Personen (exposure) alle Kontaktdaten auf den Server geladen werden würden, um dort	D-5.1-11b		✓ Die Designentscheidung ist bewusst auf die dezentrale Lösung der Architektur der App gefallen. Die Berechnung der kritischen Kontakte mit infizierten Personen findet lokal auf dem mobilen Gerät statt. Dafür werden die Positivschlüssel (Tagesschlüssel) aller infizierten Personen von dem Server auf das Gerät geladen. In dem Exposure Notification Framework (ENF) von Google und Apple werden aus den heruntergeladenen Tagesschlüsseln (TEK) die dazugehörigen kurzlebigen IDs (RIP) der positiv getesteten Benutzer (die diese wechselnd aller 10 bis 20 Minuten ausgesendet haben) durch komplizierte Berechnungen wiederhergestellt. In dem Framework werden diese IDs mit den durch das Gerät empfangenen IDs abgeglichen. Hierin besteht die oben beschriebene Schnittmenge (Intersection). Sowohl die berechnete Schnittmenge als auch alle	DSK CWA App 4.2.2

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
die Berechnung vorzunehmen (zentrale Lösung).			anderen Kontaktdaten sind durch die Nutzung des vor anderen Apps abgeschirmten ENF gut geschützt. Da kein Austausch der Kontakthistorie mit dem Server stattfindet, ist die Anwendbarkeit des Protokolls PSI nicht einschlägig.	
Von EDSA genannte Maßnahmen, die durch andere Maßnahmen ersetzt wurden Von EDSA Anhang SEC-4 vorgeschlagenes Protokoll „Private Information Retrieval" (PIR) Hierbei handelt es sich um ein Protokoll, bei dem eine Anfrage an eine Datenbank gestellt und auch beantwortet werden kann, ohne dass die Datenbank Aussagen über den angeforderten Eintrag machen kann. Die Anfragen können daher auch nicht miteinander verknüpft werden, um die Interessen des Anfragenden zu ermitteln. So wird die Privatheit des Anfragenden unterstützt, auch wenn er öffentliche Datenbanken benutzt.	D-5.1-11c		✓ Für den Abruf der Positivschlüssel aller infizierten Benutzer wäre dieses Protokoll ungeeignet, da hier ohnehin der gesamte Inhalt also alle Positivschlüssel vom Content Delivery Network (CDN) zum Download zur Verfügung gestellt werden. Denkbar wäre der Einsatz dieses Protokolls also nur für den Abruf des Testergebnisses. Da hier jedoch, wie bereits oben unter "Private Membership Test mit Bloom Filter" beschrieben, nur bereits stark pseudonymisierte Daten verarbeitet werden, ist ein Rückschluss auf den einzelnen allein durch die auf dem Server befindlichen Daten nicht möglich. Die pseudonymisierten Daten haben zudem nur eine begrenzte Gültigkeit. So wird die gehashte GUID nach 14 Tagen von den Servern gelöscht. Später folgende Abfragen werden ignoriert.	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
Von EDSA genannte Maßnahmen, die durch andere Maßnahmen ersetzt wurden Von EDSA Anhang SEC-4 vorgeschlagene „homomorphe Verschlüsselung“ Homomorphe Verschlüsselung kann zur Wahrung der Privatsphäre bei der ausgelagerten Speicherung und Berechnung verwendet werden. Auf diese Weise können Daten verschlüsselt und zur Verarbeitung in kommerzielle Cloud-Umgebungen ausgelagert, wobei alle Daten verschlüsselt werden.	D-5.1-11d		✓ Die Homomorphe Verschlüsselung wird nicht angewandt, weil die Auslagerung von Daten nicht notwendig ist.	
	D-5.1-12		**Erschwerung Re-Identifizierung durch Trennung der IT-Systeme** ✓ Die Testergebnisse werden nicht auf dem Verification Server, sondern nur auf dem Testresult Server gespeichert.	Solution Architecture.md – GitHub
	D-5.1-13		✓ Der Verification Server und der CWA Server werden von unterschiedlichen Personen und in verschiedenen Cloud Subscriptions der OTC betrieben.	DSK Rahmendokument, 9.8

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
Re-Identifizierungsversuche durch Peilung Verwendet ein potenzieller Angreifer zwei oder mehrere Mobilgeräte, besteht für ihn die Möglichkeit über Bluetooth oder WiFi die Sender von Signalen oder Datenpaketen in seiner Umgebung zu peilen und ihre ungefähre Richtung und Entfernung zu ermitteln. Durch den zusätzlichen Einsatz z.B. einer Videokamera könnte die Identifizierung sendender Personen gelingen.	D-5.1-14		**Erschwerung der Re-Idenditfizierung durch Peilung** ✓ Die Peilung mit Bluetooth wird dadurch erschwert, dass sich die ausgesandten Rolling Proximity Identifier alle zehn bis zwanzig Minuten ändern.	DSK CWA App 5.5.12
	D-5.1-15		**Abschirmung von Kommunikationsmustern** ⚠ Neben einzelnen Nachrichten, die vom System übertragen werden, müssen auch Kommunikationsmuster abgeschirmt werden. Ein Beispiel: Der Sendeaufruf von Testergebnissen und die Übermittlung von Positivschlüsseln würde normalerweise nur im Fall einer tatsächlichen Infektion stattfinden. In diesem Fall könnte man durch die Beobachtung des Netzwerkverkehrs erkennen, dass	DSK CWA App, 5.4.8

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
			eine nutzende Person einen Covid19-Test gemacht hat und positiv getestet wurde. Ab dem Folge-Release werden, um dies zu verhindern, zufällig generierte unechte Meldungen versendet, die von gültigen Meldungen in Größe und Reaktion des Servers nicht unterschieden werden können (Dummy Pakete). Dadurch sind die Übermittlung von Schlüsseln und der Abruf von Testergebnissen nicht vom Hintergrundrauschen der Systeme unterscheidbar. Dies führt selbst bei beobachtbarem Netzwerkverkehr zu einer plausiblen Abstreitbarkeit. Damit ein „Fake Request“ eine gleiche Antwortzeit hat, wird die Antwort verzögert ausgegeben. Ermittlung eines Wertes für die Bearbeitungszeit von fake Requests, damit von außen nicht unterschieden werden kann, ob ein echter oder ein fake Request bearbeitet wird. Der jeweils verwendete Wert wird zu einem bestimmten Anteil vom realen Zeitverbrauch beeinflusst.	
	D-5.1-16		**Verhinderung Personenbezug bei Positivschlüsseln** ✓ Um zu verhindern, dass auf indirektem Weg der Bezug von Positivschlüsseln zu einer natürlichen Person hergestellt werden kann, werden die Daten der Netzwerkverbindung (insbesondere die verwendete IP-Adresse), mit der die Positivschlüssel vom Client auf	DSK CWA Server, 5.3.2

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
			den CWA Server geladen werden, nur kurzfristig in den Logs der Netzwerkebene abgespeichert. Dort werden sie zur Abwehr von Denial of Service Attacken benötigt (s. unten). ✓ Die Anwendungsschicht des CWA Servers erhält keinen Zugriff auf die Daten der Netzwerkverbindung. Zur Einhaltung der Aufbewahrungsfristen und, um den Clients das gezielte Laden von Deltabeständen der Positivschlüssel zu ermöglichen, werden die empfangenen Positivschlüssel jeweils mit einem Zeitstempel versehen. Dieser Zeitstempel wird auf die letzte volle vergangene Stunde abgerundet. Dadurch ist ein Bezug auf den genauen Zeitpunkt der Netzwerkverbindung nicht möglich, und selbst bei Zugriff auf die Logs der Netzwerkschicht können die Daten der ursprünglichen Netzwerkverbindung nicht zugeordnet werden.	
	D-5.1-17		✓ Um zu verhindern, dass die gespeicherten Positivschlüssel über Netzwerkinformationen zu mobilen Geräten zugeordnet werden können, wird der Zeitstempel des Übertragungszeitpunkts auf die letzte volle vergangene Stunde abgerundet.	DSK CWA Server, 4.4.8.3

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
	D-5.1-18	EDSA Anhang PRIV-16	✓ Auf dem Portal Server werden keine IP-Adressen aufbewahrt.	DSK Verifikation und Testergebnis, 6.3.5.4.
	D-5.1-19		✓ Die Server werden von getrennten Teams betrieben, um Re-Identifikationsattacken durch Admins zu erschweren. Um Sicherzustellen, dass kein Missbrauch der Administrationsrechte stattfindet werden die Logs in regelmäßigen Abständen geprüft und ausgewertet.	DSK Rahmenkonzept 9.8
Bluetooth Sniffer Ein Angreifer könnte das Bluetooth Netzwerk überwachen, um festzustellen, welche Rolling Proximity Identifier (RPI) von welchem mobilen Gerät gesendet werden, um den Sender zu identifizieren und den Personenbezug herstellen zu können.	D-5.1-20		**Randomisierte Geräteadressen** ✓ Für das Broadcasting der Rolling Proximity Identifier (RPI) werden randomisierte Geräteadressen genutzt, die sich regelmäßig ändern. So können die RPI anderer Nutzer zwar empfangen werden. Aber durch die sich ständig ändernden Bluetooth Adressen kann nicht zugeordnet werden, welches Gerät die RPI gesendet hat.	Exposure Notification Bluetooth Specification, Seite 5 (Broadcasting Behaviour)
Verdecktheit und Vertraulichkeit bei der Verifikations-Hotline	D-5.1-21		⚠ Der Prozess der Verifikations-Hotline wurde aufgrund des schnellen Marktanganges der CWA App entwickelt. Er soll zuallererst der Überbrückung der Prozessdiskrepanzen und Fragen der Benutzer der	DSK Verifikations-Hotline, 8.2.1

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
Wenn der Benutzer die Verifikationshotline anruft, um eine teleTAN zu erfragen, stellt er sich ggf. dem Mitarbeiter der Hotline namentlich vor. Der Mitarbeiter schreibt den Namen des Benutzers bei Bedarf auf einen Zettel. Der Mitarbeiter verwendet den Namen des Benutzers allenfalls, um ihn während des Telefonats namentlich anzusprechen. Der Mitarbeiter stellt sodann die Plausibilitätsfragen. Die Antworten auf diese Fragen werden ebenfalls in keiner Form persistiert, weder in einem System noch auf Papier. Das Stellen der Fragen dient lediglich der Prüfung des Mitarbeiters, ob der Benutzer so sicher und schlüssig antwortet, dass der Mitarbeiter mit großer Sicherheit davon ausgehen kann, dass ein positives Testergebnis des Benutzers vorliegt. Der Mitarbeiter erfragt sodann die Telefonnummer des Benutzers. Diese schreibt er auf einen Zettel, um den Benutzer zurückrufen und ihm die teleTAN telefonisch übermitteln zu können. Die Telefonnummer			App in der Startphase der CWA dienen. Risiken für Rechte und Freiheiten Betroffener wurden in der DSFA betrachtet und im DSK aufgeführt und bewertet. **Vertragliche Bindung des Hotline - Betreibers** ✓ Zwischen der DTAG und dem Hotline-Betreiber AXIVAS wird ein AVV geschlossen und über den Rahmenvertrag hinaus folgendes verbindlich vereinbart (Auszug) : • Der Auftragsverarbeiter verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist. Der Verantwortliche weist den Auftragsverarbeiter darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, nach § 203 Abs. 4 S. 1. StGB strafbar machen. Der Auftragsverarbeiter wird seine Beschäftigten und andere für den Auftragsverarbeiter tätige Personen entsprechend den gesetzlichen	DSK Verifikation-Hotline, 8.2.2

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
und ggf. der Name wird allein für den Zweck des Rückrufs verwendet. Sie wird spätestens eine Stunde nach erfolgtem Rückruf durch einen Reißwolf datenschutzgerecht zerstört.			Anforderungen auf diese Geheimnisschutzregeln nach § 203 StGB verpflichten. • Die DTAG stellt AXIVAS von der Verpflichtung frei, ankommende oder ausgehende Rufnummern zu speichern oder Gespräche aufzuzeichnen. • AXIVAS versichert, dass entsprechende Speicherungen nicht vorgenommen werden, respektive Anrufnummern direkt nach dem Gespräch wieder gelöscht werden. ⚠ Beschleunigte Anbindung der Labore. Mögliche Handlungsoptionen: Abgestuftes Verfahren zur Persistierung eines minimalen Sets an personenbezogenen Daten, um stichprobenhaft möglichen Missbrauch zu überprüfen. Prüfung alternativer Verifikationsprozesse.	

5.2 Grundlegende Privatsphäre

Nachfolgend werden Designentscheidungen zusammengefasst, die der Sicherstellung der Privatsphäre dienen.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
	D-5.2-1	CCC, Nr. 3 EDSA, Anhang PRIV-2	✓ Die CWA App ermöglicht keine direkte Identifizierung der Benutzer.	DSK CWA App, 5.6
	D-5.2-2		✓ Die Benutzer müssen sich für keinen Prozess der CWA App identifizieren und können fortlaufend unter einem Pseudonym agieren. Auch die Verifikationshotline, die zur Anfrage einer teleTAN genutzt werden kann, erfragt nicht den Namen des Benutzers, sondern nach der Stellung von Plausibilitätsfragen nur dessen Telefonnummer.	DSK Verifikations-Hotline, 8.1.1.
	D-5.2-3	EDSA DATA-2	✓ Zur Pseudonymisierung des Covid19-Tests und damit des Benutzers wird ein GUID (QR-Code) vergeben. Der Verification Server verarbeitet nur gehashte GUIDs. Der GUID hat eine Gesamtlänge von 152 Bit. Er besteht aus einem Präfix von 24 Bit und einem Hauptteil von 128 Bit. Der Hauptteil wird durch ein kryptografisches Verfahren generiert. Hashing der GUID: SHA-256, no salt, no pepper,	Solution Architecture.md – GitHub Software Design Verification Server
	D-5.2-4	EDSA DATA-4	✓ Täglich wird ein neuer Temporary Exposure Keys (TEK) vergeben, aus dem aller 10 bis 20 Minuten ein neuer Rolling Proximity Identifier (RPI) berechnet wird. Letzterer wird über das Bluetooth Low Energy (BTLE) permanent an andere Benutzer der App gesendet.	Solution Architecture.md – GitHub

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
	D-5.2-5		✓ Die mit den RPI verbundenen Metadaten (z.B. Signalstärke) werden verschlüsselt.	Solution Architecture.md – GitHub
	D-5.2-6		✓ Das Laborsystem hashed die GUID und das Testergebnis.	Solution Architecture.md – GitHub
	D-5.2-7		✓ Personenbezogene Daten werden nur verhasht auf dem Server gespeichert.	DSK Verifikation und Testergebnis 6.1.5, 6.2.5., 6.3.5.
	D-5.2-8	EDSA Anhang SEC-5	✓ Es werden keine persistenten IP-Adressen auf dem Portal Server gespeichert.	DSK Verifikation und Testergebnis, 6.3.5.4
	D-5.2-9		✓ Metadaten, die eine Identifizierung ermöglichen (z.B. die IP-Adresse), werden entfernt, bevor der CWA Server Positivschlüssel verarbeitet. Dadurch wird das Risiko weiter verringert, dass ein Angreifer diese Informationen miteinander verknüpfen kann, da sie auf Datenbankebene nicht verkettet werden können.	Github - Prüfsteine für die Beurteilung von „Contact Tracing“-Apps

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
	D-5.2-10	EDSA Anhang ID-5	✓ Anwendungs-Logfiles enthalten keine personenbezogenen Daten, keine GUID, keinen gehashten GUID, keine Testergebnisse oder den Registration Token.	DSK Verifikation und Testergebnis, 6.1.6.1., 6.2.6.1, 6.3.6.1
	D-5.2-11		✓ Logfiles werden nach 30 Tagen gelöscht.	DSK Verifikation und Testergebnis, 6.1.6.1., 6.2.6.1, 6.3.6.1
	D-5.2-12		⚠ Ab dem Folge-Release werden auch Dummy Pakete an den CWA Server gesendet, um „Noise“ zu erzeugen. Es soll so verhindert werden, dass falls der Traffic im WLAN abgehört wird, die Benutzer, die Daten hochladen, automatisch als infiziert identifiziert werden können.	Solution Architecture.md – GitHub DSK CWA App, 5.4.8
	D-5.2-13		✓ Schon dadurch, dass die Positivschlüssel der letzten 2 Wochen zusammen in einem Bündel hochgeladen und auch dementsprechend in der Datenbank gespeichert werden, stehen diese miteinander in Verbindung. Um diese Verbindung aufzulösen, werden die Datenbankeinträge durch ORDER BY RANDOM durchmischt.	Solution Architecture.md – GitHub

5.3 Datenabfluss an Google und Apple und andere Externe

An dieser Stelle wird beschrieben, wie der Datenabfluss an Google/ Apple durch Designentscheidungen reduziert wird. App Stores und ENF können verwendet werden, um Daten abzuleiten.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
Datenabfluss an Google und Apple Es besteht die Gefahr, dass durch Notification-Frameworks wie Googles Firebase Cloud Messaging (FCM) oder Apples Push Notification Services (APN) Daten über die Kommunikation zwischen App und Server an Google und Apple gelangen und diese Daten durch die Anbieter ausgewertet werden.	D-5.3-1	FifF DSFA S. 75; Digitalcourage zur Einordung zur geplanten „Corona-Kontakt-Tracing-App“ des RKI; EDSA Anhang SEC-2	**Vermeidung von Push-Nachrichten durch Google/ Apple** ✓ Nach der Erteilung der Einwilligung für den Erhalt der Testergebnisse innerhalb der App werden immer wieder Anfragen an den Verification Server geschickt, ob das Testergebnis schon vorliegt. Hierfür werden Polling und lokale Benachrichtigungen verwendet. Wenn der Benutzer sich gegen lokale Benachrichtigungen entscheidet, kann er die Abfrage des Testergebnisses auch manuell durchführen. So wird die Nutzung von externen Push-Nachrichten, die über die Infrastruktur von Apple und Google versendet werden müssten, vermieden. Denn allein die Abfrage des Testergebnisses enthält die Information, dass der Benutzer sich einem Corona-Test unterzogen hat und damit Gesundheitsdaten.	Solution Architecture.md – GitHub

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
	D-5.3-2		⚠ Inwieweit Google und Apple die Daten, etwa im Zusammenhang mit sog. Crashlogs verarbeiten, entzieht sich der Kontrolle der am Projekt Beteiligten. Hierfür wird nach den verfügbaren Dokumentationen von Google/Apple die Einwilligung der Benutzer des mobilen Geräts auf Systemebene abgefragt.	

Festzuhalten bleibt, dass Risiken für die Rechte und Freiheiten von Betroffenen bestehen, die sich aus der Entscheidung ergeben, das Framework von Apple und Google für die Corona-Warn-App zu nutzen.

Diese Risiken wurden im Rahmen der Datenschutzfolgenabschätzung betrachtet und werden hier nur beispielhaft aufgeführt:

- Abhängigkeiten von Dienstleistern/ Software- und Firmware Hersteller (Ausfall externer Dienstleistern) - Google/ Apple
- Fehlende/ unzureichende vertragliche Regelungen mit Dienstleistern (Auftragsverarbeitung/ Vertrag zur gemeinsamen Verantwortung) - Google/ Apple
- Erhebung und Speicherung nicht-notwendiger Daten, inklusive Nutzer- und Metadaten durch Apple/ Google
- (Bewusste/ Unbewusste) Erteilung von Berechtigungen an Google/ Apple/ andere App-Anbieter auf Smartphone
- Zugang/ Zugriff zu Gesundheitsdaten (Infektionsstatus) trotz fehlender Berechtigungen zu CWA über API/ ENF (Datenabfluss an Google/ Apple)

6. Datensparsamkeit/ Datenminimierung

Nachfolgend werden Designentscheidungen beschrieben, die dem Datenschutzziel der Datenminimierung dienen. Danach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
Fehlende Wartung und Überprüfung der Software- bzw. Infrastruktur-Komponenten Fehlende Überprüfungen von Software kann zu mangelnder Akzeptanz und verzögerten Gegenmaßnahmen bei Security-Lücken führen.	D-6-1	CCC, Nr. 4 EDSA Anhang GEN-3	✓ Die App und die Backend-Infrastruktur folgen dem Open-Source-Prinzip - lizenziert unter Apache 2.0 . ✓ Um eine Prüfbarkeit der CWA App und Infrastruktur durch Auditoren, Aufsichtsbehörden und die kritische Öffentlichkeit zu ermöglichen, muss der vollständige Quelltext zur Verfügung stehen.	Github Dokumentation, README.de.md unter „Über dieses Projekt“
Datenanhäufung von Nutzern Durch eine hohe Installationsanzahl besteht die Gefahr, dass zu viele, zweckfremde Daten gespeichert werden und diese für andere Zwecke genutzt werden.	D-6-2	CCC, Nr. 6 EDSA, Rn. 40, Anhang PRIV-1	✓ Nach der Dokumentation von Apple und Google werden im Fall eines positiven Corona-Tests nur die Positivschlüssel der letzten 2 Wochen hochgeladen. ✓ Die pseudonymen Daten der Benutzer unterliegen einer strengen Zweckbindung. Sie werden nach 2 Wochen aus dem Exposure Notification Framework (ENF) von Google und Apple und von dem CWA Server gelöscht. Die Datensätze auf dem Verification Server werden 21 Tage nach ihrer Erstellung gelöscht (Hash der GUID und Hash des Registration Token). Das Testergebnis wird auf dem Test Result Server nach 21 Tagen durch den Zustand „redeemed“ überschrieben und damit maskiert. Nach 90 Tagen wird der Datensatz endgültig gelöscht. ✓ Es dürfen nur minimale und für den Anwendungszweck notwendige Daten und Metadaten gespeichert werden.	Solution Architecture.md – GitHub DSK CWA Server, 4.4 DSK CWA App, 4.6 DSK Verifikation und Testergebnis, 6.1.6, 6.2.6

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
Übertragung von nicht Verarbeitungsnotwendigen Daten bei Schnittstellen Durch eine unsaubere Schnittstellendefinition werden zu viele Daten übertragen, welche zweckentfremdet verwendet werden können.	D-6-3	EDSA DATA-5, DATA-7	✓ Es werden nur die absolut notwendigen Datenkategorien von der Schnittstelle (API) des Exposure Notification Framework an die App übertragen (und das gilt auch nur für den Fall, dass sich unter den gespeicherten Rolling Proximity Identifier (RPI) eine infizierte Person befindet und es zu einer Ansteckungsgefahr (exposure) gekommen sein kann): • Dämpfungswert (gemeldete Signalstärke - gemessene RSSI) • Dämpfungsbehälter (enthält z.B., ob die Signalstärke <=50 dB oder >50 dB war; es wird davon ausgegangen, dass eine Dämpfung von kleiner als 50 dB auf einen Abstand der Personen von unter 2 Metern schließen lässt) • Dauer der Begegnung mit der infizierten Person (exposure) in 5er Schritten (<5/5/10/15/20/25/30/>30 Minuten) mit Zeitstempel • Übertragungsrisikolevel (Wahrscheinlichkeit, das Benutzer infiziert wurde) in Verbindung mit den Positivschlüsseln der infizierten Person • Gesamtergebnis der Risikobewertung (berechnetes Risiko der Ansteckung entsprechend den vom RKI definierten Parametern) ✓ Weitere Informationen über die Begegnung (exposure), wie der Rolling Proximity Identifier, Temporary Exposure Keys oder die exakte Zeit	Solution Architecture.md – GitHub

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
			verbleiben in dem sicheren Bereich des Frameworks und können von der App nicht abgefragt werden. Die an die App übertragenen Datenkategorien sind für den Benutzer nicht sichtbar, sondern werden an die App über die Schnittstelle für die interne Berechnung übergeben. Dem Benutzer wird nur das Gesamtergebnis angezeigt, wenn das definierte Risikolevel erreicht ist.	
Notwendige Zustimmung von Benutzern für nicht relevante Aspekte der Datenverarbeitungen Unter dem Vorwand der zielgerichteten Nutzung der App werden zu viele Berechtigungen bzw. Zustimmungen beim Benutzer eingeholt, welches eine Zweckentfremdung der App nach sich ziehen kann.	D-6-4		✓ Die nutzenden Personen können und müssen in Verbindung mit der App ausschließlich der folgenden Angaben machen: • Zustimmung zur Nutzung des Exposure Notification Frameworks • Scannen eines QR-Codes mit dem Testergebnis • Eingabe einer teleTAN bei der Verifizierung eines Testergebnisses per Hotline • Zustimmung zum Upload der täglichen Positivschlüssel Es werden somit keine Zustimmung für nicht relevante oder überschießende Aspekte eingeholt.	Github - Prüfsteine für die Beurteilung von „Contact Tracing“-Apps
Fehlerhafte Entwicklung und Konfiguration	D-6-5	EDSA Anhang PRIV-17	✓ App und Server wurden mit großer Sorgfalt entwickelt und konfiguriert, damit keine unnötigen Daten	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
Durch Entwicklung qualitativ schlechter Software entstehen Fehler beim Betrieb der Software und derer Konfiguration, welche zu Sicherheitslücken führen kann.			erhoben werden (z.B. werden keine Kennungen in die Serverprotokolle aufgenommen) und um die Verwendung von SDK Dritter zu vermeiden, die Daten für andere Zwecke sammeln.	
Bei Anfragen an den Server werden zu viele Informationen übertragen Durch mangelnde Schnittstellenkontrakte werden zu viele Daten übertragen, welche für die Zweckerfüllung der Schnittstelle nicht von Relevanz sind.	D-6-6	EDSA Anhang PRIV-11, ID-4	✓ Anfragen der App an den zentralen Server geben keine unnötigen Informationen über den Benutzer preis, außer wenn dies in Bezug auf seine pseudonymisierten Kennungen notwendig ist.	DSK Verifikation und Testergebnis 6.1.3, 6.1.5
Übernahme von Daten aus Fremdsystemen Durch mangelnde Identifikation der übertragenen Daten werden auch Daten von interoperablen Dritten Systemen verarbeitet.	D-6-7	EDSA Anhang PRIV-15	✓ Die App erfasst nur Daten, die von Instanzen der Anwendung oder interoperablen, gleichwertigen Anwendungen übermittelt werden. Daten, die andere Apps und/oder Nahkommunikationsgeräte betreffen, werden nicht erhoben.	
Nachverfolgung von Benutzerbewegungen Die Applikation dokumentiert auch Benutzerbewegungen mit.	D-6-8	EDSA Anhang PRIV-3	✓ Die App ermöglicht keine Nachverfolgung der Benutzerbewegungen.	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
Standortdaten werden gespeichert Es werden Standortdaten durch die App gespeichert, welche eine Nachverfolgung von Benutzerbewegungen ermöglicht.	D-6-9	EDSA Anhang DATA-6	✓ Es werden keine Standortdaten für die Kontaktnachverfolgung verarbeitet, auch nicht, um die Interoperabilität mit Mitgliedsstaaten zu ermöglichen.	Section 3.3 Exposure Notification APIs Addendum Section 3.c Google COVID-19 Exposure Notifications Service Additional Terms

7. Zweckbindung/ Nichtverkettbarkeit

Nachfolgende Designentscheidungen dienen insbesondere dem Schutzziel der Zweckbindung und dem Gewährleistungsziel der Nichtverkettung. Personenbezogene Daten sind nur im Rahmen des ursprünglichen Zweckes der Verarbeitung zu verwenden und nicht mit anderen Daten zusammenzuführen. Dementsprechend darf im Laufe der Verarbeitungszwecke stehts nur der ursprünglich festgelegte Zweck verfolgt werden.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Zentrale Verarbeitung von Daten	D-7-1	CCC, Nr. 5 EDSA Anhang PRIV-5	✓ Das Vertrauen in den zentralen Server ist bei der CWA begrenzt. Die App wird auf der Grundlage einer Technologie mit einem dezentralisierten Ansatz	Github Dokumentation, README.de.md

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Durch eine zentrale Verarbeitung von Daten können pseudonymisierte Daten schneller wieder zu direkt zuordenbaren Daten zusammengefügt werden.			entwickelt. Als Grundlage dienen die Protokolle DP-3T (Decentralized Privacy-Preserving Proximity Tracing) und TCN sowie die Spezifikationen für Privacy-Preserving Contact Tracing von Apple und Google. ✓ Die dezentrale Verarbeitung personenbezogener Daten ist das mildere Mittel gegenüber einer zentralen Verarbeitung (Verhältnismäßigkeit der Maßnahme).	unter „Über dieses Projekt“
Zentrale Verarbeitung der Begegnungsdaten Durch eine zentrale Speicherung aller Daten können Benutzerprofile und Bewegungsdaten der Bevölkerung abgeleitet werden.	D-7-2	EDSA Anhang TECH-4	✓ Die Begegnungsdaten mit einer infizierten Person (exposures) verbleiben lokal auf dem Gerät und werden nicht geteilt (dezentrale Lösung).	Solution Architecture.md – GitHub
Daten der Smartphones werden zentral gespeichert Durch eine zentrale Speicherung aller Kontaktdaten der mobilen Endgeräte entsteht eine Datenanhäufung welche Auswertungen nicht zweckgemäßen Ursprungs erlaubt.	D-7-3	EDSA Anhang TECH-4	✓ Die Rolling Proximity Identifier (RPI), die über die Bluetooth Low Energy Schnittstelle von anderen Benutzern empfangen wurden, verbleiben lokal auf dem Gerät in dem Exposure Notification Framework (ENF) von Apple und Google. Selbst wenn der zentrale CWA Server kompromittiert sein sollte, können diese Informationen nicht zu Smartphones zurückverfolgt werden, wenn nicht ohnehin schon Zugriff auf das	Solution Architecture.md – GitHub

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			Smartphone besteht. Auch dann kann die App selbst nicht auf die RPIs zugreifen.	
Zentrale Berechnung von Kontakten Durch eine zentrale Berechnung von potentiellen Kontakten werden auch die Daten der Kontaktpersonen zentral abgespeichert (s.o.).	D-7-4	EDSA Anhang TECH-4	✓ Die Berechnungen, ob es durch den Kontakt zu einer infizierten Person zu einer Ansteckung gekommen sein kann, werden lokal auf dem Gerät durchgeführt.	Solution Architecture.md – GitHub
Automatisierte Übertragung der Positivschlüssel Positiv getestete Personen haben keine Möglichkeit sich für eine Übertragung der Daten aktiv zu entscheiden, sondern dies passiert automatisch durch die Nutzung der Applikation.	D-7-5		✓ Corona positiv getestete Benutzer können selbst entscheiden, ob sie ihre Positivschlüssel der letzten 2 Wochen auf den CWA Server hochladen wollen oder nicht.	Solution Architecture.md – GitHub Scoping document.md - Github E06.06
Zentrale Serverinfrastruktur wird nicht ordnungsgemäß betrieben Durch fehlende Prozesse und Zuständigkeiten entstehen Fehler beim Betrieb, welche sich im Datenschutz als auch bei der Sicherheit niederschlagen.	D-7-6	EDSA Anhang PRIV-5	✓ Die Verwaltung des zentralen Servers folgt klar definierten Governance-Regeln und schließt alle erforderlichen Maßnahmen zur Gewährleistung seiner Sicherheit ein. Der Standort des zentralen Servers ist in Deutschland, so dass eine wirksame Aufsicht durch die zuständige Aufsichtsbehörde gewährleistet ist.	DSFA Bericht, Anhang TOMs, Ziff. 1103

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Gewöhnungseffekt durch Einsatz der CWA-App Die Contact Tracing-App darf nicht zur Gewöhnung an Dauerüberwachung dienen. Ihre Nutzung muss zeitlich begrenzt werden. Nicht nur die Daten, sondern auch die App selbst müssen nach einer zeitlichen Frist rückstandsfrei vom Smartphone entfernt werden (es sei denn, der oder die Benutzer.in bestätigt aktiv, dass die App behalten werden soll). Auch die Änderungen in den Betriebssystemen Android und iOS sollten nach einer klaren Frist rückgängig gemacht werden. Die App darf nur solange eingesetzt werden, bis die Zahl der Neuinfektionen mit den Techniken der manuellen Kontaktnachverfolgung allein bewältigt werden kann.	D-7-7	Digitalcourage zur Einordung zur geplanten „Corona-Kontakt-Tracing-App“ des RKI EDSA, Anhang GEN-1, GEN-2	⚠ Es ist ein Verfahren eingerichtet, um die Erfassung der Kennungen zu unterbinden (allgemeine Deaktivierung der Anwendung, Aufforderung zur Deinstallierung der Anwendung, automatische Deinstallierung usw.) und die Löschung aller erhobenen Daten aus allen Datenbanken (mobile Anwendungen und Server) zu veranlassen, sobald die zuständigen Behörden über die „Rückkehr zur Normalität“ entscheiden.	
Sekundärnutzung bei zentraler Vergabe von ID-Tokens	D-7-8	FifF DSFA S. 74	✓ Die GUID werden nur gehasht auf Servern gespeichert. Für Server bestehen Berechtigungskonzepte. Die Server werden von getrennten Teams betrieben, um Re-Identifikationsattacken durch Administratoren zu	DSFA Bericht, Anhang TOMs, Ziff. 1010, 1014

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Gefahr der Sekundärnutzung bei zentraler Vergabe der ID-Token soll vermieden werden. Der Prozess zur Vergabe der GUID muss organisatorisch so ausgestaltet sein, dass eine Zusammenführung mit personenbeziehbaren Daten im Betrieb ausgeschlossen ist.			erschweren. Um sicherzustellen, dass kein Missbrauch der Administrationsrechte stattfindet werden die Logs in regelmäßigen Abständen geprüft und ausgewertet.	
Verhaltensauswertung durch die CWA Daten Behavioral Profiling und Compliance Scoring bei Infizierten muss vermieden werden. Betreiber können die Kontakthistorien infizierter Benutzer dazu verwenden, ein Verhaltens-Scoring zu erstellen.	D-7-9	FifF DSFA S. 70	✓ Die Auswertung der Kontakte und ein damit verbundenes Verhaltens-Scoring durch eine zentrale Stelle ist nicht möglich, da die Verarbeitung der Kontakte ausschließlich lokal auf dem mobilen Gerät stattfindet. Die Benutzer laden keine Kontakthistorie auf den Server.	DSFA Bericht, Anhang TOMs, Ziff. 1102, 1104

8. Intervenierbarkeit

Nach dem Grundsatz der Intervenierbarkeit müssen Betroffene die Möglichkeit haben, ihre entsprechend der DSGVO gewährten Rechte ungehindert auszuüben. Datenverarbeitungen müssen so gestaltet werden, dass Daten berichtigt und gelöscht werden können. Um diesen Grundsatz im Rahmen der CWA zu genügen, müsste der Personenbezug hergestellt werden. Nachfolgend wird dargestellt, dass zur Erfüllung der Betroffenenrechte der Personenbezug nicht hergestellt wird.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Beachtung der Betroffenenrechte Es muss jederzeit möglich sein, Betroffenenrechte umzusetzen, insbesondere personenbezogene Daten bei Vorliegen der Voraussetzungen zu löschen, zu berichtigen und in der Verarbeitung zu beschränken. Auch muss es möglich sein, automatisierte Entscheidung durch den Verarbeiter prüfen zu lassen: Prozess durch den Benutzer das Ergebnis der App durch einen Menschen prüfen lassen kann	D-8-1	EDSA Anhang PRIV-13	**Beachtung der Betroffenenrechte** ✓ Mit der im Rahmen der App verarbeiteten Daten können die Benutzer nicht identifiziert werden. Daher können Ersuchen nach Art. 15 bis 20 DSGVO nicht beantwortet werden. Die Bereitstellung von Informationen, die die Identifizierung der Benutzer ermöglichen würde, findet nicht statt. Dies würde dem Ziel zuwiderlaufen, den Gesamtprozess so datensparsam wie möglich durchzuführen. Die Art. 15 bis 20 DSGVO sind daher nicht anwendbar (Art. 11 Abs.2 DSGVO). ✓ Der Benutzer kann die CWA App jederzeit deinstallieren und damit alle lokal gespeicherten Daten selbst löschen. Alle weiteren Daten werden spätestens nach 21 Tagen gelöscht (siehe oben D-6-2). Ein Löschgesuch müsste nach Art. 12 Abs. 3 DSGVO spätestens nach einem Monat beantwortet werden. Das Löschgesuch wäre bei Fristablauf bereits obsolet. ✓ Eine Überprüfung der automatisierten Entscheidungsfindung (Überprüfung der Empfehlungen im Kontaktfall im Rahmen der Phase 3.2) nach Art. 22 Abs. 3 DSGVO ist nicht notwendig, da durch die App keine rechtsverbindlichen	DSK CWA App, 5.6

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			Entscheidungen getroffen werden, sondern nur Empfehlungen ausgesprochen werden.	
DSMS Etablierung eines DSMS, durch das der datenschutzkonforme Betrieb der App überwacht wird	D-8-2		**Datenschutz beim Betrieb der App** Es wird ein Datenschutzmanagementsystem zum Betrieb der App etabliert werden.	DSK Rahmendokument 12
Falsche positive Berechungsergebnisse Die Gefahr falscher „Positiver“ ist zu vermeiden: Transparenz und Anfechtbarkeit der automatisiert auferlegten Selbst-Isolation (Fehldiagnostik und Fehlbehandlung)	D-8-3	FifF DSFA EDSA, Rn. 36 ff.	**Maßnahmen zur Vermeidung falscher Positiver** ✓ Falsche Ergebnisse der Berechnungen in der App: Die Berechnung von Kontakten mit Infizierten sollte einerseits möglichst wenige Benutzer alarmieren (false positives) andererseits aber auch möglichst keine Kontakte übersehen, bei denen es zu einer Übertragung der Krankheit gekommen ist (false negatives). Deshalb gibt es eine ganze Anzahl von Parametern und Gewichten, mit denen die Berechnung der Kontakte konfiguriert werden können. Auf diese Weise können die unterschiedlichen Begleitumstände eines Kontaktes gemäß den neuesten wissenschaftlichen Erkenntnissen und der aktuellen Pandemielage stets neu bewertet und die Berechnungsvorschrift entsprechend gewichtet werden. Die Parameter und Gewichte werden über	DSK CWA App, 4.5.5.1

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			den CWA Server an die Mobilgeräte der Benutzer verteilt und kommen so unmittelbar zur Anwendung. Auf diese Weise kann die CWA App stets nachjustiert werden und mit der Zeit immer akkurater arbeiten.	
	D-8-4	EDSA, Rn. 36	Die von der App implementierten Verfahren und Prozesse, einschließlich entsprechender Algorithmen, unterliegen der strengen Aufsicht von qualifiziertem Personal des RKI, um das Auftreten falscher positiver und negativer Ergebnisse einzuschränken.	DSK CWA App 4.2.2., 4.5.5.1
	D-8-4a	EDSA, Rn. 37	Die Algorithmen sind überprüfbar und werden regelmäßig von unabhängigen Sachverständigen geprüft werden, um zu gewährleisten, dass sie den Grundsätzen der Fairness, Rechenschaftspflicht und allgemeiner den gesetzlichen Anforderungen genügen.	
Zugriff oder Beschlagnahme durch staatliche Organe Staatliche Organe wie Geheimdienste oder Strafverfolgungsbehörden können sich Zugriff auf die einzelnen Komponenten der Anwendungsarchitektur verschaffen, deren	D-8-5		⚠ Der Zugriff durch staatliche Organe muss auf Grundlage von hinreichend bestimmten Gesetzen erfolgen.	DSK CWA App, 5.5.17

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Datenbestände beschlagnahmen und durch Kombination, der ihnen zur Verfügung stehenden Informationen, den Personenbezug herstellen.				

9. Löschung/ Speicherbegrenzung

Dem Datenschutzziel der Datenminimierung folgend, dürfen personenbezogene Daten nur solange verarbeitet werden, wie dies zur Zweckerreichung notwendig ist. Nachfolgend werden Designentscheidungen dargestellt, die die Speicherbegrenzung umsetzen.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Gefahr von Deanonymisierungsangriffen Sollten die Daten nicht nach 14 Tagen gelöscht werden, wäre es möglich, sie auch rückwirkend mit anderen Daten in Verbindung zu bringen sowie Deanonymisierungsangriffe zu verüben.	D-9-1	FifF DSFA S. 72 EDSA Anhang ID-3	✓ Die Positivschlüssel werden vom CWA Server gelöscht sobald sie einen Zeitraum betreffen, der länger als 14 Tage zurückliegt. ✓ Die durch die CWA App berechneten Risikowerte werden, bis zur Neuberechnung aber bis zu maximal 2 Wochen gespeichert und dann gelöscht.	Solution Architecture.md – GitHub DSK CWA App, 4.6

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
	D-9-2		✓ Die teleTAN, TAN und Registration Token werden nach Übertragung der Positivschlüssel gelöscht vom Verification Server gelöscht.	Solution Architecture.md – GitHub DSK CWA App, 4.6
	D-9-3		✓ Der QR-Code/GUID wird nach dem Pairing des mobilen Endgerätes in der CWA App gelöscht.	DSK CWA App, 4.6
	D-9-4		✓ Alle Daten werden vom Verification Server nach 21 Tagen gelöscht.	Software Design Verification Server DSK Verifikation und Testergebnis, 6.1.6
	D-9-5	EDSA Anhang TECH-2	✓ Die Kontakthistorie des Benutzers (Rolling Identifier anderer Benutzer im ENF) wird maximal über einen Zeitraum von 2 Wochen im Gerät gespeichert.	DSK CWA App, 4.6
	D-9-6	EDSA Anhang PRIV-14	✓ Die Deinstallation der App bewirkt die Löschung aller lokal erhobenen Daten.	DSK CWA App 5.7
	D-9-7		✓ Alle Daten werden vom Test Result Server nach 21 Tagen gelöscht (maßgeblich ist das Datum aus dem	Software Design Test Result Server

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			Datenfeld „result_date“). Es werden alle Daten gelöscht deren „result_date“ älter als 21 Tage ist.	DSK Verifikation und Testergebnis, 6.2.6

10. Trennungskontrolle

Im nachfolgenden Kapitel werden Designentscheidungen aufgeführt, die der der Trennungskontrolle dienen. Die Trennungskontrolle dient ebenfalls dem Schutzziel der Zweckbindung/ Nichtverkettung.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Trennungskontrolle Hierbei handelt es sich um Maßnahmen, welche gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies kann beispielsweise durch logische oder physikalische Trennung der Daten erreicht werden.	D-10-1		✓ Es erfolgt bei einer evtl. Programmentwicklung eine Funktionstrennung zwischen Test- und Produktionsumgebung.	DSFA Bericht, Anhang TOMs, Ziff. 1045, 1069

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
	D-10-2		✓ Es dürfen nur solche Daten erhoben, gespeichert oder verarbeitet werden, die unmittelbar dem eigentlichen Zweck dienen, die zur Erfüllung der Aufgabe oder Durchführung des Prozesses zwingend notwendig sind. Dieser Zweck darf sich in keinem nachgelagerten Schritt der Verarbeitung, auch nicht nach einer Übermittlung ändern.	DSFA Bericht, Anhang TOMs, Ziff. 1065
	D-10-3		✓ Regelungen und Maßnahmen zur Sicherstellung der getrennten Verarbeitung (Speicherung, Veränderung, Löschung und Übertragung etc.) und/oder Lagerung von Daten und/oder Datenträgern mit unterschiedlichen Vertragszwecken sind zu dokumentieren und anzuwenden.	DSFA Bericht, Anhang TOMs, Ziff. 1066
	D-10-4		✓ Regelungen und Maßnahmen zur Sicherstellung der getrennten Verarbeitung (Speicherung, Veränderung, Löschung und Übertragung etc.) und/oder Lagerung von Daten und/oder Datenträgern mit unterschiedlichen Vertragszwecken sind zu dokumentieren und anzuwenden.	DSFA Bericht, Anhang TOMs, Ziff. 1066
	D-10-5		✓ Die Testergebnisse werden nicht auf dem Verification Server, sondern nur auf dem Test Result Server gespeichert. Die Daten werden auf dem Verification	DSFA Bericht, Anhang TOMs, Ziff. 1067

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			Server, Test Result Server und Portal Server getrennt voneinander verarbeitet.	
	D-10-6		✓ Die Testergebnisse werden nicht auf dem Verification Server, sondern nur auf dem Test Result Server gespeichert. Die Daten werden auf dem Verification Server, Test Result Server und Portal Server getrennt voneinander verarbeitet.	DSFA Bericht, Anhang TOMs, Ziff. 1067

11. Vertragsverhältnisse

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Einhaltung des Datenschutzes durch Dienstleister Verantwortlicher für die CWA App ist die Bundesrepublik Deutschland, vertreten durch das Bundesministerium für Gesundheit, vertreten durch das Robert Koch Institut (RKI).	D-11-1		**Abschluss von Auftragsverarbeitungsverträgen** ✓ Die Einhaltung der datenschutzrechtlichen Bestimmungen wird durch den Abschluss von Auftragsverarbeitungsverträgen (nach Art. 28 DSGVO) mit den Unterauftragnehmern sichergestellt.	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Vertragspartner des RKI sind: • Google und Apple (für die Bereitstellung der App in den App Stores und die Bereitstellung des Exposure Notification Frameworks (ENF)). Das RKI bedient sich als Verantwortlicher für den Betrieb der CWA App verschiedener Dienstleister. Direkte Unterauftragnehmer des RKI sind: • T-Systems International GmbH (für den Betrieb des CWA Backends in der Open Telekom Cloud (OTC) und der Hotline), • SAP SE (für den 3rd-Level-Support der CWA App), Die T-Systems International GmbH hat ihrerseits Unterauftragsverhältnisse mit: • Deutsche Telekom Regional Solutions & Products GmbH (1st & 1,5 Level Support für OTC)				

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
• IT Services Hungary (Operation, 1st and 2nd Level Support für OTC) • Deutsche Telekom IT GmbH (User support MyWorkplace für OTC) • Axivas Deutschland GmbH (Service Desk für OTC) • Deutsche Telekom Individual Solutions & Products GmbH (DC Hardware disposal and replace für OTC) • Axivas Deutschland GmbH (Call-center Leistung für Hotline) • Deutsche Telekom Technik GmbH (für das Content Delivery Network (CDN) über das der Gemeinschaft die Positivschlüssel zum Download zur Verfügung gestellt werden). Die SAP Deutschland SE & Co. KG hat ihrerseits Unterauftragsverhältnisse mit den folgenden Unternehmen für Dienstleistungen im Rahmen des Supports, der Pflege und Weiterentwicklung für die CWA App, bei denen ein Zugriff auf die				

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Server der CWA App und damit auf die darauf gespeicherten personenbezogenen Daten nicht ausgeschlossen werden kann: • SAP România SRL • SAP Bulgaria Ltd. • SAP Ireland Limited Die Deutsche Telekom Individual Solutions & Products GmbH hat ihrerseits Sub-Unterauftragsverhältnisse mit: • GULP Solutions Services GmbH & Co.KG (Servicedesk für OTC) Die Axivas Deutschland GmbH hat ihrerseits Sub-Unterauftragsverhältnisse mit: • 3 W Phone GmbH (100 Prozent Tochter der Axivas, eingesetzt für Call-Center Leistung für Hotline) • Enghaus AG (Dienstleister für TK-Anlage) Es muss sichergestellt werden, dass auch die Vertragspartner die datenschutzrechtlichen Bestimmungen einhalten.				

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Wahrung der Betroffenenrechte Die Wahrung der Betroffenenrechte könnte gefährdet sein, wenn die Vertragspartner des RKI bei der Wahrung der Betroffenenrechte, beispielsweise den Auskunftspflichten, nicht kooperieren. Dem Benutzer wird durch die Datenschutzhinweise der CWA App transparent gemacht, dass die Datenverarbeitungen durch das Exposure Notification Framework von Google und Apple verantwortet werden.	D-11-2		**Vertragliche Regelungen** ✓ Die Auftragsverarbeitungsverträge mit den Unterauftragnehmern enthalten Regelungen wonach die Vertragspartner zur Kooperation verpflichtet sind. ⚠ Inwieweit Google und Apple diese Daten, entgegen der öffentlich verfügbaren Dokumentationen verarbeiten, entzieht sich der Kontrolle der am Projekt Beteiligten. Betroffene können sich auf deren Verträge mit Google und Apple berufen.	

II. Bedrohungen durch Hacker, Trolle, Stalker und Einzelpersonen (STRIDE)

Das folgende Kapitel erläutert auszugsweise, welche Sicherheitsbedrohungen erkannt wurden und durch welche Maßnahmen den Sicherheitsrisiken durch Designentscheidungen bei der Entwicklung der CWA App begegnet wurde. Schutzziele der IT-Sicherheit sind die Vertraulichkeit, Integrität und Verfügbarkeit. Die Vertraulichkeit schützt, dass nur berechtigte Personen Zugriff auf die Daten haben. Authentizität und Integrität schützen, dass der Empfänger sicher sein kann, dass die Informationen tatsächlich von dem Absender stammen, von dem er glaubt, sie erhalten zu haben (Authentizität, z.B. gesendete E-Mail oder gespeicherte Datei) und die Daten nicht zwischenzeitlich durch einen Dritten verändert wurden (Integrität). Verfügbarkeit schützt, dass jederzeit auf die Daten zugegriffen werden kann.

Das Kapitel ist entsprechend der Threat Modeling Methode STRIDE aufgebaut. Threat Modeling ist eine Methode, durch die potenzielle Bedrohungen, wie z.B. strukturelle Schwachstellen oder das Fehlen geeigneter Schutzmaßnahmen, identifiziert, aufgezählt und die Prioritäten für Abhilfemaßnahmen festgelegt werden können. Das Threat Modeling beantwortet Fragen wie: "Wo bin ich am anfälligsten für Angriffe? Was sind die relevantesten Bedrohungen? Was muss ich tun, um mich gegen diese Bedrohungen zu schützen?“

Eine Methode für das Threat Modeling ist die sogenannte STRIDE Methode. Diese ordnet die Bedrohung sechs verschiedenen Kategorien zu. Dabei steht jeder Buchstabe der Methode für eine Bedrohung:

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

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

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

I – Information Disclosure (Angreifer verursacht Datenleck; Schutzziel: Vertraulichkeit)

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

E – Elevation of Privilege (Angreifer weitet seine Rechte aus; Schutzziel Authentizität)

1. Spoofing (Identität verschleiern)

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Missbräuchliche Verwendung des QR-Codes nach Scan	B-1-1	FifF DSFA S. 77	**Austausch des QR-Codes gegen neue ID** ✓ Um dem zu begegnen, wird von der CWA App unmittelbar nach dem Scannen des QR-Codes der QR-	DSK CWA App, 5.4.2

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Wie bereits oben beschrieben erhält der Benutzer bei der Durchführung des Corona-Tests einen QR-Code, den er mit seinem mobilen Gerät einscannen kann. Nach dem Scan besteht die Möglichkeit, das Testergebnis mit der CWA App abzurufen. Soweit ein positives Testergebnis in der Datenbank mit der in dem QR-Code enthaltenen ID verknüpft ist, kann der Benutzer außerdem seine Positivschlüssel der letzten 2 Wochen der Gemeinschaft zur Verfügung zu stellen. Verliert ein Benutzer den QR-Code nach dem Scannen oder wirft er ihn achtlos weg, besteht die Gefahr, dass dieser Code in die Hände einer anderen Person gelangt und diese den Code missbräuchlich an Stelle des Benutzers verwendet, um dessen Testergebnis zu erfragen oder gegebenenfalls seine Tagesschlüssel wahrheitswidrig als Positivschlüssel auf den CWA Server zu laden.			Code auf dem Verification Server gegen einen sogenannten Registration Token eingetauscht und der QR-Code auf dem Server als verbraucht gekennzeichnet. Mit dem Registration Token authentifiziert sich die CWA App fortan gegenüber dem Server. Damit kann das Testergebnis nunmehr nur noch mit dem mobilen Gerät abgefragt werden, mit dem der QR-Code gescannt wurde. Der QR-Code ist somit für andere Personen nutzlos geworden und kann nicht missbräuchlich verwendet werden.	
Missbrauch des QR-Codes vor dem Scan	B-1-2		**Aufklärung des Benutzers**	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Verliert der Benutzer seinen QR-Code bereits vor dem Scannen durch sein mobiles Endgerät oder lässt er sich nach dem Scannen des Codes Zeit, bevor er eine Netzwerkverbindung ermöglicht, um den QR-Code beim Verifikationsserver zu registrieren, besteht grundsätzlich die Möglichkeit, dass eine andere Person des QR-Codes habhaft werden und diesen an Stelle des Benutzers verwenden kann, bevor der Code auf dem Verifikationsserver durch den Scan als verbraucht gekennzeichnet wurde. Der Angreifer könnte so das Testergebnis des Benutzers erfragen oder für den Fall, dass schon ein positives Testergebnis für den Benutzer vorliegt, seine Tagesschlüssel als die einer vermeintlich infizierten Person auf den Server laden.			⚠ Der Benutzer muss durch entsprechende Aufklärungsmaßnahmen darauf hingewiesen werden, dass er seinen QR-Code unmittelbar nach Empfang scannen und dabei eine Netzwerkverbindung ermöglichen soll.	
Täuschung der Hotline über die Identität Ein Benutzer könnte die eingerichtete Hotline über seine Identität oder das angebliche Vorliegen eines positiven Testergebnisses täuschen. (Quelle: DSK CWA App, 5.4.4)	B-1-3		**Plausibilitätsfragen und Rückruf des Benutzers** ✓ Die Verifikationshotline steht Benutzern der App zur Verfügung, die keinen ihrem positiven Testergebnis zugehörigen QR-Code haben und ihre Positivschlüssel mit der Gemeinschaft teilen wollen. Um die Vortäuschung von falschen positiven Testergebnissen	DSK Hotline, F.2.2.3.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			zu vermeiden und den daraus folgenden falschen Empfehlungen für andere Benutzer, werden dem anrufenden Benutzer zunächst Plausibilitätsfragen gestellt. Wenn der Mitarbeiter der Hotline die Antworten für schlüssig hält und den Anrufer somit als positiv getesteten Benutzer identifiziert, fragt er den Benutzer nach seiner Telefonnummer. Der Mitarbeiter notiert sich die Telefonnummer auf einem Zettel. Danach beendet er das Gespräch, um über eine Weboberfläche die teleTAN zu generieren, die er sodann dem Benutzer durch einen Rückruf telefonisch mitteilt. Durch den Rückruf soll die Authentizität des Benutzers weiter verifiziert und ein Missbrauch ausgeschlossen werden. Der Zettel mit der Rufnummer wird nach einer Stunde durch den Reißwolf datenschutzgerecht zerstört. Dies entspricht auch der Gültigkeitsdauer der teleTAN.	
Authentizität von CWA App und Server Eine Person könnte ihre Identität verschleiern und sich beispielsweise als Benutzer der CWA App oder als Server ausgeben und damit die Kommunikation kompromittieren.	B-1-4	EDSA Anhang SEC-3 und SEC-9	**Signatur der Daten** ✓ Um die Authentizität des Gesprächspartners prüfen zu können, werden die ausgetauschten Daten auf der Serverseite mit einem privaten Schlüssel signiert, während die CWA App mit dem öffentlichen Schlüssel die Unterschrift prüft.	Solution Architecture.md – GitHub

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Vorgetäuschtes Backend Durch DNS Spoofing oder eine Man-in-the-Middle Attacke könnte ein Angreifer die CWA App dazu bringen, statt mit den legitimen Backends mit einem Server seiner Wahl zu kommunizieren. Das betrifft sowohl den CWA Server als auch den Verification Server. Durch das Senden unzulässiger oder gefälschter Inhalte könnte der Angreifer die Funktion der CWA App beeinträchtigen oder gar zum Erliegen bringen. Außerdem kann er so Informationen abgreifen, die nicht für ihn bestimmt sind, und versuchen, beispielsweise über Metadaten der Netzwerkverbindung einen Personenbezug herzustellen.	B-1-5		**HTTP Public Key Pinning** ✓ Als Abwehrmaßnahmen werden neben einer strikten Inputvalidierung TLS Zertifikatvalidierung und -pinning eingesetzt.	DSK CWA App, 5.4.10
	B-1-6	EDSA Anhang SEC-6	**Authentifizierung der CWA App** ✓ Um Identitätsbetrug oder die Erstellung falscher Benutzerprofile zu verhindern, wird die CWA App durch den Server authentifiziert.	
	B-1-7	EDSA Anhang SEC-7	**Authentifizierung des Servers** ✓ Der zentrale Server wird seinerseits durch die CWA App authentifiziert.	DSK CWA Server 5.3.6.
	B-1-8	EDSA Anhang SEC-8	**Schutz der Server vor Replay-Angriffen** ✓ Die Server-Funktionen sind vor Replay-Angriffen geschützt.	
Grundlegende Risiken für Bluetooth Verbindungen	B-1-9		**Kein Pairing mit anderen Geräten** ✓ Um die RPIs zu übertragen, werden nur Bluetooth Advertisement Pakete verwendet, die kein Pairing	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Bei der Nutzung Bluetooth Schnittstelle bestehen grundlegende Risiken. Das Gerät wird je nach Konfiguration, für jedes andere Bluetooth Gerät in der Umgebung sichtbar, wenn die Bluetooth Schnittstelle aktiv ist. Angreifer könnten sich für ein Gerät ausgeben, nach dem das mobile Gerät in seiner Umgebung sucht, weil es bereits zuvor mit diesem Gerät verbunden war. So könnte der Angreifer beispielsweise behaupten, er sei das Headset und könnte dann die Kommunikation, die über das mobile Gerät stattfindet, belauschen.			(aktive Verbindungen) zwischen den Geräten benötigt. Das minimiert die Angriffsoberfläche für Bluetooth Geräte. ✓ Die Mindestanforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) werden eingehalten. Eine Freigabe durch das BSI liegt vor.	
Bluetooth Range Extension Angreifer könnten die eigenen Bluetooth-Signale, mit denen sie ihre Rolling Proximity Identifier (RPI) senden, um ein Vielfaches verstärken und mit weiteren Repeatern weiter verbreiten als mit der ursprünglichen Signalstärke. Dadurch würden Benutzer, ohne eigentlich in der Nähe des Angreifers gewesen zu sein, die RPI des Angreifers empfangen und im Fall einer Infektion falsch informiert werden.	B-1-10		**Erfassung der gesendeten Signalstärke** Derzeit wird der Berechnung für die räumliche Distanz der Kontakte die empfangene Signalstärke zugrunde gelegt. Wenn ein Signal mit unter 50 dB empfangen wird, wird davon ausgegangen, dass die Person unter 2 Metern entfernt war. ⚠ Für die Absendung der gemessenen abgestrahlten Sendeleistung von Bluetooth Nachrichten wird im Exposure Notification Framework (ENF) von Google und Apple ein Byte (aus den 4 verfügbaren „Service	Exposure Notification Bluetooth Specification, S. 4 Advertising Payload Bluetooth Core Specification Version 5.2 | Vol 6, Part A

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			Data“ der Metadaten) vorgesehen, in dem Werte zwischen -127 und 128 dBm kodiert werden. „Class A“ Bluetooth Geräte strahlen mit 100 mW, also 20 dBm. Ein Angreifer könnte diese Daten verfälschen, andererseits können so überdurchschnittlich hohe Signalstärken erkannt und gefiltert werden, so dass solche Kontakte keine Berücksichtigung für die Berechnungen finden und falsche Ergebnisse ausgeschlossen werden.	

2. Tampering (Daten verändern)

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Vortäuschen positiver Testergebnisse mit QR-Code	B-2-1	CCC, Nr. 7 und 8 FifF DSFA S. 83	**Verifikation des positiven Testergebnisses durch TAN** ✓ Nach dem Einscannen des QR-Codes (GUID) des Tests, tauscht die App den QR-Code beim Verifikation Server	Solution Architecture.md – GitHub, Fig. 3

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Ein oder mehrere Angreifer könnten ihre Positivschlüssel auf den Server laden und behaupten, infiziert zu sein, um so das System zu stören.		EDSA, Rn. 41, Anhang PRIV-7, PRIV-8	gegen ein Registration Token ein. Damit kann das Testergebnis nur noch von diesem Mobilgerät aus angefragt werden. ✓ In regelmäßigen Abständen kontaktiert die CWA App den Verification Server, um das Testergebnis zu erfragen. Sobald ein Testergebnis vorliegt, wird es der CWA App mitgeteilt. ✓ Wenn das Testergebnis positiv ist, wird der Benutzer gefragt, ob er seine Positivschlüssel auf den Server laden möchte, um anderen mitzuteilen, dass sie sich angesteckt haben könnten. ✓ Wenn der Benutzer zustimmt, generiert der Verification Server eine TAN, die er gehasht speichert (Hashing of TAN: SHA-256, no salt, no pepper) und an die CWA App, nachdem diese sich wieder mit ihrem Registration Token authentifiziert hat, sendet. ✓ Die TAN wird als Autorisierung im HTTP-Header der POST-Anforderung für den Upload der Diagnoseschlüssel der letzten 2 Wochen auf den CWA Server verwendet. Die TAN ist der Beweis dafür, dass ein positives Testergebnis vorliegt.	Software Design Verification Server DSK CWA App, 5.4.4 Scoping document. md - Github E05.01 EDSA Anhang SEC-1

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			✓ Der CWA Server benutzt die TAN, um den Upload bei dem Verification Server zu verifizieren. Dazu schickt er die TAN zum Verification Server und fragt, ob diese valide ist. Der Verification Server antwortet ggf., dass die TAN valide ist. In diesem Moment wird die TAN verbraucht und damit ungültig. Sie kann kein weiteres Mal verwendet werden. ✓ Der CWA Server erhält die positive Bestätigung vom Verification Server und speichert die Positivschlüssel in der Datenbank. ✓ Falls der Upload fehlschlägt, erhält der Benutzer eine entsprechende Rückmeldung, dass die Daten erneut eingereicht werden müssen.	
Vortäuschen positiver Testergebnisse ohne QR-Code Das Laden der Positivschlüssel eines Benutzers auf den CWA Server soll nur bei Vorliegen eines positiven Testergebnisses möglich sein. Um sicherzustellen, dass keine positiven Testergebnisse vorgetäuscht werden können, muss sich das mobile Endgerät vor dem Laden der Positivschlüssel	B-2-2		**Verifikation des positiven Testergebnisses durch TAN** ✓ Auch in diesem Verfahren wird das positive Testergebnis durch eine TAN verifiziert. ✓ Betroffen sind die folgenden Szenarien:	Software Design Verification Server Scoping document.md - Github E06.04 DSK CWA App, 5.4.4 EDSA Anhang SEC-1

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
auf den CWA Server gegenüber diesem Server ausweisen. Im Standardverfahren (siehe oben unter B-2-1) scannt der Benutzer dazu den QR-Code, den er bei Abgabe seines Tests erhalten hat, mit seinem mobilen Endgerät. Die CWA App tauscht diesen QR-Code beim Verification Server gegen ein Registration Token ein. Damit kann das Testergebnis nur noch von diesem mobilen Endgerät aus angefragt werden. Sobald ein Testergebnis vorliegt, wird es der CWA App mitgeteilt: Nur wenn das Testergebnis positiv ausgefallen ist, kann sich die CWA mit ihrem Registration Token vom Verifikationsserver TANs ausstellen lassen, mit denen die App sich beim Laden der Positivschlüssel gegenüber dem CWA Server ausweisen kann. Aber auch das Verfahren ohne QR-Code muss entsprechend abgesichert sein.			• der Benutzer entscheidet sich dafür, den erhaltenen QR-Code nicht in die CWA App einzulesen, • der QR-Code wurde unwiederbringlich verloren oder ist beschädigt • das Labor ist technisch nicht entsprechend ausgerüstet, um an das System angebunden zu werden ✓ In diesen Fällen kann der Benutzer bei der Verifikationshotline zur Plausibilisierung seines positiven Testergebnisses eine teleTAN erfragen. ✓ Diese teleTAN besteht aus 35 Bit und hat eine Lebensdauer von einer Stunde. ✓ Durch die manuelle Eingabe der teleTAN in die CWA App, erhält der Benutzer von dem Verification Server zunächst einen Registration Token, mit dem sich die CWA App fortan gegenüber dem Server authentifiziert. ✓ Der Benutzer wird nun gefragt, ob er seine Positivschlüssel mit der Gemeinschaft teilen möchte.	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			✓ Bestätigt er dies, erhält er von dem Verification Server eine TAN, mit der er seine Positivschlüssel auf den CWA Server laden kann.	
Vortäuschen falscher Kontakte Die Positivschlüssel infizierter Personen sind auf dem CWA Server für die mobilen Geräte von Millionen Benutzern zugänglich, damit diese bei möglichen Kontakten mit Infizierten von der App entsprechend gewarnt werden können. Mit den in den Positivschlüsseln enthaltenen Daten kann das Exposure Notification Framework (ENF) von Google und Apple nach einem öffentlich bekannten Verfahren die Rolling Proximity Identifier berechnen, die der Infizierte an dem Tag ausgesendet hat, für den der jeweilige Positivschlüssel Gültigkeit hatte, ohne den Infizierte zu kennen. Danach kann das ENF ermitteln, ob das mobile Gerät des Benutzers einen solchen Rolling Proximity Identifier empfangen hat, also ob ein Kontakt zu einem Infizierten stattgefunden hat.	B-2-3		**Verifikation des positiven Testergebnisses durch TAN** Dem wird durch zweierlei Maßnahmen vorgebeugt: ✓ Wenn im Fall eines positiven Corona-Tests der Benutzer die Positivschlüssel der letzten 2 Wochen hochlädt, wird der Positivschlüssel des aktuellen Tages nicht gleich mit hochgeladen. Denn aus dem tagesaktuellen Positivschlüssel können für den Rest des Tages noch neue Rolling Proximity Identifier (RPI) gebildet werden. Stattdessen wird der Positivschlüssel erst hochgeladen, wenn er durch einen neuen Positivschlüssel ersetzt wurde. Es finden also zwei Uploads statt. ✓ Außerdem sind im Rahmen der Berechnungsvorschrift die Zeitintervalle bekannt, in denen die Rolling Proximity Identifier Gültigkeit haben. Findet ein Kontakt mehr als zwei Stunden außerhalb dieses Zeitintervalls statt, findet dieser Kontakt keine Berücksichtigung.	Solution Architecture.md – GitHub DSK CWA App, 5.4.9

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Ein potenzieller Angreifer könnte aus den zum Abruf auf dem CWA Server bereitstehenden Positivschlüsseln ebenfalls die Rolling Proximity Identifier berechnen, die von den infizierten Personen ausgesendet worden sein müssten. Er könnte nun diese Rolling Proximity Identifier in seiner Umgebung per Bluetooth versenden, um bei anderen Personen Kontakte mit Infizierten vorzutäuschen.				
Sabotage der Berechnungsparameter für gefährdende Kontakte Gelänge es einem Angreifer, die von Wissenschaftlern ermittelten und festgelegten Parameter zu verändern, die an die mobilen Endgeräte der Benutzer verteilt und bei der Berechnung der Kontakte der Benutzer mit infizierten Personen verwendet werden, so kann dadurch die Zweckerfüllung der Anwendung grundlegend sabotiert werden.	B-2-4		**Parameter in CWA Server integriert** ✓ Aus diesem Grund sind die Parameter so fest in den Programmcode des CWA Servers integriert, dass zu ihrer Veränderung das Backend in einer streng abgesicherten Build-Umgebung neu aus dem Programmcode erzeugt werden und in die ebenfalls streng abgesicherte produktive Cloud-Umgebung ausgeliefert werden muss. Dabei durchläuft sie einen Testzyklus.	DSK CWA Server, 5.3.4

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Bei Anwendung verfälschter Parameter wird das Ansteckungsrisiko von Kontakten auf den mobilen Endgeräten falsch berechnet. Es kann dann sowohl zur Anzeige von Kontakten mit Infizierten kommen, die für eine Ansteckung nicht relevant sind, als auch zur Unterdrückung solcher Kontakte, die in der Tat relevant wären.				
Verhinderung des Einspielens falscher Datenpakete	B-2-5		**Digitale Signatur** ✓ Um die vom CWA Server verteilten Daten zu autorisieren und das Bereitstellen gefälschter Inhalte durch andere zu verhindern, werden die Datenpakete des CWA Servers digital signiert und vom Client verifiziert.	DSK CWA Server, 5.3.6

3. Repudiation (Abstreiten)

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Leugnen eines Angriffs Ein Angreifer versucht, nach Bekanntwerden und Identifikation des Angreifers die Tat zu leugnen.	B-3-1		✓ Es werden aussagekräftige Logfiles mitgeschrieben und diese im Anlassfall entsprechend ausgewertet. Hierbei werden die Daten stets auf das mindestens notwendige Ausmaß beschränkt.	

4. Information Disclosure (Datenleck)

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Offenlegung vertraulicher Daten Es besteht die Gefahr, dass durch einen Angriff sensible und vertrauliche Informationen der Benutzer beispielsweise durch das Abhören des Traffics offengelegt werden.	B-4-1		✓ Für die Transportwege wird die Methode POST statt der Methode GET verwendet, weil die transportierten Informationen mit der Methode POST in den Body geschrieben werden können (wie z.B. der Registration Token oder die TAN). Mit der Methode GET wären die Informationen Teil der URL und damit sichtbar und würden ggf. in den Komponenten der Infrastruktur geloggt werden.	Software Design Verification Server Solution Architecture.md – GitHub

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Abhören des Bluetooth Verkehrs Ein potenzieller Angreifer kann die Bluetooth-Signale seiner Umgebung empfangen und versuchen, ihre Sender zu identifizieren.	B-4-2		✓ Aus diesem Grund ändern sich die Rolling Proximity Identifier, die von der Apple/Google ENF API ausgesandt werden im Abstand von zehn bis zwanzig Minuten. Die Rolling Proximity Identifier werden aus einer täglich gezogenen Zufallszahl, dem Temporary Exposure Key, errechnet. Es ist aber umgekehrt nicht möglich, den Temporary Exposure Key an Hand der Rolling Proximity Identifier zu ermitteln. Die zusammen mit den Rolling Proximity Identifiern verschickte Sendesignalstärke wird in Abhängigkeit vom jeweiligen Temporary Exposure Key und dem Rolling Proximity Identifier verschlüsselt. Sie kann daher auf Empfängerseite erst entschlüsselt und gelesen werden, wenn die CWA App vom CWA Server den Positivschlüssel des Senders erhält. Dies geschieht nur, nachdem der ursprüngliche Sender ein positives Testergebnis erhalten und sich zum Upload seiner Positivschlüssel auf den Server entschlossen hat.	DSK CWA App, 5.4.7

5. Denial of Service (Mutwillige Überlastung)

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Zugriffsspitzen bewirken einen Ausfall von Servern Durch ein hohes Nutzeraufkommen entstehen Zugriffsspitzen welche die Server überlasten und zu Ausfällen führen.	B-5-1		✓ Um Zugriffspitzen am Backend zu vermeiden werden die Downloads der Positivschlüssel App-seitig gleichmäßig über eine Stunde verteilt (derzeit eine Stunde). Um eine gleichmäßige Verteilung der Serveranfragen zu erreichen und um mit Zugriffsspitzen umzugehen, wird außerdem ein Content Delivery Network (CDN) eingesetzt. Insgesamt wird mit 60 Millionen aktiven Benutzern gerechnet.	Solution Architecture.md – GitHub
Missbrauch der App für einen DoS Angriff Es ist möglich, dass z.B. durch einen DoS-Angriff die Dienste des Servers vorübergehend oder auf unbestimmte Zeit unterbrochen werden. Dies wird in der Regel damit erreicht, dass die angegriffene Ressource mit überflüssigen Anfragen überflutet und das System so überlastet wird.	B-5-2		✓ Um eine Verwendung der App im Rahmen eines Denial of Service Angriffs zu verhindern, sind die Kommunikationspunkte hart kodiert und durch Verifikation mit Zeitstempel versehener digitaler Signaturen abgesichert.	DSK CWA App, 5.4.11
Überlastung der Server durch bewusste Angriffe mit falschen TANs Eine Vielzahl von Aufrufen der TAN-Verifikations-Schnittstelle durch falsche	B-5-3		✓ Wird eine TAN vom Verification Server nicht als gültig anerkannt, wird dieser Umstand vom CWA Server in den Logdateien festgehalten. An Hand einer Häufung solcher Einträge in den Logs kann das Betriebspersonal eine Denial of Service Attacke (s.u.)	DSK CWA Server, 5.3.3

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
TANs kann zu einer erhöhten Last auf den Servern führen und Ausfälle provozieren.			erkennen, die von der Netzwerkschicht nicht erfolgreich abgewehrt werden konnte.	
Überlastung der Server durch Laden ungültiger Daten auf den CWA Server Durch Übermittlung von vielen ungültigen Daten auf den CWA Server und deren Validierung bei der Annahme durch die Schnittstelle können hohe Lasten entstehen, welche zu Ausfällen des CWA Server führen kann.	B-5-4		✓ Das Laden ungültiger Daten auf den CWA Server und darauf basierende Denial of Service Angriffe werden durch strikte Inputvalidierung (inklusive TAN-Überprüfung) und den Einsatz von TLS abgewehrt. Sollte es zu massenhaften Versuchen kommen, den CWA Server durch das Laden von Daten zu überlasten, greifen die Denial of Service-Abwehrmethoden des Security Incident & Event Monitoring der Open Telekom Cloud.	DSK CWA Server, 5.3.5

6. Elevation of Privilege (Ausweiten der Rechte)

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Unbefugter Zugriff auf die zentralen Server Fehlende oder falsche Berechtigungen führen dazu, dass unbefugte Personen Zugriff auf die zentralen Server der CWA haben.	B-6-1	EDSA Anhang SEC-10	✓ Durch ein Berechtigungskonzept und der klaren Trennung der Verantwortlichkeiten des Betriebspersonals ist sichergestellt, dass nur befugte Personen Zugang zu allen auf dem zentralen Server gespeicherten und nicht öffentlich zugänglichen Daten erhalten	DSK Rahmendokument 9.8

G. Abkürzungsverzeichnis

Begriff	Beschreibung
BLE	Bluetooth Low Energy
CCC	Chaos Computer Club
CDN	Content Delivery Network, CDN-Magenta
CDN-Magenta	Content Delivery Network
CWA	Corona-Warn-App
DSFA	Datenschutzfolgenabschätzung
DSGVO	Datenschutzgrundverordnung
DSK	Datenschutzkonzept
EDSA	Europäischer Datenschutzausschuss
ENF	Expositionsbenachrichtigungswerk
FifF	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.
GUID	Globally Unique Identifier

LIS	Laboratory Information System
RKI	Robert Koch Institut
RPI	Rolling-Proximity-Identifier
TAN	Transaktionsnummer
teleTAN	telefonisch bekanntgegebene Transaktionsnummer
TEK	Temporary Exposure Key