Bericht über die Datenschutz-Folgenabschätzung für die Anwendung

Stopp Corona-App des Österreichischen Roten Kreuzes

ÖSTERREICHISCHES ROTES KREUZ

Aus Liebe zum Menschen.

Version 2.0. vom 04.08.2020

AutorInnen[1] dieses Berichts:

Christof Tschohl, Heidi Scheichenbauer, Markus Kastelitz, Walter Hötzendorfer, Jan Hospes, Thiago Eisenberger, Moritz W. Rothmund-Burgwall

Der vorliegende Bericht[2] dient primär der internen Dokumentation des Österreichischen Roten Kreuzes (OeRK) sowie allenfalls zur Vorlage an die österreichische Datenschutzbehörde und das Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (Gesundheitsministerium). Obwohl die Veröffentlichung eines Datenschutz-Folgenabschätzungs-Berichts rechtlich nicht zwingend geboten ist, hat sich das OeRK aus Transparenzgründen dazu entschlossen, den Bericht der Allgemeinheit zugänglich zu machen.

1 Diese Angabe bezieht sich auf die Autorenschaft des vorliegenden Berichts. Die Datenschutz-Folgenabschätzung als solche wurde von einem Team aus VertreterInnen des Roten Kreuzes (Verantwortlicher), Research Institute (Berater) und Accenture (Entwickler der App) durchgeführt. Siehe dazu Kapitel 1.3.

2 Erstellt nach dem Muster von *Kastelitz/Hötzendorfer/Riedl*, Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO. In: Jahnel, D. (Hrsg) Jahrbuch Datenschutzrecht 2017, Neuer Wissenschaftlicher Verlag (NWV), Wien, Graz, 2017, 113–141.

Änderungshistorie

Änderung			Beschreibung der Änderung	Freigabe des Berichts	Stadium
Nr.	Datum	Version			
1	25.03.2020	V 0.9	prä-finale Version für Behörden	Christof Tschohl	draft
2	31.03.2020	V 1.0	Erste finale Version	Christof Tschohl	Final
3	09.04.2020	V 1.1	Finale Version zu Release 1.1	Christof Tschohl	Final
4	22.04.2020	V 1.1.3	Finale Version zu Release 1.1.3	Christof Tschohl	Final
5	12.05.2020	V 1.2	Finale Version zu Release 1.2	Christof Tschohl	Final
6	26.06.2020	P 2.0	Präfinale Version zu Release 2.0	Christof Tschohl	draft
7	04.08.2020	V 2.0	Finale Version zu Release 2.0	Christof Tschohl	final

Vorbemerkung

Die Datenschutz-Folgenabschätzung (DSFA) wurde in einer durch die Corona-Pandemie bedingten kurzen und sehr intensiven Entwicklungsphase ab dem frühesten Entwicklungsstadium durchgeführt und am 24.3.2020 abgeschlossen. Am 9.4.2020, 22.4.2020, 8.5.2020, 12.5.2020 und 26.6.2020) erfolgten jeweils Updates der App (Releases 1.1, 1.1.3, 1.1.4, 1.2).

Seit 26.6.2020 ist mit Release 2.0 eine weitere und verbesserte Version der Stopp Corona-App des Österreichischen Roten Kreuz in den Stores verfügbar. Der automatische digitale Handshake funktioniert nach dem Update nun auf allen Geräten mit den Mobil-Betriebssystemen iOS (Apple) und Android (Google). Die App verwendet dafür die neuen Schnittstellen, die Apple und Google kürzlich zur Verfügung gestellt haben. Österreich gehört damit zu den ersten Ländern in Europa, das über eine voll funktionsfähige App verfügt, die den Vorgaben des „Privacy-Preserving Contact-Tracing“ entspricht und damit eine Unterbrechung von Infektionsketten unter strenger Wahrung der Privatsphäre ermöglicht. Durch die Verwendung der neuen Schnittstellen konnten die Risiken auf das allgemeine, aus der Verwendung von Smartphones resultierende Risiko, reduziert werden. In der Vorbereitung dieser Updates wurde jeweils eine Aktualisierung bzw. Fortsetzung der Datenschutz-Folgenabschätzung durchgeführt. Der vorliegende Bericht dient der konsolidierten Dokumentation der Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO nunmehr erweitert um die Funktionen der Stopp Corona-App Releases 1.1, 1.1.3, 1.2 und 2.0 sowie dem Nachweis des rechtmäßigen Betriebs der Datenanwendung in der aktuellen Version im Sinne der Rechenschaftspflicht des Verantwortlichen gemäß Art 24 DSGVO.

Wie die Stopp Corona-App selbst wird auch der Bericht zur DSFA ständig aktualisiert und erweitert. Der Sachverhalt ist auch im Hinblick auf den Zweck stets neu zu bewerten und neue Erkenntnisse, auch aus dem öffentlichen Diskurs, sind umzusetzen. In dieser Hinsicht ist die DSFA als Prozess zu verstehen, der niemals abgeschlossen ist, solange die Datenanwendung existiert. Dem entsprechend ist auch der vorliegende Bericht als „lebendiges Dokument“ zu sehen, dass ständig aktualisiert wird. Die vorliegende Version stellt die konsolidierte Fassung dar, Versionierungen sind in der obenstehenden Tabelle angeführt. Die finale Freigabe des Berichts zur Ablage als jeweils aktuellste Version der Dokumentation obliegt der Datenschutzbeauftragten des Österreichischen Roten Kreuzes / Generalsekretariat (ÖRK/GS) und wird im Datenschutz-Management-System des Verantwortlichen zur Dokumentation abgelegt. Die Durchführung der Folgenabschätzung zu Release 2.0 wurde am 26.6.2020 abgeschlossen und ein interner Bericht abgelegt. Die Publikation des Berichts erfolgte erst mit einem Monat Verzögerung.

Wien, am 04.08.2020

Inhalt

1 Einleitung und organisatorische/administrative Angaben („Deckblatt“)

1.1 Kurzüberblick geplante Verarbeitung, Ablauf der DSFA

Der Verantwortliche, das Österreichische Rote Kreuz, plant den Einsatz der sogenannten Stopp Corona-App. Diese dient der Sensibilisierung und der Verhinderung der weiteren Verbreitung des COVID-19 Virus in der Bevölkerung. NutzerInnen der App zeichnen dabei Ihre Begegnungen/Intensivkontakte mittels digitalen Handshakes auf, d.h. es wird ein digitales Kontakttagebuch geführt. Meldet sich eine der Person mit einer bestätigten COVID-19 Infektion bzw. aufgrund der Ergebnisse eines selbst auszufüllenden Fragebogens als krank, werden alle in den letzten 3 Tage als kontaktiert gespeicherten Personen informiert.

Der Hintergrund hierzu ist, dass die Inkubationszeit bei COVID-19 im Schnitt bei 5,2 Tagen liegt, man jedoch nur in den letzten Tagen der 5,2 Tage/der Inkubationszeit auch infektiös für andere ist. Erfolgt eine rechtzeitige Information und nachfolgende Selbstisolierung, kann die Kontaktkette unterbrochen werden. Darüber hinaus enthält die App Informationsmaterial zum COVID-19 Virus.

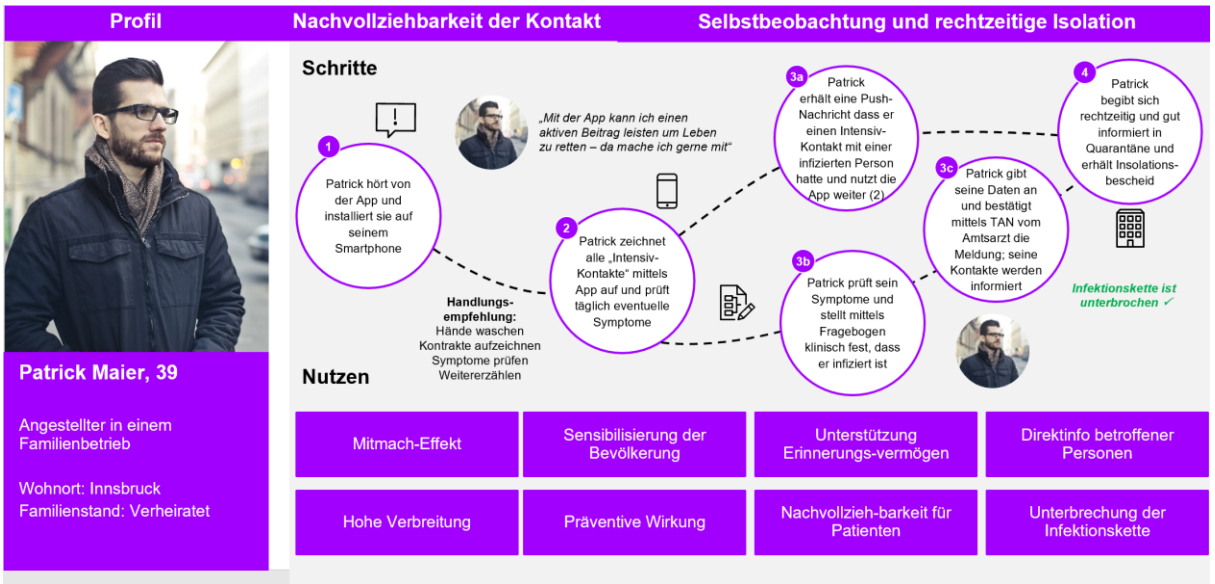


Abbildung 1: Kurzüberblick App-Funktionalität (Quelle: Accenture GmbH)

Gemäß Art 35 DSGVO ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen, wenn die Form der Verarbeitung, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Die verpflichtende Durchführung einer DSFA für die mit der Stopp Corona-App verbundenen Verarbeitungstätigkeiten ergibt sich dabei (bereits) aus Art 35 Abs 3 DSGVO, **der eine verpflichtende DSFA vorsieht, wenn eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO erfolgt**.

Da davon auszugehen ist, dass die App von einer Vielzahl an Nutzern verwendet werden wird, dürfte das Kriterium der umfangreichen Verarbeitung von besonderen Datenkategorien relativ schnell erfüllt sein. Nach Ansicht der Datenschutzbehörde kann bereits eine Aufzeichnung von Gesundheitsdaten in einem Suchtgiftbuch, welches Datensätze von (nur) ca 150 Patienten (Vorname, Nachname, körperlicher Gesundheitszustand, verabreichtes Suchtgift und ausgegebene Menge) und ca 60 Rettungsdienstmitarbeitern (Personalnummer und Unterschrift) eine umfangreiche Verarbeitung von sensiblen Daten darstellen.[3]

Zudem ist darauf hinzuweisen, dass gemäß § 2 Abs 3 der Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) die folgende 2 Kriterien erfüllt sein könnten (und ebenfalls zu einer verpflichtenden DSFA führen):

- Je nach Verbreitungsgrad der App: **Umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art 9 DSGVO** (Z 1)
- **Verarbeitung von Daten schutzbedürftiger betroffener Personen**, wie unmündige Minderjährige, Arbeitnehmer, **Patienten**, psychisch Kranker und Asylwerber (Z 4)

Die Geschäftsleitung hat am 18.03.2020 zur Unterstützung auch formal beschlossen, eine Folgenabschätzung durchzuführen und hat die unter 1.3 Genannten mit deren Durchführung samt Berichtslegung beauftragt. Das Prüfteam hat seine Arbeit am 19.03.2020 aufgenommen und den vorliegenden Bericht erstellt sowie (für die darauffolgenden Releases) Updates eingearbeitet. Wichtig ist festzuhalten, dass die Folgenabschätzung durch das Datenschutz-Team des Verantwortlichen durchgeführt wurde. Die Beiziehung eines externen Beratungsunternehmens bedeutet keine Auslagerung, wohl aber eine wesentliche Hilfestellung insbesondere aufgrund des hohen Zeitdrucks.

Vorauszuschicken ist für die im Folgenden näher erfolgte Analyse der Datenverarbeitung im Rahmen der App-Nutzung, dass außergewöhnliche Umstände, wie eine Pandemie, außergewöhnliche und kreative Lösungen, wie die vorliegende Stopp Corona-App, erfordern. Das Österreichische Rote Kreuz bekennt sich jedoch auch in einer krisenhaften Situation ausdrücklich zur Einhaltung der unionsrechtlichen und innerstaatlichen Rechtsvorschriften insbesondere mit Hinblick auf das Grundrecht auf Datenschutz, den Schutz personenbezogener Daten und die Achtung des Privat- und Familienlebens (§ 1 Datenschutzgesetz, Art 8 EMRK sowie Art 7 und 8 EU-Grundrechtecharta). Anzumerken ist weiters, dass der Verantwortliche zusammen mit dem Entwickler-Team von Beginn an die Anforderungen des Art 25 DSGVO (Datenschutz durch Technikgestaltung und Voreinstellungen) mitberücksichtigt hat. Auch in der letzten Phase der Durchführung der Datenschutz-Folgenabschätzung (DSFA) – im engeren Sinn einer systematischen Prüfung und Dokumentation – wurden noch Anpassungen der App aufgrund von Erkenntnissen im Zuge der DSFA durchgeführt.

Die Einbindung der Fachöffentlichkeit durch grundrechtsaffine Organisationen aus Zivilgesellschaft und Wissenschaft wie epicenter.works, noyb.eu und SBA Research hat wesentlich zu weiteren Verbesserungen der App beigetragen. [4]

[3] Siehe dazu Entscheidung der DSB vom 8.8.2018, DSB-D084.133/0002-DSB/2018.

[4] Siehe Bericht der Technischen und Rechtlichen Analyse der Stopp Corona App des Österreichischen Roten Kreuzes von Epicenter.Works, NOYB und SBA-Research, abrufbar unter https://noyb.eu/sites/default/files/2020-04/bericht_stopp_corona_app_v1.0.pdf (zuletzt abgerufen am 11.05.2020).

1.2 Angaben über den Verantwortlichen gem Art 4 Z 75

Dieser Dienst (**Stopp Corona-App**) wird vom **Österreichischen Roten Kreuz** (Generalsekretariat und Blutspendezentrale für Wien, Niederösterreich und Burgenland, Wiedner Hauptstrasse 32**,** 1040 Wien**,** ZVR-Zahl: 432857691**,** E-Mail: service@roteskreuz.at) als Verantwortlicher im Sinne des geltenden Datenschutzrechts zur Verfügung gestellt.

1.3 Angaben über das DSFA-Projektteam

Die Datenschutz-Folgenabschätzung wurde von einem Team aus VertreterInnen des Roten Kreuzes (Verantwortlicher), Research Institute (Berater) und Accenture (Entwickler der App) durchgeführt.

Aus Datenschutzgründen sind Angaben über die einzelnen beteiligten Personen in der veröffentlichten Version dieses Dokuments nicht enthalten.

1.4 Stellungnahme des/der Datenschutzbeauftragten)

Der Rat des bis 9.4.2020 als Karenzvertretung bestellten externen Datenschutzbeauftragten (DSBA) Ing. Dr. Christof Tschohl und der regulären internen Datenschutzbeauftragten wurde eingeholt und in Folge mehrere Änderungen an den geplanten Verarbeitungstätigkeiten vorgenommen. Die Stellungnahme des/der Datenschutzbeauftragten liegt zur Dokumentation im Datenschutz-Managementsystem des Verantwortlichen.

2 Systematische Beschreibung der geplanten Verarbeitungsvorgänge (Prüfgegenstand)

2.1 Angabe des Zwecks/der Zwecke der Verarbeitung

Die **Stopp Corona-App** soll einen wesentlichen Beitrag zur raschen Unterbrechung von Infektionsketten im Zuge der Corona (offiziell COVID-19 genannt)-Krise leisten und zielt zur Verwirklichung dieser Aufgabe konkret auf die automationsunterstützte **Erfassung von sogenannten Intensivkontakten** ab. Darunter werden Kontakte zwischen natürlichen Personen verstanden, die länger als 15 Minuten dauern und bei denen der räumliche Abstand zwischen den App-Nutzern weniger als 2 Meter beträgt. Zwar empfiehlt die Weltgesundheitsorganisation WHO[6] sogenanntes „Social Distancing", d.h. das Abstandhalten zwischen Personen, um eine potentielle Übertragung des Virus zu unterbinden, Intensivkontakte lassen sich dennoch aktuell nicht immer vermeiden, beinhalten jedoch ein deutlich höheres Infektionsrisiko. Durch die stufenweise Öffnung des Handels seit April 2020 und der Gastronomie/Hotellerie seit Mai 2020 und die weiteren Änderungen im Zuge der COVID-19-LV-Novellen ist es zu einer zunehmenden Mobilität der österreichischen Bevölkerung gekommen, was jedoch auch zu einer Zunahme von möglichen Ansteckungsszenarien führt.

Die Stopp Corona-App bietet die Funktionalität möglicherweise infizierte Personen unmittelbar über eine (mögliche) COVID-19-Infektion eines Intensivkontaktes zu verständigen zu der innerhalb der letzten 3 Tage vor Ausbruch der Erkrankung ein intensiver Kontakt bestanden hat.

---

5 Im Folgenden beziehen sich Angaben von Artikeln und ErwGr ohne nähere Angaben auf die DSGVO.

6 https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public (zuletzt abgerufen am 25.03.2020).

Dadurch wird zur Entlastung des Systems allgemein und insbesondere der behördlichen und medizinischen Ressourcen beigetragen. Durch die nachfolgende freiwillige Selbstisolation und (bei Auftreten von Symptomen) COVID-19 Testung können Infektionsketten unterbrochen werden und eine wesentliche Unterstützung zur Aufrechterhaltung der öffentlichen Gesundheit durch Eindämmung der COVID-19 Pandemie geleistet werden.

Durch die Verwendung der App sollen die Nutzer zudem fundiert über COVID-19 informiert und bei Bedarf entsprechende Handlungsempfehlungen erteilt werden.

Durch entsprechende Sicherheitsvorkehrungen werden Missbrauchsfälle iSv Falschmeldungen über das Vorliegen einer ärztlich attestierten COVID-19 Infektion hintangehalten.

Derzeit erfolgt keine statistische Auswertung der über die Stopp Corona-App erstatteten Meldungen.

2.2 Funktionale Beschreibung der Verarbeitung

Die Stopp Corona-App kann von NutzerInnen auf ihren Smartphones installiert werden. Sie ist über die App-Stores von Google und Apple (bei Android im Google Play Store unter https://play.google.com/store/apps/details?id=at.roteskreuz.stopcorona und im Apple AppStore unter https://apps.apple.com/at/app/apple-store/id1503717224) kostenlos via Download erhältlich. Die App kommuniziert über das Internet mit einem Server, der vom Verantwortlichen betrieben wird. Nachfolgend wird die Beschreibung wiedergegeben, welche die Betroffenen im Rahmen der Datenschutz-Information erhalten. Der finale Text selbst ist letztlich ein Ergebnis aus dem Prozess der Durchführung der DSFA und zielt darauf ab, möglichst hohe Transparenz zu schaffen.

Die App ermöglicht Nutzern den Abruf und Darstellungen folgender Informationen/Funktionen:

- Informationen zum COVID19-Virus (“Content-Services“);
- Services zur Beurteilung von Symptomen (“Content-Services“);
- Services zur Dokumentation seiner menschlichen Kontakte (Kontaktpersonen“) in Zeiten der COVID19-Epidemie (“Log-Buch“) mit den Zielen
    - der raschen Benachrichtigung der Kontaktpersonen sowie
    - Meldung der (möglichen) COVID-19-Erkrankung an den Verantwortlichen zum Zweck der anonymen Information der aktiv hinterlegten infektionsgefährdeten Intensiv-Kontakte
    - Entwarnung von Nutzern, wenn App-Nutzer nach Nutzung des Symptom-Checkers eine Verdachtsmeldung an ihre Kontakte der letzten 54 Stunden geschickt haben, und sich dann herausstellt, dass es ein „falscher Alarm“ war
    - Widerruf einer Krankmeldung wenn App-Nutzer im Zuge der Nutzung der App eine Krankmeldung an ihre Kontakte der letzten 54 Stunden geschickt haben, es sich dabei jedoch um einen „falschen Alarm“ (=eine irrtümliche Meldung) gehandelt hat
- Weiterempfehlung der App an Bekannte und Freunde von App-Nutzern

1. Die Content-Services ermöglichen es dem Nutzer, Informationen zu einer möglichen COVID-19-Erkrankung zu bekommen; die Content-Services sollen die Bewusstseinsbildung beim Nutzer fördern. Die Auswertung der Informationen obliegt dem Nutzer selbst. Ausdrücklich wird darauf hingewiesen, dass die Services nicht die Konsultation eines Arztes zu ersetzen vermögen. Für Fragen zur Krankheit und Therapie wird die Kontaktaufnahme mit einem Arzt empfohlen. Aus der

Anwendung der Content-Services werden keine Schlüsse gezogen und keine Therapieempfehlungen abgegeben

2. Die "Log-Buch"-Funktion ermöglicht es Nutzern, mit Einwilligung der Kontaktperson die laufenden menschlichen Kontakte auf ihrem Endgerät zu dokumentieren und in weiterer Folge über (mögliche) eigene COVID-19-Infektionen zu informieren bzw. ggf. zu entwarnen. Das Einvernehmen wird durch den wechselseitigen Datenaustausch zwischen den Endgeräten der Kontaktpersonen bestätigt. Dies konnte bis zum Release 2.0 entweder durch den manuellen Handshake oder durch den automatischen Handshake erfolgen. Beim manuellen Handshake mussten digitale Handshakes zwischen den Intensiv-Kontakten von beiden Nutzern jeweils einzeln bestätigt werden. Seit dem Release 2.0 besteht nur noch die Funktion des automatischen Handshakes bei dem dies automatisiert erfolgt.

Zwischen Android-Geräten ist standardmäßig der **automatische digitale Handshake** aktiviert, welcher innerhalb der App vom Nutzer deaktiviert werden kann. Dieser wurde bis zum Release 2.0 technisch mithilfe von p2pkit der Uepaa AG (Schweiz) abgewickelt. Ab dem Release 2.0 wird eine von Google und Apple gemeinsam entwickelte Schnittstelle verwendet.

Auf der Ebene des Betriebssystems des Endgeräts der App-User wird dabei der TEK (= temporary exposure key) generiert. Dieser bildet die Identität des App Users für den Tag, die sich alle 24 Stunden ändert. Jeden Tag wird also ein neuer TEK erzeugt. Der TEK ist geheim und wird bei einem Kontakt nicht mit anderen Endgeräten ausgetauscht. Mit einem TEK kann ein RPI berechnet werden – aber nicht umgekehrt.

Der RPI (=rolling proximity identifier) dagegen ist eine ständig wechselnde Kontaktnummer der App, die bei einem Kontakt mit einer anderen Endgeräten mit einer aktivierten App via Bluetooth übertragen wird und am Endgerät der Kontaktperson gespeichert wird. Der RPI ist durch den Bluetooth-Übertragungsweg somit für alle sichtbar. Der RPI, der sich gemeinsam mit der MAC Adresse des BLE (Bluetooth Low Energy) Stack ändert (etwa alle 10 Minuten), wird für den Austausch mit anderen App-NutzerInnen verwendet, damit es niemanden möglich ist, eine App-UserIn über den ganzen Tag hinweg zu verfolgen. Da sich der RPI laufend und synchron zur BLE MAC Adresse ändert, kann kein Bewegungs- oder Kontaktprofil erstellt werden. Es entsteht damit kein höheres Risiko als durch die sonstige Nutzung der Bluetooth-Funktionen des Endgeräts.

Wenn eine Nutzerin/ein Nutzer eine Verdachts- oder Krankmeldung schickt, dann werden die Kontakte der letzten 3 Tage gewarnt. Die konkrete Zeitspanne hängt dynamisch von epidemiologischen Erkenntnissen ab und kann bis zu 14 Tage betragen. Nach dem Kenntnisstand per Juni 2020 werden die Kontakte der letzten 3 Tage informiert. Bei einer Krankmeldung schickt die App den TEK der letzten 3 Tage (nach dem jeweils epidemiologisch definierten Zeitraum) an unseren Server. Von dort holt sich jede App einmal pro Tag die gesamte Liste aller TEKs ab und berechnet damit die RPIs. Durch den Abgleich der berechneten RPIs mit den am Endgerät gespeicherten RPIs können App-User also erkennen, ob sie Kontakt mit einer als krank gemeldeten Person hatten.

Außerdem werden verschlüsselte Metadaten (Associated Encrypted Metadata (AEM)) zum Transport der) für die Protokoll-Versionierung und der Sendeleistung (Tx) für und eine bessere Entfernungsannäherung genutzt. Die zugehörigen verschlüsselten Metadaten wechseln etwa alle 10 Minuten mit der gleichen Geschwindigkeit wie die Rolling Proximity Identifier, um eine drahtlose Verfolgung des Geräts zu verhindern.

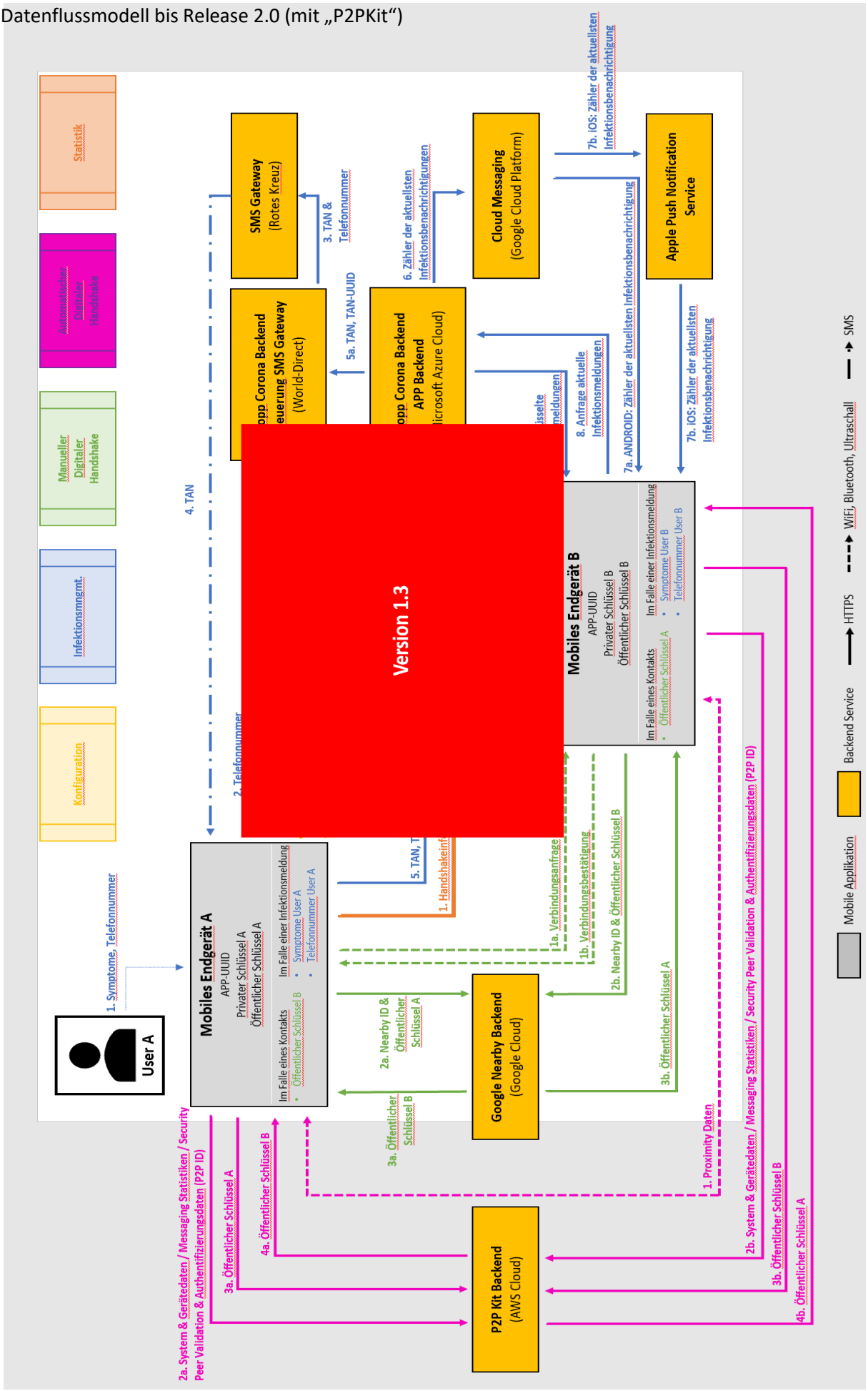
Für die Betätigung des Kommunikationstools und dem damit verbundenen Auslösen des Kommunikationsvorgangs an die Kontaktpersonen ist der Nutzer verantwortlich, der für die App Verantwortliche führt die Benachrichtigung als technischer Verbreiter durch. Dabei kann eine Warnung über eine mögliche COVID-19-Infektion an jene Kontaktpersonen übermittelt werden, mit denen der Nutzer in den vergangenen 3 Tagen in intensiveren Kontakt war und (sofern sich der Verdacht nicht erhärtet), nachfolgend eine Entwarnung übermittelt werden.

3. Weiterempfehlung der App

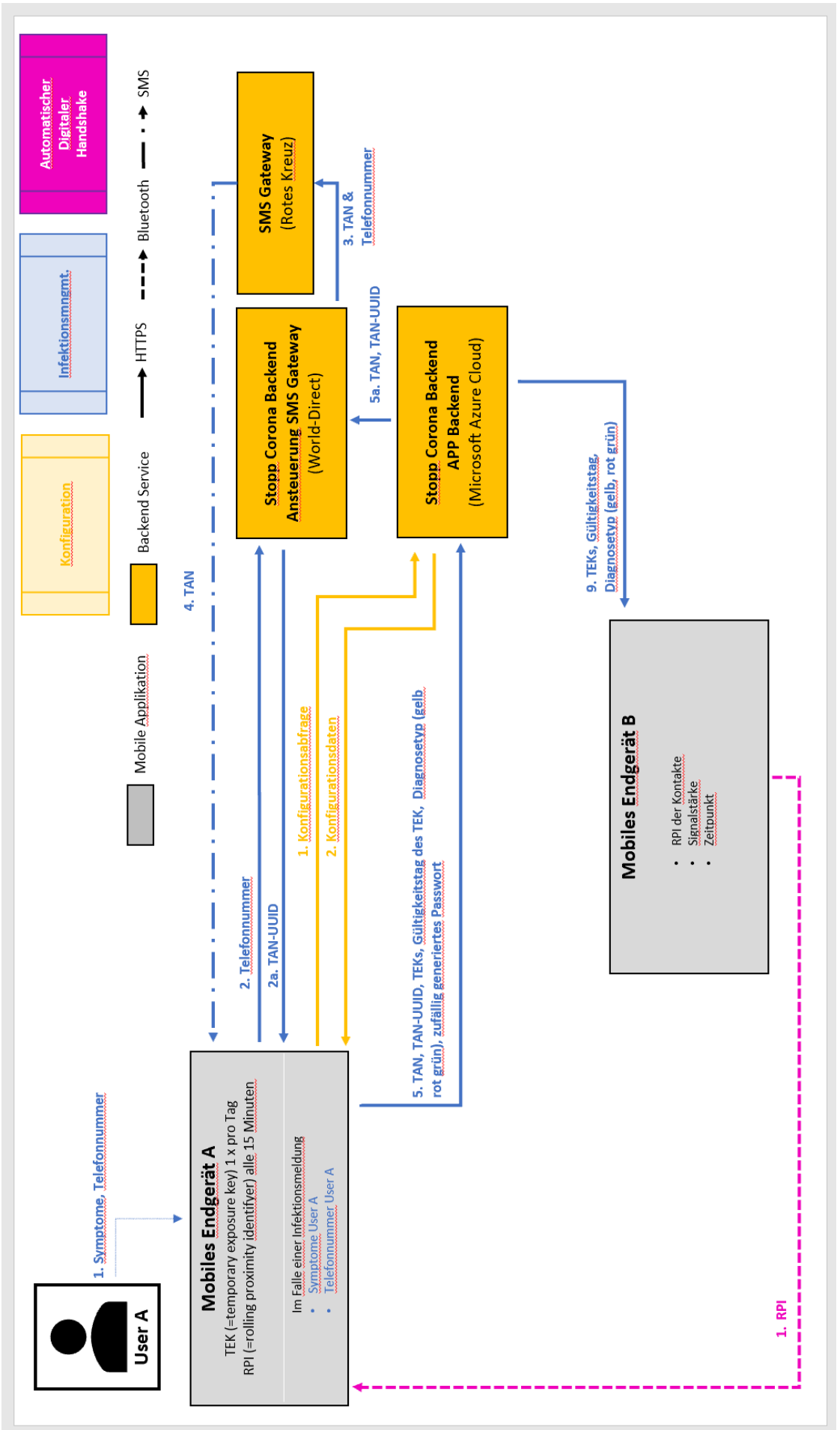
App-Nutzer können die App ihren Freunden oder Bekannten empfehlen. Dies erfolgt dies durch die jeweilige Sharing-Funktion des jeweiligen Betriebssystems. Im Zuge der Empfehlungsabgabe wählen App Nutzer eine Anwendung aus, durch die der Link zur Stopp Corona-App freigegeben wird (E-Mail, Signal, Whatsapp, etc.). Diese Verarbeitung erfolgt ausschließlich durch die App- Nutzer und liegt außerhalb des Einflussbereiches des ÖRK, weshalb das ÖRK nicht die verantwortliche Stelle für diese Verarbeitung ist.

In technischer Hinsicht bietet sich an, die Funktionalität durch ein Datenfluss-Modell darzustellen. Interessant ist dabei zu sehen, wie sich die Datenflüsse geändert haben, nachdem auf die „proximity-tracing-frameworks“ der Hersteller Apple und Google nunmehr mit Relesase 2.0. Aus diesem Grund wird das Datenflussmodell zuerst vor Release 2.0 (noch mit dem Dienst „P2PKit“ für das „proximity tracing“) dargestellt und anschließend das Modell ab Release 2.0.

Datenflussmodell bis Release 2.0 (mit „P2PKit“)



Datenflussmodell Release 2.0 („proximity tracing framework" von Apple/Google)



3 Datenverarbeitung in der App

3.1 Datenerhebung bei Anmeldung in der App

Wie bereits weiter oben gesagt, ist für die Nutzung der App ist vorerst keine Eingabe von personenbezogenen Daten durch die Nutzer notwendig. Die App ist darauf ausgerichtet, dass keinerlei technische Rückschlüsse auf Personen, Standorte oder Geräte möglich sind. Es werden lediglich verschiedene Schlüssel zur Erfassung der Kontakt-Ereignisse erzeugt und ausgetauscht. Konkret werden auf den Endgeräten auf der Ebene des Betriebssystems zwei verschiedene Schlüssel erzeugt:

- TEK (= temporary exposure key) – hiervon gibt es einen pro Tag
- RPI (=rolling proximity identifier) – diese wird aus den TEK abgeleitet und in kurzen Abständen (ca alle 10 Minuten) neu generiert

Die Erzeugung und Verarbeitung dieser Daten erfolgt grundsätzlich bereits auf der Ebene des Betriebssystems des Endgeräts als Teil der sogenannten “Exposure Notification API” . Das Rote Kreuz ist für diese Verarbeitungsvorgänge nur soweit verantwortlich, als die App diese Schnittstelle der Hersteller nutzt. Darüber hinaus besteht eine unmittelbare Rechtsbeziehung zwischen dem Betreiber des Betriebssystems (Apple oder Google) auf Basis der jeweiligen Lizenzbedingungen mit der Nutzerin/dem Nutzer.

Die App erzeugt außerdem pro TEK einen Sicherheitscode, der für 14 Tage am Endgerät gespeichert wird. Dieser Code wird bei einer Verdachts- oder Infektionsmeldung zur technischen Authentifizierung der Meldung an den Server übermittelt.

Die Verarbeitung Ihrer personenbezogenen Daten durch die App erfolgt auf Basis der ausdrücklichen Einwilligung (Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. a DSGVO). Nur wenn diese Einwilligung erteilt wird, um die die Nutzer gleich zu Beginn gefragt werden, können die Nutzer die App auch nutzen.

Nutzer können ihre Einwilligung auch jederzeit widerrufen. Solange noch keine Krankmeldung geschickt wurde, kann dies über die Deinstallation bzw. Löschung der Stopp Corona App erfolgen.

Damit werden keine personenbezogenen Daten des Nutzers mehr verarbeitet. Ein partieller Widerruf ist zudem dadurch möglich, dass der automatische „digitale Handshake” innerhalb der App deaktiviert wird. Die Rechtmäßigkeit der Verarbeitung bis zum Widerruf wird dadurch nicht berührt.

Die folgenden Funktionen werden von der App angeboten:

Installation

Person A installiert App
Generierung Schlüsselpaar
(Privater Schlüssel: PA und Öffentlicher Schlüssel: ÖA)

Person B installiert App
Generierung Schlüsselpaar
(Privater Schlüssel: PB und Generierung Öffentlicher Schlüssel: ÖB)

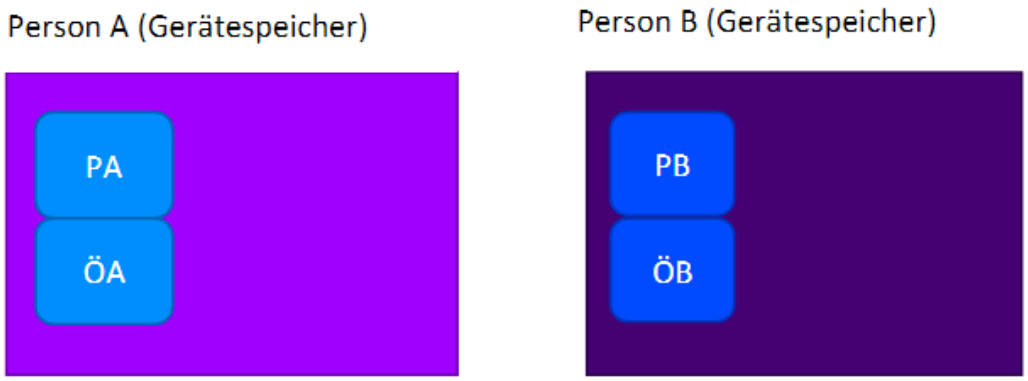


Abbildung: Schlüssel im Gerätespeicher

3.2 Speicherung der Intensiv-Kontakte im Endgerät

Die öffentlichen Schlüssel von anderen Personen, die die App nutzen, mit denen man Kontakt hatte, werden ausschließlich auf dem eigenen Endgerät der App-NutzerInnen gespeichert, nicht jedoch auf dem Server. Die App eröffnet keine Möglichkeit, die öffentlichen Schlüssel der Intensivkontakte aus der App mit Kontaktdaten auf dem Endgerät der Nutzer zu verknüpfen. Falls sich ein Nutzer in seiner eigenen Sphäre ein Notiz macht, die dem Nutzer persönlich eine unmittelbare Verbindung zwischen öffentlichem Schlüssel aus der App mit einer bestimmten Person aus dem Kreis seiner eigenen Kontakte erlaubt, ist dies dem Nutzer zuzurechnen. Auch wenn ein solcher Vorgang nicht unmittelbar in die Verantwortung der Datenanwendung Stopp Corona-App fällt, ist das Bestehen der Möglichkeit selbst in der rechtlichen Beurteilung zu berücksichtigen. Deshalb wird auch der öffentliche Schlüssel als personenbezogen und pseudonymisiert betrachtet und nicht vertreten, es handle sich rechtlich nur um anonyme Daten.

Nach Übereinkunft der 2 Personen (Person A & Person B) mit installierter App die Daten auszutauschen (Initiierung des Handshake), erhalten beide den öffentlichen Schlüssel der anderen Person d.h.

1. Person A und B öffnen die App und initiieren den Handshake
2. Person A erhält von Person B automatisch den **öffentlichen** Schlüssel ÖB
3. Person B erhält von Person A automatisch den **öffentlichen** Schlüssel ÖA

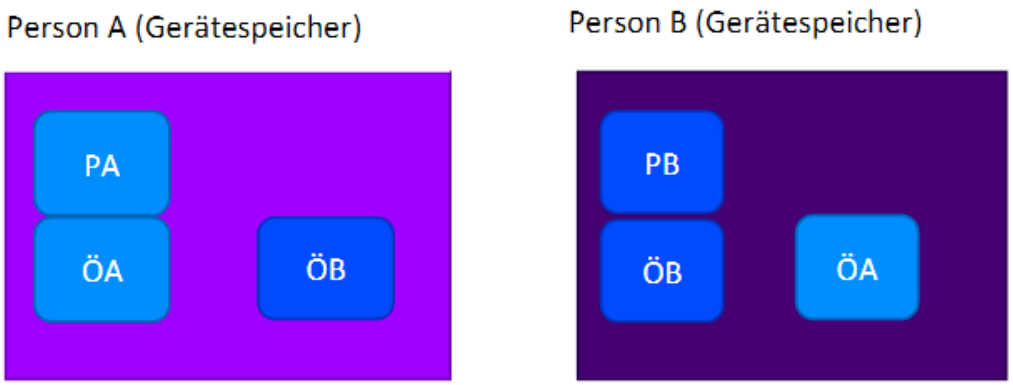
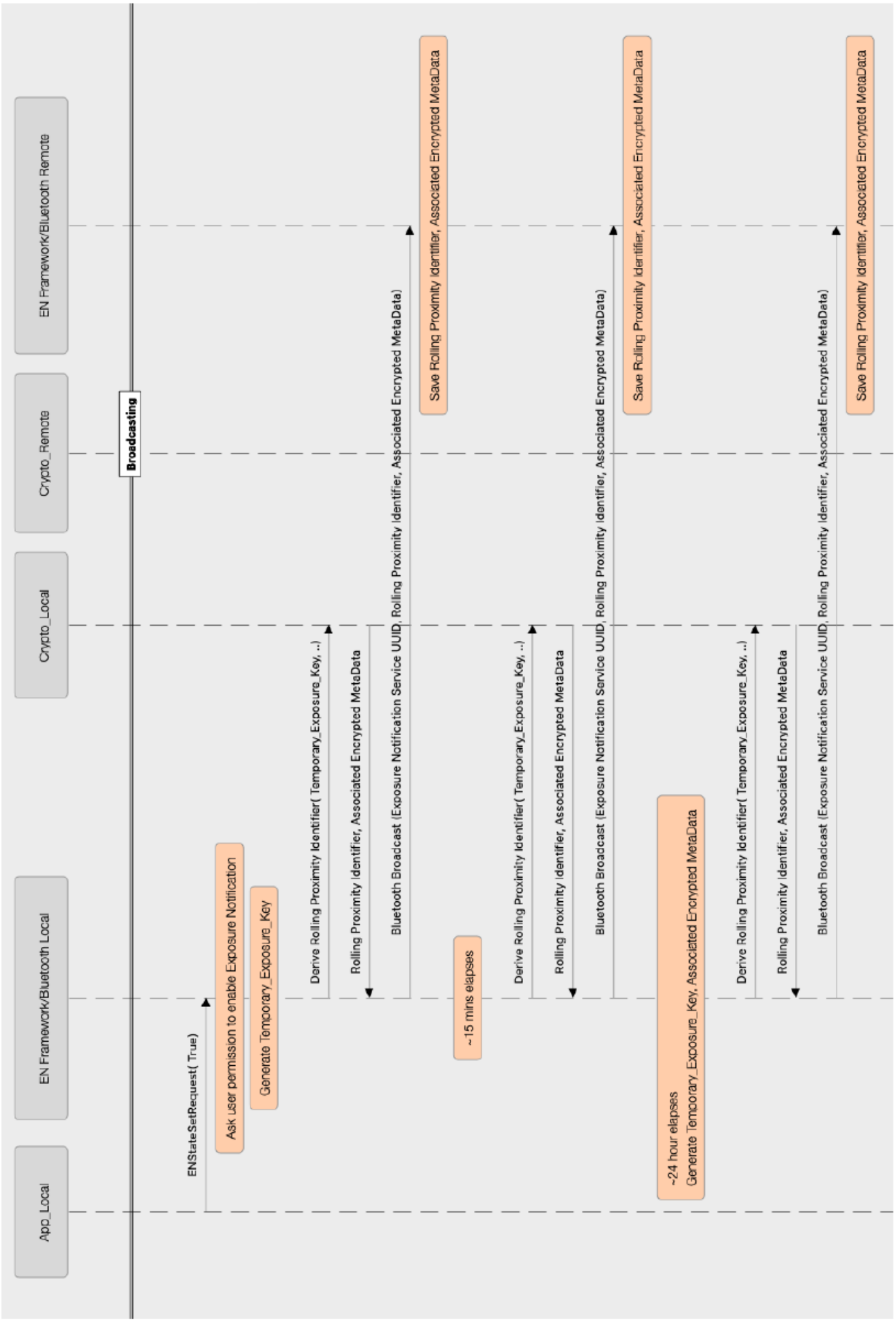


Abbildung: Durchführung Digitaler Handshake

Die Erfassung der Endgeräte in der Umgebung erfolgt mittels Exposure Notification Service - Der Bluetooth-Niedrig-Energie-Dienst zur Erkennung von Gerätenähe von Google/Apple. Der Benutzer muss diese Funktion autorisieren, d.h. die Verwendung von Bluetooth muss durch den Benutzer freigegeben werden.

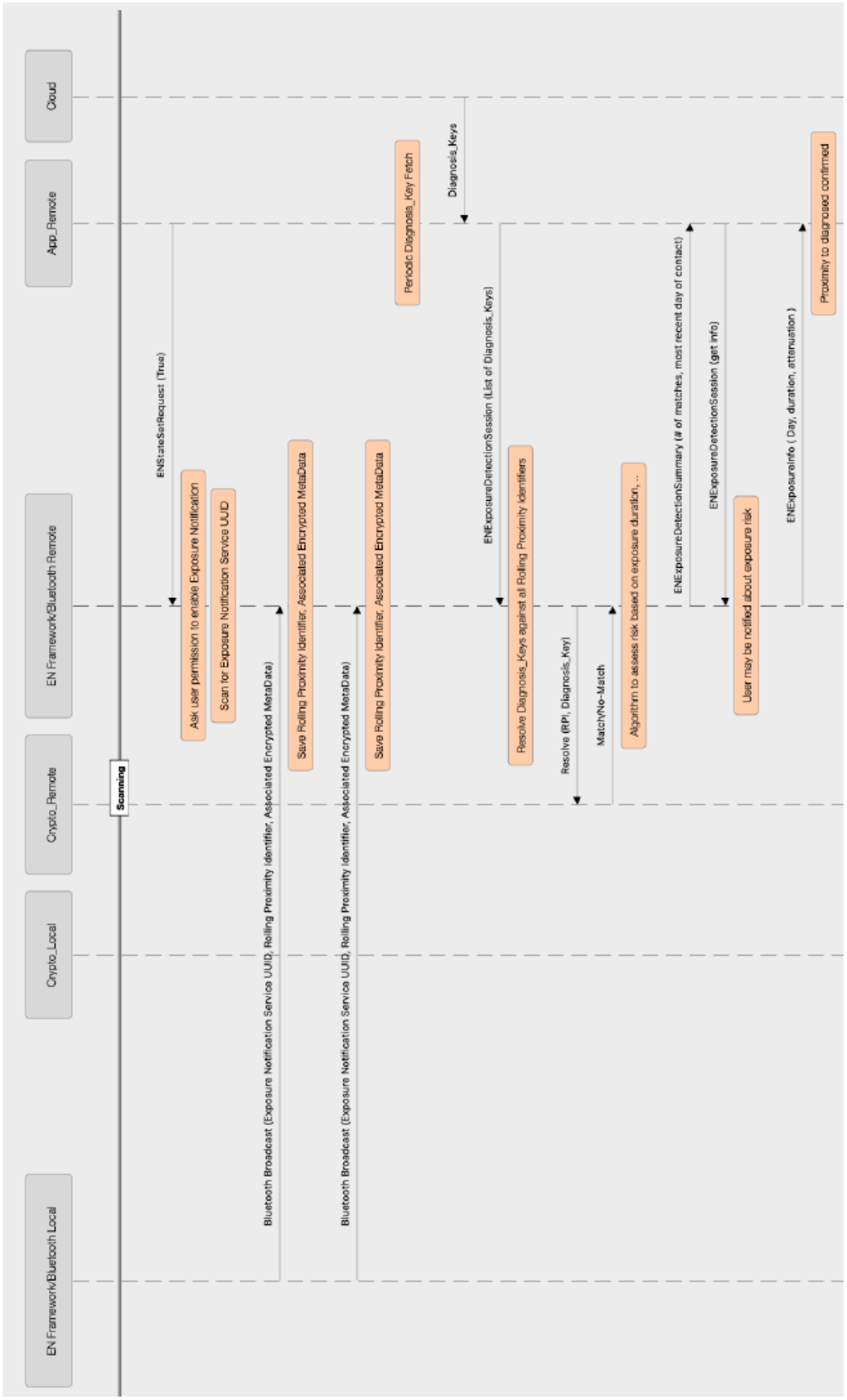
Darstellung Übertragung von Daten zwischen den Endgeräten:[7]

[7] Google/Apple Exposure Notification/ Bluetooth Specification, Preliminary — Subject to Modification and Extension, April 2020, v1.2.


App_Local
EN Framework/Bluetooth Local
Crypto_Local
Crypto_Remote
EN Framework/Bluetooth Remote
Broadcasting
ENStateSetRequest(True)
Ask user permission to enable Exposure Notification
Generate Temporary_Exposure_Key
Derive Rolling Proximity Identifier(Temporary_Exposure_Key, ..)
Rolling Proximity Identifier, Associated Encrypted MetaData
Bluetooth Broadcast (Exposure Notification Service UUID, Rolling Proximity Identifier, Associated Encrypted MetaData)
Save Rolling Proximity Identifier, Associated Encrypted MetaData
~15 mins elapses
Derive Rolling Proximity Identifier(Temporary_Exposure_Key, ..)
Rolling Proximity Identifier, Associated Encrypted MetaData
Bluetooth Broadcast (Exposure Notification Service UUID, Rolling Proximity Identifier, Associated Encrypted MetaData)
Save Rolling Proximity Identifier, Associated Encrypted MetaData
~24 hour elapses
Generate Temporary_Exposure_Key, Associated Encrypted MetaData
Derive Rolling Proximity Identifier(Temporary_Exposure_Key, ..)
Rolling Proximity Identifier, Associated Encrypted MetaData
Bluetooth Broadcast (Exposure Notification Service UUID, Rolling Proximity Identifier, Associated Encrypted MetaData)
Save Rolling Proximity Identifier, Associated Encrypted MetaData

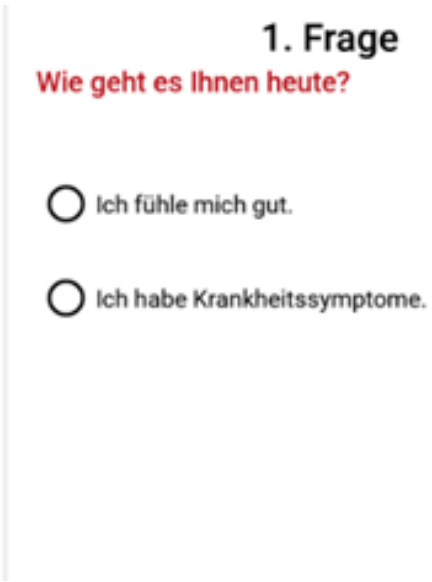
Das folgende Diagramm veranschaulicht den Ablauf und das Verhalten der Geräteabtastung:[8]

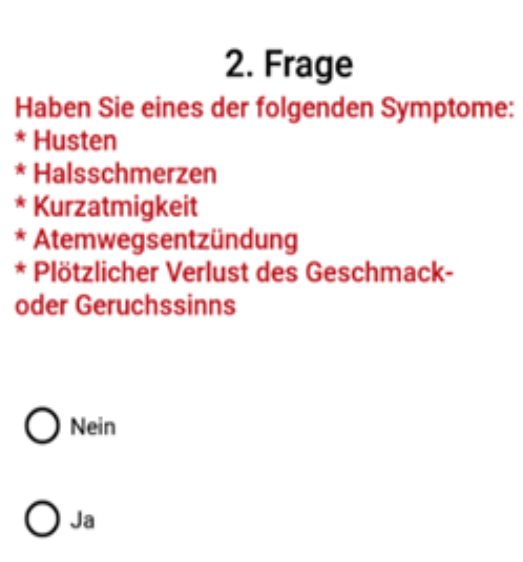
[8] Google/Apple Exposure Notification/ Bluetooth Specification, Preliminary — Subject to Modification and Extension, April 2020, v1.2.

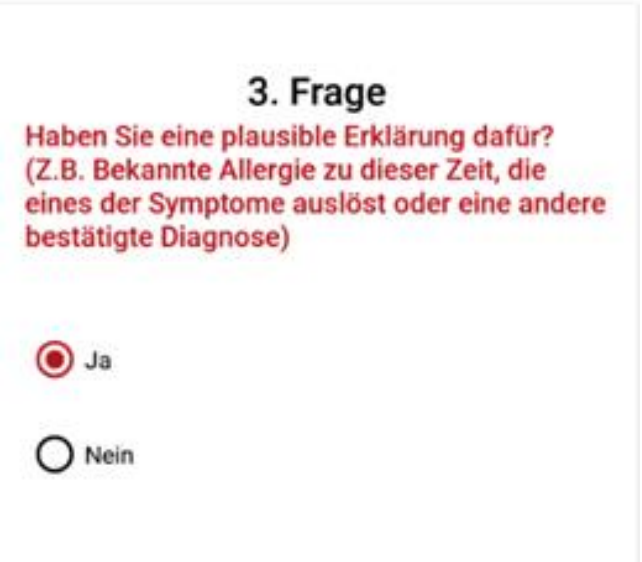

EN Framework/Bluetooth Local
Crypto_Local
Crypto_Remote
EN Framework/Bluetooth Remote
App_Remote
Cloud
Scanning
ENStateSetRequest (True)
Ask user permission to enable Exposure Notification
Scan for Exposure Notification Service UUID
Bluetooth Broadcast (Exposure Notification Service UUID, Rolling Proximity Identifier, Associated Encrypted MetaData)
Save Rolling Proximity Identifier, Associated Encrypted MetaData
Bluetooth Broadcast (Exposure Notification Service UUID, Rolling Proximity Identifier, Associated Encrypted MetaData)
Save Rolling Proximity Identifier, Associated Encrypted MetaData
Periodic Diagnosis_Key Fetch
Diagnosis_Keys
ENExposureDetectionSession (List of Diagnosis_Keys)
Resolve Diagnosis_Keys against all Rolling Proximity Identifiers
Resolve (RPI, Diagnosis_Key)
Match/No-Match
Algorithm to assess risk based on exposure duration, ..
ENExposureDetectionSummary (# of matches, most recent day of contact)
ENExposureDetectionSession (get info)
User may be notified about exposure risk
ENExposureInfo (Day, duration, attenuation)
Proximity to diagnosed confirmed

3.3 Datenverarbeitung betreffend den Symptom-Checker-Fragebogen

Nutzer der App können einen Fragebogen zu möglichen COVID-19 Symptomen ausfüllen.
Beim Ausfüllen des Fragebogens werden dem Nutzer Fragen zu typischen Symptomen einer COVID-19 Erkrankung gestellt. Die Inhalte des Fragebogens wurden (und werden laufend) zwischen dem Österreichischen Roten Kreuz und dem Gesundheitsministerium abgestimmt und medizinisch fachlich validiert. Wenn der Nutzer aufgrund der Ergebnisse des Fragebogens zu dem Ergebnis kommt an COVID-19 erkrankt sein zu können, kann er seine Intensivkontakte der letzten 54 Stunden über seinen Verdacht mittels einer "Verdachtsmeldung" informieren. Die verständigten Nutzer können sich dann selbst zur Sicherheit in Selbstisolation begeben und medizinischen Rat über die weitere Vorgehensweise einholen.
Die auf den Fragebogen gegebenen Antworten werden hier lediglich lokal verarbeitet und nach Beendigung des Fragebogens verworfen. Nur im Fall einer Verdachtsmeldung erfolgt eine vom Nutzer aktiv anzustoßende Verständigung seiner Intensivkontakte über die Verdachtslage.





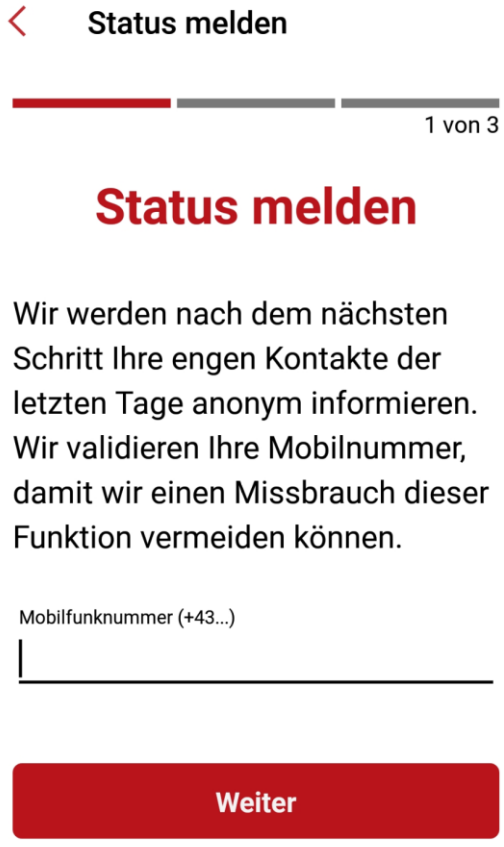


Abbildung, wenn laut Fragebogen kein Verdachtsfall vorliegt:

Abbildung, wenn laut Fragebogen ein Verdachtsfall vorliegt:

Wenn ein Verdachtsfall vorliegt, wird der Nutzer aufgefordert, diesen Verdacht über die App zu melden. Hierfür erhält er ein Formular, in dem die Mobilfunknummer gefordert wird. In weiterer Folge wird dem Nutzer eine TAN übermittelt, diese dient dazu, die Person zu authentifizieren.

Abbildung: Verdachtsmeldung:



Für die Speicherung der Telefonnummer setzen wir den österreichischen Hostingdienst World-Direct eBusiness solutions GmbH, Lassallestrasse 9, 1020 Wien als unseren Auftragsverarbeiter ein. Durch den Wechsel von Microsoft Azure auf einen österreichischen Anbieter wurde der Empfehlung 3.1.2 aus dem Bericht der Technischen und Rechtlichen Analyse der Stopp Corona App des Österreichischen Roten Kreuzes von Epicenter.Works, NOYB und SBA-Research Folge geleistet, wonach die Verwendung alternativer Auftragsverarbeiter, die nicht unter US-Gesetze fallen, empfohlen wurde. Die erhobene Mobilfunknummer geht an das Backend und wird am Server in der Cloud gespeichert und ist somit dem Roten Kreuz zugänglich. Die Telefonnummer wird den Intensivkontakten des Nutzers dabei zu keinem Zeitpunkt preisgegeben. Das Rote Kreuz speichert die Telefonnummer in weiterer Folge für 30 Tage ausschließlich für den Fall, dass sich der konkrete Verdacht auf missbräuchliche und/oder rechtswidrige Nutzung ergibt. Das ist eine erforderliche Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, die durch Art 6 Abs 1 lit f sowie Art 9 Abs 2 lit f DSGVO gerechtfertigt ist.

Abgesichert ist dies durch eine entsprechende technisch-organisatorische Gestaltung. Die Daten liegen zwar auf dem Server, sind dort aber asymmetrisch verschlüsselt, wobei der private Schlüssel im „Tresor" des Datenschutzbeauftragten aufbewahrt wird, wo nur ein sehr enger Personenkreis (der Datenschutzbeauftragte und dessen Vertreter entsprechend Vertretungsregelungen) Zugang haben. Dieser stellt sicher, dass tatsächlich nur für den beschriebenen Zweck auf die Telefonnummern

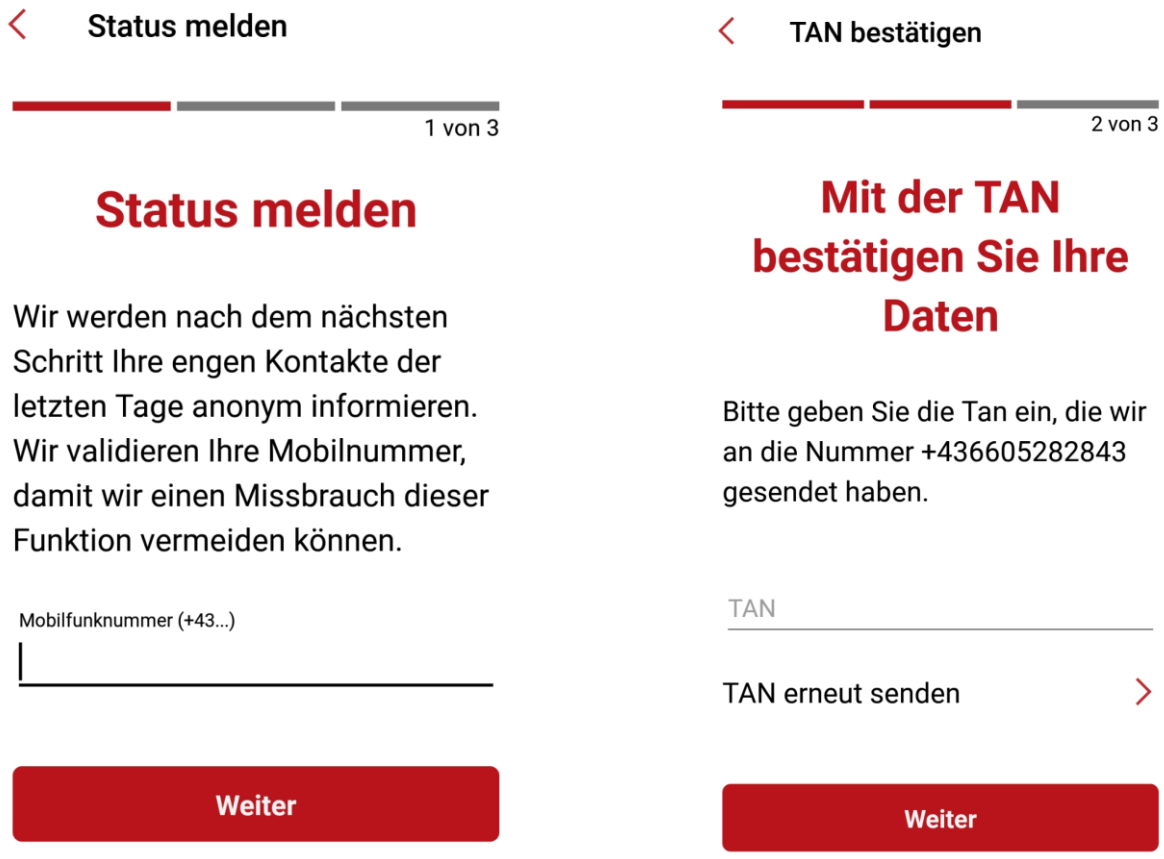
zugegriffen werden kann und würde in diesem Fall praktisch „kommissarischen Rechtsschutz" für den Betroffenen ausüben.

3.4 Daten über Krankmeldung

Zu einer Krankmeldung wird eine Person dann aufgefordert, wenn diese einen Befund eines Arztes betreffend eine aktive COVID-19-Erkrankung erhalten hat.

In diesen Fällen wird der Nutzer aufgefordert, sich über die App als krank zu melden. Hierfür erhält er ein Formular, in dem die Mobilfunknummer gefordert wird. In weiterer Folge wird dem Nutzer eine TAN übermittelt, diese dient dazu, die Person zu authentifizieren.

Abbildung: Krankmeldung:



Auch hier wird für die Speicherung der Telefonnummer der österreichische Hostingdienst World-Direct eBusiness solutions GmbH, Lassallestrasse 9, 1020 Wien als unser Auftragsverarbeiter eingesetzt. Durch den Wechsel von Microsoft Azure auf einen österreichischen Anbieter wurde der Empfehlung 3.1.2 aus dem Bericht der Technischen und Rechtlichen Analyse der Stopp Corona App des Österreichischen Roten Kreuzes von Epicenter.Works, NOYB und SBA-Research Folge geleistet, wonach die Verwendung alternativer Auftragsverarbeiter, die nicht unter US-Gesetze fallen, empfohlen wurde. Die erhobene Mobilfunknummer geht an das Backend und wird am Server in der Cloud gespeichert und ist somit dem Roten Kreuz zugänglich. Die Telefonnummer wird den Intensivkontakten des Nutzers dabei zu keinem Zeitpunkt preisgegeben. Das Rote Kreuz speichert die Telefonnummer in weiterer Folge für 30 Tage ausschließlich für den Fall, dass sich der konkrete Verdacht auf missbräuchliche und/oder rechtswidrige Nutzung ergibt. Das ist eine erforderliche Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, die durch Art 6 Abs 1 lit f sowie Art 9 Abs 2 lit f DSGVO gerechtfertigt ist.

Abgesichert ist dies durch eine entsprechende technisch-organisatorische Gestaltung. Die Daten liegen zwar auf dem Server, sind dort aber asymmetrisch verschlüsselt, wobei der private Schlüssel im „Tresor" des Datenschutzbeauftragten aufbewahrt wird, wo nur ein sehr enger Personenkreis (der Datenschutzbeauftragte und Vertretungsregeln) Zugang haben. Dieser stellt sicher, dass tatsächlich nur für den beschriebenen Zweck auf die Telefonnummern zugegriffen werden kann und würde in diesem Fall praktisch „kommissarischen Rechtsschutz" für den Betroffenen ausüben.

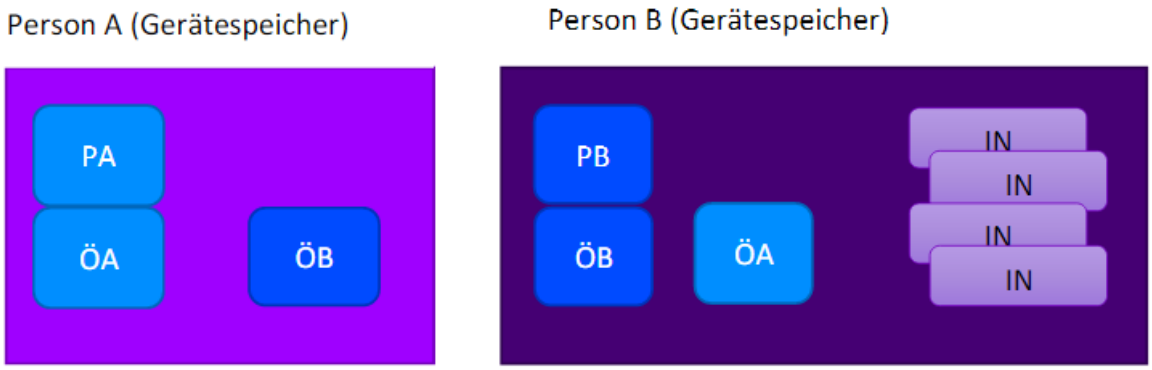
3.4.1 Übertragung einer Infektionsnachricht

Die Meldung einer Erkrankung bzw. eine Verdachtsmeldung führt zu einer Infektionsnachricht (IN), welche mit den öffentlichen Schlüsseln der Kontaktpersonen verschlüsselt wird.

Beispiel: Person A meldet eine Erkrankung/einen Verdacht und hatte zuvor Kontakt (Handshake) mit Person B. D.h. der öffentliche Schlüssel von Person B (ÖB) befindet sich im Gerätespeicher von Person A.

1. Person A verschlüsselt eine Infektionsnachricht (IN) mit dem **öffentlichen** Schlüssel der Person B (ÖB). Die verschlüsselte Nachricht wird im Backend gespeichert.

2. Die App von Person B holt sich die aktuellen Infektionsnachrichten aus dem Backend und versucht, diese mit dem privaten Schlüssel PB zu entschlüsseln.



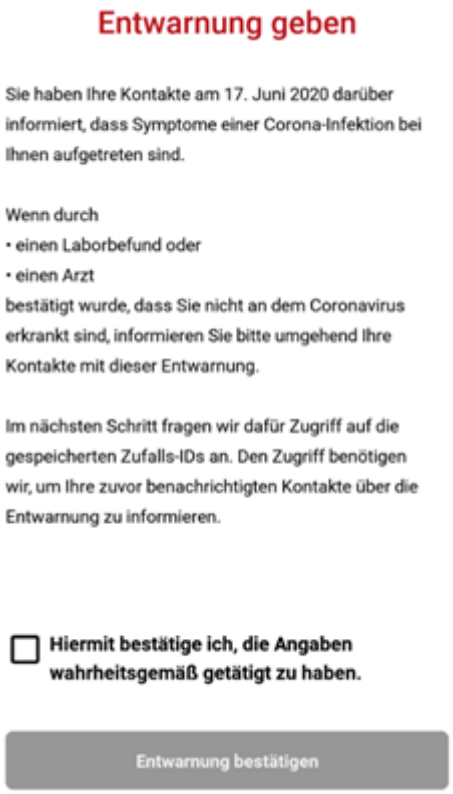
3. Der App der Person B gelingt die Entschlüsselung einer Infektionsmeldung mit Schlüssel PB. Hinweis: Nur mit dem privaten Schlüssel PB ist eine Entschlüsselung der Nachricht, welche mit ÖB verschlüsselt wurde, möglich.
   Die App von Person B hat nun die Information, dass in der vergangenen Kontaktkette **irgendeine Person** einen Verdachtsfall/Erkrankungsfall gemeldet hat. Es wird das Datum und die Uhrzeit stundengenau angegeben. Bis auf die erfolgreich entschlüsselte Nachricht, werden alle empfangenen Infektionsmeldungen, welche nicht entschlüsselt werden können, nach dem Vorgang verworfen.

   Hinweis: Es werden weder der öffentliche noch der private Schlüssel an das Stopp Corona Backend übertragen. Damit ist keine Personenbindung im Stopp Corona Backend an die Schlüssel möglich, und es wird eine größtmögliche Datensparsamkeit gewahrt.

3.4.2 Daten die bei einer Entwarnung verarbeitet werden (wenn sich der Verdacht nicht erhärtet)

Wenn ein App-Nutzer nach Nutzung des Symptom-Checkers eine Verdachtsmeldung an seine Kontakte der letzten 54 Stunden geschickt hat und sich dann herausstellt, dass es sich dabei um einen „falschen Alarm“ gehandelt hat, weil z.B. ein COVID-19-Test ergeben hat, dass keine COVID-19-Infektion vorliegt, kann die Funktion „Entwarnung“ genutzt werden. Das führt dazu, dass die zuvor benachrichtigen Kontakte eine Nachricht mit dem Entwarnungs-Status erhalten.

Abbildung: Entwarnung:



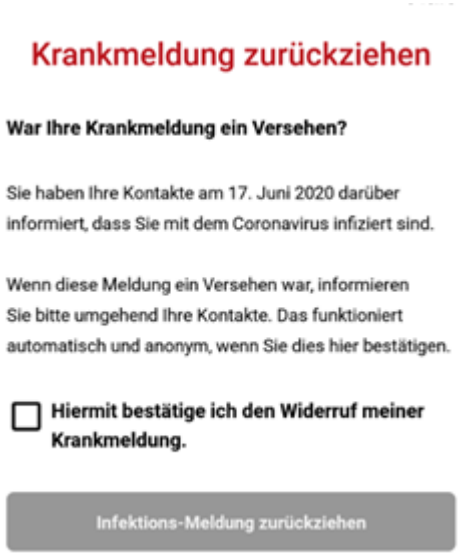
3.4.3 Widerruf einer Krankmeldung

Hat der Nutzer eine Krankmeldung an seine Kontakte der letzten 54 Stunden geschickt, es sich dabei jedoch um einen „falschen Alarm“ (=eine irrtümliche Meldung) gehandelt hat, kann er die Funktion „Widerruf der Krankmeldung“ nutzen. Das führt dazu, dass die zuvor von ihm benachrichtigen Kontakte eine Nachricht mit dem Widerruf seiner Krankmeldung erhalten.

In diesem Fall muss der Nutzer vor dem Abschicken der Meldung seine Telefonnummer angeben. Dadurch wollen wir uns vergewissern, dass kein Missbrauch betrieben wird. Zur Sicherstellung, dass nicht eine beliebige Nummer eingegeben wird, wird dem Nutzer dann eine TAN aufs Handy geschickt, die er zum Fortfahren ins Meldeformular eingeben muss.

Die TAN und die Telefonnummer gehen über das SMS Gateway von uns und dann an den Server. Die Telefonnummer wird nur am Server von World-Direct gespeichert. Für die weiteren Umstände und die rechtliche Beurteilung der Speicherung der Telefonnummer ist auf Punkt 5.4 zu verweisen.

Abbildung Widerruf der Krankmeldung:



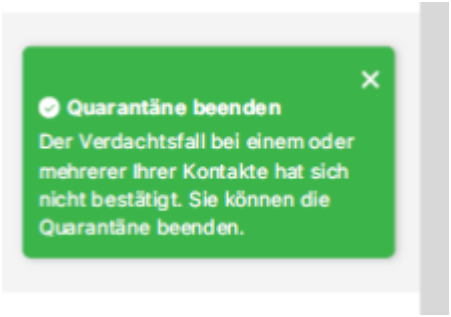
3.5 Näheres zur Benachrichtigung kontaktierter Personen

Die Information darüber, mit welchen anderen IDs man in Kontakt war, ist ausschließlich am Endgerät der App-NutzerInnen gespeichert. Eine Übertragung dieser Informationen in die Cloud findet nicht statt.

Meldet sich eine Person als (möglicherweise) krank, wird über das Backend in der Cloud eine diesbezügliche Information an die Apps **aller** App-NutzerInnen versendet. Diese Information ist aber nur für die Apps von Personen zu entschlüsseln, die mit der als (möglicherweise) krank gemeldeten Person Kontakt hatten. Diese Personen erhalten dann eine Nachricht, dass jemand in ihrem Umfeld (möglicherweise) erkrankt ist. Es wird ihnen jedoch nicht mitgeteilt, wer das ist. Über die Eingrenzung des Kontaktzeitraums können die so Verständigten die Verbindung seit dem Release 2.0 möglicherweise aus ihrer Erinnerung nicht mehr herstellen, da protokollierte Begegnungen mit anderen Mobiltelefonen nunmehr nicht mehr angezeigt werden.

Abbildung: Erfolgte Verständigung über Krank- und Verdachtsmeldungen:

Abbildung: Entwarnung nach erfolgter Verständigung über Verdachtsmeldungen:



4 Ausführungen zur technischen Kommunikation zwischen den Endgeräten (Smartphones)

4.1 Digitaler Handshake:

Der RPI (=rolling proximity identifier) ist eine ständig wechselnde Kontaktnummer der App, die bei einem Kontakt mit anderen Endgeräten mit einer aktivierten App via Bluetooth übertragen wird und am Endgerät der Kontaktperson gespeichert wird. Der RPI ist durch den Bluetooth-Übertragungsweg somit für alle sichtbar. Der RPI, der sich gemeinsam mit der MAC Adresse des BLE (Bluetooth Low Energy) Stack ändert (etwa alle 10 Minuten), wird für den Austausch mit anderen App-NutzerInnen verwendet

4.2 Berechtigungen der App

Die App kann auf Folgendes zugreifen:

- receive data from Internet (Daten aus dem Internet abrufen)
- view network connections (Netzwerkverbindungen ansehen)
- full network access (voller Netzwerkzugriff)
- run at startup (App ausführen beim Start)
- prevent device from sleeping (Aktivierung des Schlafmodus verhindern)

Die App verwendet zudem das Mikrofon und Bluetooth, um andere Handys in der Nähe des Nutzers orten zu können. Dies ist zur Erbringung der App-Funktionalitäten (Kontakttagebuch) erforderlich.

4.3 Systemübersicht:

Die technische Architektur der Stopp Corona-App besteht in Kern aus den folgenden Komponenten:

- Mobile Applikation für iOS und Android
- Azure Cloud als Backend für die Apps und als Entwicklungssystem
- Google Play Store und Apple Store zur Verteilung der mobilen Applikationen an die Endanwender
- SMS Gateway des Roten Kreuzes

Die mobile Applikation wird auf den Geräten (iOS oder Android Betriebssystem) der Endanwender installiert und ausgeführt. Die Komponenten der App kommunizieren via HTTPS (sicheres Hypertext-Übertragungsprotokoll) mit dem Hintergrundsystem (Backend). Das Backend wird in der Azure Cloud gehostet und beinhaltet den Applikationsserver und die Datenbank (Azure Cosmos DB). Im Backend verarbeiten Microservices die Anfragen und nutzen die Datenbank zur Speicherung der übertragenen Daten.
Für die Nutzung der App ist vorerst keine Eingabe von personenbezogenen Daten notwendig. Auf dem Endgerät werden auf der Ebene des Betriebssystems eindeutige, zufällige Zahlenketten („Zufalls-IDs“) generiert, die von der App genutzt und bei einer Infektions- oder Verdachtsmeldung an unseren Server übermittelt werden.

Konkret werden auf dem Endgerät auf der Ebene des Betriebssystems zwei verschiedene Zahlenketten erzeugt:

1. TEK (= temporary exposure key) – hiervon gibt es einen pro Tag
2. RPI (=rolling proximity identifier) – diese wird aus den TEK abgeleitet und regelmäßig in kurzen Abständen neu generiert

Solange keine Verdachts- oder Infektionsmeldung abgeben wird, handelt es sich in beiden Fällen um anonyme Daten. Im Falle einer Verdachts- oder Infektionsmeldung werden die TEK durch deren Übermittlung an das Backend zu sogenannten pseudonymen Daten.

4.3.1 Assets auf welche die Verarbeitung angewiesen ist

Basierend auf dem Strukturbild „Systemkontext Stopp Corona" in Systemübersicht werden die Assets gegliedert.

1. Mobiles Endgerät

Unterstützte Betriebssysteme:

- Android Version 6.0 oder höher
- iOS Version 13.5 oder höher

Das Schlüsselpaar (privater & öffentlicher Schlüssel) werden im KeyStore des Gerätes gespeichert.

Folgende Daten werden lokal in der Applikations-Sandbox im Gerätespeicher des Mobilgerätes abgelegt:

TEK (= temporary exposure key)

RPI (=rolling proximity identifier)

- Öffentlicher Schlüssel von anderen App Nutzern mit letztem Kontaktzeitpunkt (sofern räumlicher Kontakt stattgefunden hat und ein Handshake durchgeführt wurde)
- Gesundheitsstatus (Verdachtsmeldung oder Infektionsmeldung)
- Konfigurationsdaten ()

Der KeyStore verhindert das Auslesen des privaten Schlüssels. Er werden nur adäquate kryptografische Funktionen mit dem privaten Schlüssel (z.B. Entschlüsseln einer Nachricht, Signieren einer Nachricht) ermöglicht.
Die Kernel-Level Applikationssandbox ermöglicht durch die Zuteilung einer eindeutigen Applikations-ID eine robuste Trennung von Prozessen und dadurch einen bewährten und prüffähigen Schutz vor unautorisiertem Datenzugriff. Die Applikationssandbox der führenden mobilen Betriebssysteme Android und iOS wird regelmäßig von den Herstellern auf potenzielle Sicherheitslücken geprüft und, falls vorhanden, werden diese im Rahmen von Updates geschlossen. Die Daten der "Stopp Corona" App werden in der Applikationssandbox gespeichert und sind gegen Zugriffe durch das Betriebssystem oder andere Applikationen geschützt.

2. Backend

Sämtliche Hardware-Instanzen für das Backend werden vom Cloud Provider im Rahmen eines Platform-as-a-Service Modell bereitgestellt. Das Backend besteht im Wesentlichen aus den folgenden Komponenten:

- **Azure Front Door** dient als zentraler Einstiegspunkt und umfasst eine Web Application Firewall sowie DDoS Protection – alle übrigen Assets liegen hinter der Azure Front Door
- **API Management** zur konsistenten Erstellung von API-Gateways für die Überprüfung von API-Schlüsseln, JWT-Tokens, Zertifikaten etc.
- **Azure Functions** zur ereignisgesteuerten serverlosen Durchführung von Prozessen (e.g. TAN Generierung, TAN Validierung, etc.)
- **Web Applikation** (Java, Spring) welche die Schnittstellen für die App bereitstellt (z.B. Abfrage der Infektionsmeldungen)
- **Azure Cosmos Datenbank** – vollständig verwalteter Datenbankdienst

Folgende Daten werden verschlüsselt in der Datenbank gespeichert:

- App-UUID und Anzahl an digitalen Handshakes dieser UUID
- TAN (im Fall der Meldung einer Erkrankung bis Infektionsmeldung durchgeführt wurde)
- Telefonnummer (sofern Infektionsmeldung durchgeführt wurde)
- Meldungstyp (bestätigte Infektion/Verdachtsmeldung/Entwarnung)
- Verschlüsselte Infektionsnachricht
- Konfigurationsdaten

Hinweis: Die Speicherung der Telefonnummer erfolgt, um Missbrauch vorzubeugen und ist auf 30 Tage beschränkt.

Das produktive Backend besitzt Schnittstellen (via HTTPS) zu den folgenden Systemen:

- SMS-Gateway ÖRK

3. Statistikauswertungen

Seit der Stopp Corona App Version 1.1.3 vom 22.4.2020 werden keine Daten für Statistikzwecke erhoben. Für spätere Versionen sind statistische Auswertungen nach folgenden Maßgaben geplant. Zur Auswertung von aggregierten digitalen Handshakes und Infektionsmeldungen wird ein Analytical Datastore auf Basis DWH implementiert.

Daten:

- Aggregierte Kontakt & Infektionsmeldungen

Für die Statistikauswertungen ist ein Staging-Konzept vorhanden.

4. SMS Gateway

Das SMS Gateway ermöglicht die Versendung von TANs über das GSM Netzwerk mittels SMS Protokoll. Die Implementierung & Wartung der Hard- und Software, sowie die für den Durchführung notwendigen Telekomdienste (Abonnements, SIM Karten, etc.) obliegt dem Verantwortungsbereich des Österreichischen Roten Kreuz.

Die durch das SMS Gateway verarbeiteten Daten bestehen aus:

- Telefonnummer
- TAN

5. App Stores

Information: Um die Verbreitung von Falschinformation bzgl. der Corona-Krise einzudämmen, haben sowohl Apple als auch Google ihre offiziellen Kriterien zur Aufnahme von mobilen Applikationen in ihre jeweiligen App Stores aktualisiert. Mobile Applikationen deren Hauptfunktionen mit COVID-19 verbunden sind, werden nur noch von anerkannten Institutionen wie zum Beispiel Regierungsbehörden, Gesundheits-NGOs, Firmen aus dem Gesundheitsbereich oder medizinischen bzw. Bildungsinstitutionen akzeptiert.

Google PlayStore
Eine detaillierte Auflistung der sicherheitsrelevanten Kriterien für die Aufnahme einer mobilen Applikation zur Distribution via Google PlayStore kann unter folgender URL gefunden werden: https://play.google.com/about/developer-content-policy/

Apple App Store
Eine detaillierte Auflistung der sicherheitsrelevanten Kriterien für die Aufnahme einer mobilen Applikation zur Distribution via Apple App Store kann unter folgender URL gefunden werden: https://developer.apple.com/app-store/review/guidelines/#safety

6. Entwicklungsumgebung

Die Entwicklungsumgebung besteht aus den folgenden Tools:

- Ticketsystem: JIRA
- Versionsmanagement: Azure DevOps
- Configuration Management: Azure DevOps
- Change Management: JIRA
- IDE: Visual Studio, Android Studio, Xcode, IntelliJ

7. Testumgebung

Es besteht für alle in Punkt 4.3 Backend aufgelisteten Cloud Dienste eine separate Testumgebung in denen keine Produktivdaten verarbeitet oder gespeichert werden.

Gespeicherte Daten:

- UUID von zu Testzwecken installierten Applikationen
- TANs die zu Testzwecken erstellt wurden
- Telefonnummern die zu Testzwecken verwendet werden
- Konfigurationsdaten

Die Testumgebung besitzt Schnittstellen (via HTTPS) zu den folgenden Systemen:

- SMS Gateway ÖRK (Test)

4.4 Angaben zur Einhaltung genehmigter Verhaltensregeln gem Art 40 DSGVO (sofern zutreffend)

Für die geplanten Verarbeitungstätigkeiten existieren (zum Zeitpunkt der Durchführung der DSFA) keine Verhaltensregeln. Sollten künftig relevante Verhaltensregeln (Codes of Conduct) anwendbar werden, wird dies bei Aktualisierungen dieser DSFA entsprechend berücksichtigt.

5 Zulässigkeitsprüfung inkl. Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck

5.1 Liegen personenbezogene Daten vor?

Gemäß Artikel 4 Z 1 DSGVO sind personenbezogene Daten "alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen."

Die Definition des Begriffs „personenbezogene Daten" ist somit sehr weit gefasst, da es keinerlei Einschränkungen gibt, denn es werden alle Informationen die sich auf eine natürliche Person beziehen, davon umfasst.[9] Es kann sich dabei um persönliche Informationen wie Name und Anschrift, also herkömmliche Bestandsdaten, um äußere Merkmale wie Geschlecht, Größe und Gewicht, sowie innere Zustände iSv Überzeugungen und Meinungen, aber auch sachliche Informationen wie Vermögens- und Eigentumsverhältnisse und sonstige Beziehungen der Person zu Dritten können als personenbezogene Daten gem. Art 4 Z 1 DSGVO qualifiziert werden.[10] Die gängigsten Angaben zur Identifizierung einer natürlichen Person sind Name, Adresse, Handynummer, E-Mail-Adresse, Sozialversicherungsnummer[11], KFZ-Kennzeichen[12], IP-Adresse[13] und auch medizinische Diagnosen[14].

Die Qualifikation von personenbezogenen Daten gem. Art 4 Z 1 DSGVO hängt im Wesentlichen von vier Faktoren ab: Information, Personenbezug, natürliche Person und Identifizierung bzw. Identifizierbarkeit.[15]
Die Information kann sich zusammensetzen aus sachbezogenen Aussagen zu Verhältnissen oder überprüfbaren Eigenschaften sowie Einschätzungen und Urteile über die betroffene Person.[16] Der Personenbezug von Daten kann wiederum durch jene Information hergestellt werden, welche ein Inhaltselement, Zweckelement oder Ergebniselement beinhaltet.[17]
Das dritte wesentliche Element der Begriffsbestimmung von personenbezogenen Daten gem. Art 4 Z 1 DSGVO richtet sich auf die betroffene Person, bei der es sich immer um eine natürliche Person handeln muss.[18]
Das vierte und letzte wesentliche Element der Begriffsbestimmung personenbezogener Daten gem. Art 4 Z 1 DSGVO nimmt Bezug auf die Identifizierung bzw. Identifizierbarkeit. Bei der vorliegenden Identitätskomponente bedarf es eine klare Abgrenzung zwischen den sogenannten *„primären*

9 *Hödl* in Knyrim, DatKomm Art 4 Rz 9 DSGVO (Stand 1.12.2018, rdb.at).
10 Vgl *Klar/Kühling* in Kühling/Buchner, DS-GVO Art 4 Rz 8.
11 Vgl DSK 12. 11. 2004, K120.902/0017-DSK/2004.
12 Vgl VfGH 15. 6. 2007, G 147/06; DSK 11.7.2008, K121.359/0016-DSK/2008.
13 Vgl EuGH 19. 10. 2016, C-582/14, Breyer/BRD.
14 Vgl *Hödl* in Knyrim, DatKomm Art 4 Rz 9 DSGVO (Stand 1.12.2018, rdb.at).
15 Vgl *Klabunde* in Ehmann/Selmayr, DS-GVO[2] Art 4 Rz 8.
16 Vgl Art 29-Datenschutzgruppe, 2007 S 7; *Klabunde* in Ehmann/Selmayr, DS-GVO[2] Art 4 Rz 9.
17 Vgl Art 29-Datenschutzgruppe, 2007 S 10; *Klabunde* in Ehmann/Selmayr, DS-GVO[2] Art 4 Rz 10.
18 Vgl *Heißl* in Lachmayer/v. Lewinski, Datenschutz im Rechtsvergleich (2019) 39; *Klabunde* in Ehmann/Selmayr, DSGVO[2] Art 4 Rz 12.

Identifikationsmerkmalen“[19] und jenen Daten, die für die Identifizierbarkeit einer natürlichen Person geeignet sind.

Jene Informationen aus denen die Identität der Person unmittelbar hervorgeht, werden als „*primäres Identifikationsmerkmal*“ bezeichnet, da jene Person durch diese Daten bereits identifiziert ist.[20] Wird somit der Name einer Person verarbeitet, handelt es sich hierbei zweifelsohne um ein personenbezogenes Datum, da die Person idR. bereits durch die Namensangabe identifiziert ist.[21] Dies hat zur Folge, dass sämtliche weiteren Informationen die direkt der identifizierten Person zuordenbar sind als personenbezogene Daten gem. Art 4 Z 1 DSGVO zu werten sind.

Die Identifizierbarkeit richtet sich gem. Art 4 Z 1 2. Halbsatz DSGVO wiederum danach , ob eine natürliche Person „ *(…) direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;*“.
Die Literatur[22] und unionsrechtlichen Judikatur[23] setzen am „*relativen Personenbezug* oder an der *relativen Theorie*“[24] an, wonach für die Qualifikation einer Einzelangabe als personenbezogenes Datum gem. Art 4 Z 1 DSGVO die Kenntnisse und Mittel der datenverarbeitenden Stelle ausschlaggebend sind, wonach sich letztendlich die Identifizierbarkeit richtet. Sofern der Verantwortliche (auch überdie dem Verantwortlichen zurechenbaren (Sub-)Auftragsverarbeiter durch relevantes Zusatzwissen[25] Einzelangaben einer Person direkt zuordnen kann, ist die Identifizierbarkeit zu bejahen, wodurch diese Einzelangaben für die datenverarbeitende Stelle als personenbezogene Daten gem. Art 4 Z 1 DSGVO zu qualifizieren sind.[26] Selbige Auffassung vertrat der EuGH in der Rechtssache C-582/14 zum Urteil Breyer gegen BRD, wonach dynamische IP-Adressen einer natürlichen Person für den Anbieter als personenbezogene Daten gem. Art 4 Z 1 DSGVO (ex-Art 2 lit a EG-DSRL) zu beurteilen sind, sofern der Anbieter *über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, (…), bestimmen zu lassen.*“[27]

5.1.1 Personenbezug in der Stopp Corona-App:

Im vorliegenden Projekt der Stopp Corona-App sind manche individuellen Informationen, die im Zuge der Inbetriebnahme und Nutzung verarbeitet werden, als personenbezogene Daten gem Art 4 Z 1 DSGVO zu qualifizieren.

Für die Nutzung der App ist vorerst keine Eingabe von personenbezogenen Daten notwendig. Auf dem Endgerät werden auf der Ebene des Betriebssystems eindeutige, zufällige Zahlenketten („Zufalls-IDs“)

---

19 Vgl *Hödl* in *Knyrim*, DatKomm Art 4 Rz 11 DSGVO (Stand 1.12.2018, rdb.at).

20 Vgl EuGH 19. 10. 2016, C-582/14, *Breyer/BRD*.

21 Vgl. *Klar/Kühling* in *Kühling/Buchner*, DS-GVO Art 4 Rz 18; *Eßer* in *Eßer/Kramer/v.Lewinski* (Hrsg.), DSGVO/BDSG[6] Art 4 Rz 17.

22 Vgl *Eßer* in *Eßer/Kramer/v.Lewinski* (Hrsg.), DSGVO/BDSG[6] Art 4 Rz 20; *Hödl* in *Knyrim*, DatKomm Art 4 Rz 14 DSGVO (Stand 1.12.2018, rdb.at).

23 Vgl. EuGH 19.10.2016, C-582/14, *Breyer/BRD*.

24 Vgl. *Hödl* in *Knyrim*, DatKomm Art 4 Rz 14 DSGVO (Stand 1.12.2018, rdb.at); *Klar/Kühling* in *Kühling/Buchner,* DS-GVO Art 4 Rz 26 ff; *Eßer* in *Eßer/Kramer/v.Lewinski* (Hrsg.), DSGVO/BDSG[6] Art 4 Rz 20.

25 Ob zudem unter der DSGVO noch das Kriterium “rechtlich zulässige Mittel” zu berücksichtigen ist, ist nicht völlig geklärt, krit *Karg* in *Simitis/Hornung/Spiecker* (Hrsg), Datenschutzrecht (2019) Art 4 Nr. 1 Rz 64; deutlicher *Brauneck*, EuZW 2019, 680 (688).

26 Vgl. *Eßer* in *Eßer/Kramer/v.Lewinski* (Hrsg.), DSGVO/BDSG[6] Art 4 Rz 20.

27 EuGH 19. 10. 2016, C-582/14, *Breyer/BRD*, Rz 65.

generiert, die von der App genutzt und bei einer Infektions- oder Verdachtsmeldung an unseren Server übermittelt werden.

Konkret werden auf dem Endgerät auf der Ebene des Betriebssystems zwei verschiedene Zahlenketten erzeugt:

1. TEK (= temporary exposure key) – hiervon gibt es einen pro Tag

2. RPI (=rolling proximity identifier) – diese wird aus den TEK abgeleitet und regelmäßig in kurzen Abständen neu generiert

Solange keine Verdachts- oder Infektionsmeldung abgeben wird, handelt es sich in beiden Fällen um anonyme Daten. Im Falle einer Verdachts- oder Infektionsmeldung werden die TEK durch deren Veröffentlichung zu sogenannten pseudonymen Daten. Auch bei den Telefonnummern handelt es sich um personenbezogene Daten.

Die Qualifikation des der TEK als personenbezogenes Datum ab Verdachts- oder Infektionsmeldung ist auf die bereits angeführte EuGH-Judikatur[28] zurückzuführen. Jedem App-Nutzer werden die Zufalls-IDs bei Verwendung der App zugewiesen. Der Verantwortliche hat keine direkte Möglichkeit der Zuordnung zu einer bestimmten Person (Nutzer). Eine solche Möglichkeit könnte dann bestehen, wenn zusätzliche Daten erhoben würden, die eine Identifikation des Betroffenen ermöglichen (zB MAC Adresse, etc). Weil die Stopp Corona-App bewusst so gebaut wurde, dass keine solchen zur Identifikation geeigneten Daten zusätzlich erhoben werden, ist in aller Regel nicht möglich, einen Personenbezug herzustellen. Weil jedoch unwahrscheinliche aber doch theoretisch mögliche Konstellationen im Einzelfall bestehen können, die eine Identifikation durch komplexe Verknüpfungen erlauben könnten, muss auch der TEK ab Verdachts- bzw. Infektionsmeldung - rechtlich korrekt als Pseudonym dargestellt werden.

Nur aus diesen Nummern und den uns sonst zur Verfügung stehenden Daten kann der Verantwortliche nicht herausfinden, wer der Betroffene ist. Dies gilt, solange Betroffene keine Infektion melden - nur dann erfasst der Verantwortliche für 30 Tage die Mobiltelefonnummer, damit Missbrauch möglichst verhindert wird. Hier besteht ein Widerspruchsrecht gem. Art 21 DSGVO, allerdings müssen Betroffene triftige Gründe vorbringen, wenn die Telefonnummer vor Ablauf der 30 Tage nach der Infektionsmeldung gelöscht werden soll. Darüber hinaus hat der Verantwortliche keine Möglichkeit, Betroffene zu identifizieren, deren Bewegungen oder sozialen Kontakte nachzuvollziehen. Im allgemeinen Sprachgebrauch wird dies als anonyme Verarbeitung bezeichnet. Nach einem strengen juristischen Begriffsverständnis ist dies aber nicht korrekt. Rechtlich richtig ausgedrückt sind die Daten (extrem stark) pseudonymisiert.

Die Rechtsprechung des Gerichtshofs der EU (EuGH Rs Breyer) ist hier mit guten Gründen sehr streng. Schon geringe Wahrscheinlichkeiten reichen für die Einordnung als personenbezogene, oder auch pseudonymisierte, Daten aus. Auch wenn nur unter außergewöhnlichen und seltenen Umständen ein Personenbezug hergestellt werden kann, wenn man also sprichwörtlich „alle Register zieht“, müssen die Daten als personenbezogen gelten. Weiter im Dokument wird daher nur noch von pseudonymisierten Daten die Rede sein.

Personenbezogene Angaben, die im Zuge der Nutzung erhobenen werden sind: Zufalls-IDs, Telefonnummer sowie Gesundheitsdaten im Fall einer Krankmeldung, Verständigung der Intensiv-Kontakte über COVID-19 Krankmeldung sowie die Übermittlung dieser Meldung an das ÖRK; nur im Gerät: ID der Intensiv-Kontakte und der Datenfluss zwischen Geräten der Intensiv-Kontakte) sind als personenbezogene Daten gem. Art 4 Z 1 DSGVO zu qualifizieren, da es sich hierbei einerseits um „primäre Identifikationsmerkmale“ handelt, aus denen die Identität der betroffenen Person unmittelbar hervorgeht, als auch um solche Informationen, durch deren Verarbeitung die betroffene

[28] Vgl EuGH 19. 10. 2016, C-582/14, *Breyer/BRD*.

Person identifizierbar ist. Darüber hinaus ist nach der bereits angeführten EuGH-Judikatur auch der Unique Identifier (ID) als personenbezogenes Datum anzusehen, da dieser rechtlich mit einer statischen IP-Adresse vergleichbar ist. Aufgrund dessen, dass es sich beim TEK ab Verdachts- bzw. Infektionsmeldung um ein personenbezogenes Datum handelt, sind auch sämtliche Informationen, die dieser ID zugeordnet werden können, ls personenbezogene Daten zu werten.

5.1.2 Besondere Kategorien personenbezogener Daten:

Art 9 DSGVO enthält eine Aufzählung von besonderen Kategorien personenbezogener Daten, dessen Zweck im Schutz der betroffenen Person vor der Möglichkeit tatsächlich datenbasierter Diskriminierungen liegt.[29] Jene besonderen Kategorien umfassen personenbezogene Daten einer natürlichen Person betreffend die rassistische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, das Sexualleben oder die sexuelle Orientierung, sowie genetische Daten iSv. Art 4 Z 13 DSGVO, biometrische Daten iSv Art 4 Z 14 DSGVO und Gesundheitsdaten iSv. Art 4 Z 15 DSGVO.[30]

Jene personenbezogenen Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen, einschließlich der Gesundheitsdienstleistungen, werden als Gesundheitsdaten gem. Art 4 Z 15 DSGVO definiert. Gemäß ErwGr 35 DSGVO beziehen sich Gesundheitsdaten ua. auf jene Informationen, aus denen der frühere, gegenwärtige und künftige körperliche oder geistige Gesundheitszustand der betroffenen Person hervorgeht.[31] Ferner sind unter Gesundheitsdaten auch jene Daten oder Informationen zu subsumieren, welche mittelbar einen Rückschluss auf den Gesundheitszustand der betroffenen Person ermöglichen, weshalb auch Krankheitssymptome als solches zu qualifizieren sind.[32]

Aufgrund des TEK der ab Verdachts- bzw. Infektionsmeldung als personenbezogen einzustufen ist, sind sämtliche weiteren Informationen ebenfalls als personenbezogene Daten gem Art 4 Z 1 DSGVO zu qualifizieren. Von jenen weiteren Informationen umfasst sind auch Angaben über den aktuellen Gesundheitszustand oder zu etwaigen Krankheitssymptomen, insbesondere daher auch eine allfälligee Krankmeldung als Information über die Bestätigung einer ärztlich attestierten COVID-19 Infektion. Da hierbei explizit Gesundheitsdaten gem Art 4 Z 15 DSGVO verarbeitet werden, welche zunächst dem TEK und in weiterer Folge der Telefonnummer des App-Nutzers zugewiesen werden können, handelt es sich um besondere Kategorien personenbezogener Daten gem Art 9 Abs 1 DSGVO.

5.2 Rechtsgrundlagen

5.2.1 Regelungssystematik der DSGVO zum besseren Verständnis:

Die aus der DSGVO abzuleitende Regelungssystematik in Bezug auf die Rechtsgrundlagen sieht vor, dass jegliche Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist, es sei denn, ein Erlaubnistatbestand bzw. eine Rechtsgrundlage des Art 6, 9 oder 10 DSGVO rechtfertigt die betreffende Datenverarbeitung.[33] Für die Verarbeitung von personenbezogenen Daten gem. Art 4 Z 1 DSGVO enthält Art 6 Abs 1 DSGVO eine taxative Liste von sechs Rechtsgrundlagen:

---

29 Vgl. *Schiff* in *Ehmann/Selmayr*, Datenschutz-Grundverordnung, Art 9 Rz 13 f.

30 Vgl. *Feiler/Forgó*, EU-DSGVO 3.

31 Vgl. *Hödl* in *Knyrim*, DatKomm Art 4 Rz 156 DSGVO (Stand 1.12.2018, rdb.at).

32 Vgl. *Hödl* in *Knyrim*, DatKomm Art 4 Rz 158 DSGVO (Stand 1.12.2018, rdb.at); EuGH 6. 11. 2003, C-101/1, Lindqvist.

33 Vgl. *Feiler/Forgó*, EU-DSGVO Art 6 Anm 1.

- lit a - Einwilligung der betroffenen Person für einen oder mehrere bestimmte Zwecke
- lit b - Das Vorliegen eines Vertrags, oder die Durchführung vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person
- lit c - Die Erfüllung einer gesetzlichen Verpflichtung des Verantwortlichen
- lit d - Die Erforderlichkeit zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten
- lit e - Die Erforderlichkeit für eine Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, welche dem Verantwortlichen übertragen wurde
- lit f - Zur Wahrung der überwiegend berechtigten Interessen des Verantwortlichen

In Art 9 Abs 2 DSGVO befinden sich jene zehn Rechtsgrundlagen, welche für die rechtmäßige Verarbeitung besonderer Kategorien personenbezogener (sensibler) Daten[34] erforderlich sind. Da einerseits der Gesetzgeber diesen Daten eine höhere Schutzwürdigkeit[35] zuspricht und auch erhöhte Anforderungen in jenen Rechtsgrundlagen gem. Art 9 Abs 2 DSGVO bestehen, ist für die Verarbeitung besonderer Kategorien personenbezogener Daten ein Rückgriff auf die Rechtsgrundlagen gem. Art 6 Abs 1 DSGVO ausgeschlossen.[36]

Folgende taxative Auflistung beinhaltet die zehn Rechtsgrundlagen gem. Art 9 Abs 2 DSGVO:

- lit a – Ausdrückliche Einwilligung der betroffenen Person
- lit b - Zur Erfüllung von Pflichten oder Ausübung von Rechten im Arbeits- und Sozialrecht
- lit c - Die Erforderlichkeit zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten, ohne erteilter Einwilligung
- lit d - Interne Verarbeitung durch Organisationen ohne Gewinnerzielungsabsicht
- lit e - Die Verarbeitung von offensichtlich öffentlich gemachten Daten, durch die betroffene Person selbst
- lit f - Die Erforderlichkeit der Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte
- lit g - Aus Gründen eines erheblichen öffentlichen Interesses
- lit h - Für Zwecke des Gesundheits- oder Sozialwesens
- lit i - Die Erforderlichkeit aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
- lit j - Die Erforderlichkeit für im öffentlichen Interesse liegende Archiv-, Forschungs- oder statistische Zwecke

5.2.2 Rechtsgrundlagen und Verarbeitungszwecke der Stopp Corona-App:

Nachfolgend werden die wesentlichen Rechtsgrundlagen mit Blick auf deren Anwendbarkeit näher ausgeführt und im Anschluss erfolgt die rechtliche Beurteilung zu den erforderlichen Rechtsgrundlagen der Stopp Corona-App (Subsumtion).

---

34 Gem. Art 9 Abs 1, Art 4 Z 13 - 15 DSGVO.

35 Vgl. *Kastelitz*/*Hötzendorfer*/*Tschohl* in *Knyrim*, DatKomm Art 9 Rz 4, 16 DSGVO (Stand 1.10.2018, rdb.at).

36 Vgl. *Schantz* in *Schantz*/*Wolff*, Das neue Datenschutzrecht Rz 705; *Frenzel* in *Paal*/*Pauly*, DSGVO/BDSG[2] Art 9 Rz 18.

Rechtliche Beurteilung der erforderlichen Rechtsgrundlagen der Stopp Corona-App im Überblick:

Ab App-Installation bis **vor** der Infektionsmeldung:

1. Für den Zweck Kontakt-Tagebuch: Einwilligung Art 6 Abs 1 lit a iVm Art 9 Abs 2 lit a DSGVO
2. Für die Kommunikation über das Internet, um den Informationsfluss zu ermöglichen: berechtigtes Interesse Art 6 Abs 1 lit f DSGVO

Ab der Infektionsmeldung:

1. Für den Zweck Meldung an alle relevanten Kontakte: Art 6 Abs 1 lit a und Art 9 Abs 2 lit a DSGVO
2. Für den Zweck Missbrauchsbekämpfung: Art 6 Abs 1 lit f und Art 9 Abs 2 lit f DSGVO – mit Widerspruchsrecht auch für Art 9 Abs lit f
3. Für den Zweck der Verpflichtung, behördlichen Auskunftsanfragen nachzukommen: Art 6 Abs 1 lit c iVm Art 9 Abs 2 lit i DSGVO

Rechtsgrundlage für die Verarbeitung zum Zweck der Grundfunktionalität (Kontakttagebuch) von der App-Installation bis vor der Infektionsmeldung:

Daten, die ab der Installation der App verarbeitet werden

Wie bereits weiter oben gesagt, ist für die Nutzung der App ist vorerst keine Eingabe von personenbezogenen Daten durch den Nutzer notwendig. Die App ist darauf ausgerichtet, dass keinerlei technische Rückschlüsse auf Personen, Standorte oder Geräte möglich sind. Es werden lediglich verschiedene Schlüssel zur Erfassung der Kontakt-Ereignisse erzeugt und ausgetauscht. Konkret werden auf dem Endgerät auf der Ebene des Betriebssystems zwei verschiedene Schlüssel erzeugt:

1. TEK (= temporary exposure key) – hiervon gibt es einen pro Tag
2. RPI (=rolling proximity identifier) – diese wird aus den TEK abgeleitet und in kurzen Abständen (ca alle 10 Minuten) neu generiert

Die Erzeugung und Verarbeitung dieser Daten erfolgt grundsätzlich bereits auf der Ebene des Betriebssystems des Endgeräts als Teil der sogenannten “Exposure Notification API” . Das Rote Kreuz ist für diese Verarbeitungsvorgänge nur soweit verantwortlich, als die App diese Schnittstelle der Hersteller nutzt. Darüber hinaus besteht eine unmittelbare Rechtsbeziehung zwischen dem Betreiber des Betriebssystems (Apple oder Google) auf Basis der jeweiligen Lizenzbedingungen mit der Nutzerin/dem Nutzer. Solange keine Verdachts- oder Infektionsmeldung abgeben wurde, handelt es sich in beiden Fällen um anonyme Daten.

Die App erzeugt außerdem pro TEK einen Sicherheitscode, der für 14 Tage am Endgerät gespeichert wird. Dieser Code wird bei einer Verdachts- oder Infektionsmeldung zur technischen Authentifizierung der Meldung an den Server übermittelt. Diese Verarbeitung basiert auf einer ausdrücklichen Einwilligung gem Art 6 Abs 1 lit a iVm Art 9 Abs 2 lit a DSGVO. Die ausdrückliche Einwilligung umfasst zudem die Verarbeitung der IDs der Intensiv-Kontakte sowie die Handshake-Daten zwischen den Geräten der Intensiv-Kontakte. Diese Datenverarbeitung ist dadurch gerechtfertigt, dass die

Einwilligung (Art 6 Abs 1 lit a und Art 9 Abs 2 lit a DSGVO) zur Nutzung der App erforderlich ist. Bei der Verarbeitung der Kontaktaufnahme mit Intensiv-Kontakten durch den digitalen Handshake werden die dafür verarbeiteten Daten nicht im Backend erfasst. Um mit einem anderen Stopp Corona-App Nutzer in Verbindung treten zu können. Diese Kontaktaufnahme findet nur Peer-to-Peer zwischen den Intensiv-Kontakten statt.

Für den automatisierten Handshake bedarf es neben der Erteilung der Berechtigung für die hierfür technologisch erforderlichen Funktionen (Bluetooth und grober Standort) kein weiteres Zutun der Intensiv-Kontakte. Die Erforderlichkeit der Einholung der ausdrücklichen Einwilligung, welche mittels Opt-in-Verfahren die Verarbeitung durch den automatisierten Handshake umfasst, liegt vor allem darin, dass durch diese Verarbeitung der Zweck der Grundfunktionalität, die auf die Unterbrechung der COVID-19 Infektionsketten abzielt, am effizientesten verwirklicht werden kann. Denn durch die Verarbeitung mittels automatisierten Handshake kann die Grundfunktionalität bestmöglich verwirklicht werden, indem ein möglichst lückenloses Kontakttagebuch geführt werden kann, welches alle Intensiv-Kontakte, die in einem Radius von zwei Metern in einem Zeitrahmen von fünfzehn Minuten miteinander verbracht haben, pseudonym für drei Tage lokal speichert. Sofern jedoch der Stopp Corona-App Nutzer die Funktion des automatisierten Handshakes nicht nutzen möchte, kann hierfür die ausdrückliche Einwilligung jederzeit widerrufen werden. Mit der Deaktivierung werden alle durch dem automatischen digitalen Handshake bedingten Datenverarbeitungen eingestellt. Bisher mit Handshake-Partnern geteilte Tokens verbleiben im lokalen Speicher des Handshake-Partners. Dadurch, dass sowohl beim manuellen als auch beim automatisierten Handshake die Daten primär nur für die Grundfunktionalität, zeitlich stark begrenzt und nur lokal am Endgerät des Stopp Corona-App Nutzers verarbeitet werden, kommt es durch diese Datenminimierungs- und Speicherbegrenzungsmaßnahmen zu keiner Aufzeichnung von Standortdaten, wodurch auch keine Bewegungsprofile erstellt werden können. Die Verarbeitung ist für die Erstellung eines Kontakttagebuchs erforderlich, um damit den Verarbeitungszweck der proaktiven, eigenverantwortlichen und schnellen Unterbrechung der Corona-Infektionskette zu erfüllen. Detaillierte Ausführungen bezüglich dem sogenannten Kopplungsverbot, welches iZm dieser ausdrücklichen Einwilligung näher erläutert werden muss, folgen nach der nächsten Grafik.

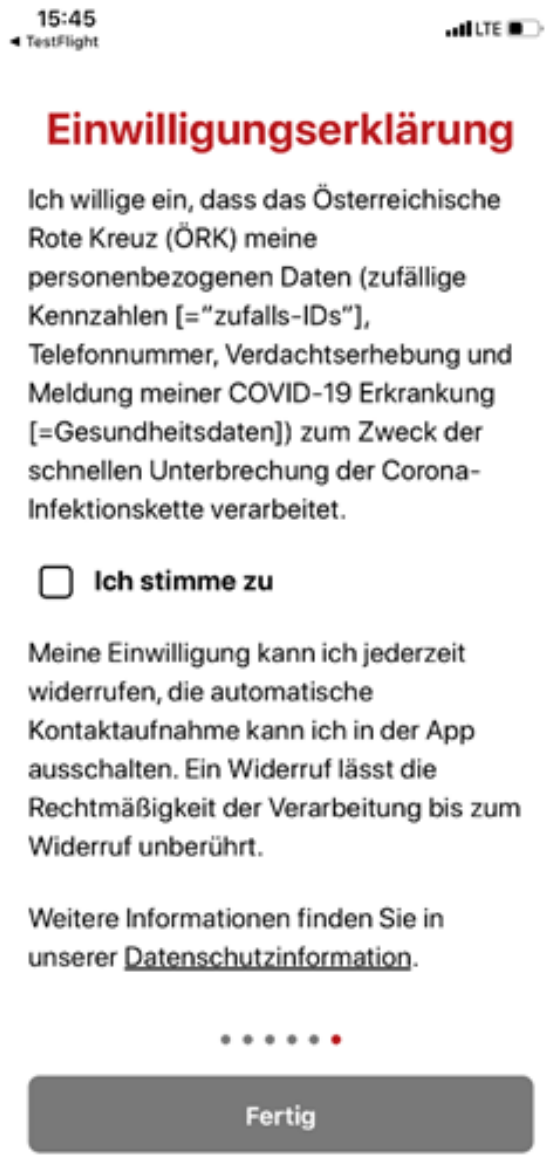
Darüber hinaus wird auf Basis der ausdrücklichen Einwilligung die Telefonnummer der betroffenen Person, die ärztlich attestierte COVID-19 Krankmeldung, die pseudonymisierte Verständigung der jeweiligen Intensiv-Kontakte über die COVID-19 Krankmeldung der betroffenen Person und die Übermittlung der COVID-19 Krankmeldung an den Verantwortlichen verarbeitet. Wie bereits ausgeführt, handelt es sich bei der COVID-19 Krankmeldung um eine besondere Kategorie personenbezogener Daten, da aus diesen Angaben über den aktuellen Gesundheitszustand der betroffenen Person hervorgehen, wodurch Gesundheitsdaten gem Art 4 Z 15 DSGVO vorliegen. Will die betroffene Person eine COVID-19 Krankmeldung bestätigen, so wird diese vom Verantwortlichen dazu aufgefordert ihre Telefonnummer bekannt zu geben, um eine authentifizierte COVID-19 Krankmeldung zu übermitteln.

Durch die verarbeitete authentifizierte COVID-19 Krankmeldung kann die betroffene Person eine pseudonymisierte Verständigung der jeweiligen Intensiv-Kontakte über die eigene COVID-19 Krankmeldung erteilen. Diese pseudonymisierte Verständigung wird mittels Verschlüsselungsmechanismen übermittelt, wodurch nur die jeweiligen Intensiv-Kontakte der betroffenen Person über eine COVID-19 Krankmeldung verständigt werden können, welche inhaltlich jedoch keinen Personenbezug aufweist. Die Verarbeitung jener Daten ist für den Zweck der Applikation als wesentlicher Beitrag zur Unterbrechung der COVID-19 Infektionskette durch proaktives und eigenverantwortliches Mitwirken der betroffenen Person zur Aufrechterhaltung der öffentlichen Gesundheit durch Eindämmung der COVID-19 Pandemie erforderlich und basiert auf der Rechtsgrundlage Art 6 Abs 1 lit a iVm Art 9 Abs 2 lit a DSGVO.

Die Möglichkeit des jederzeitigen Widerrufs der Einwilligung gem Art 7 Abs 3 DSGVO bleibt dahingehend gewahrt, dass sofern keine COVID-19 Krankmeldung oder Verdachtsmeldung verarbeitet wurde, die betroffene Person diesen jederzeit durch Löschung bzw. Deinstallation der Stopp Corona-App wahrnehmen kann. Darüber hinaus, kann die Einwilligung hinsichtlich der Verarbeitung mittels automatisierten Handshake eigenständig widerrufen werden - diesbezüglich wird im darauffolgenden Absatz näher eingegangen. Ab der Übermittlung der der COVID-19 Krankmeldung oder Verdachtsmeldung kann die Einwilligung beim Datenschutzbeauftragten des Verantwortlichen per E-Mail, Telefon oder Post jederzeit widerrufen werden.

Die Einwilligung wird vor der ersten Nutzung im Rahmen der App-Installation wie folgt eingeholt:

Aktueller Wortlaut der Einwilligungserklärung bei **Installation:**



Kommentar: Checkbox muss aktiv angehakt werden, sonst kann die Installation der App nicht fortgesetzt werden. Die ausdrückliche Einwilligung wird zum Nachweis gespeichert (zur Unique-ID zugeordnet).

Bis zum 11.05.2020 wurde für die Symptomchecker-Funktion eigens eine Einwilligung eingeholt. Diese zusätzliche Einwilligung, wurde zugunsten einer einheitlichen Einwilligungserklärung, welche gleich nach dem ersten Start der Applikation eingeholt wird, gestrichen. Diese Änderung ist Ausfluss einer Empfehlung 3.2.3 des Berichts[37] von Epicenter.Works, NOYB und SBA-Research zur Stopp Corona-App, wonach die gesonderte Einwilligung keine zusätzliche Transparenz schüfe. Die Empfehlung wurde intern auf mögliche Unvereinbarkeiten mit Art 7 Abs 2 DSGVO geprüft. Insbesondere könnte der Symptomchecker einen von den restlichen App-Funktionen gesonderten Sachverhalt iSd Art 7 Abs 2 DSGVO bilden. Dagegen sprechen die nahezu identen Datenkategorien, sowie die identen Verarbeitungszwecke zwischen der Applikation im Allgemeinen und der Symptomchecker-Funktion.

Sohin ist die Smyptomchecker-Funktion bloß als eine von mehreren Funktionen der Stopp Corona-App zu sehen. Geht man an dieser dieser Stelle von zwei getrennten Sachverhalten aus, überzeugt das Argument der Empfehlung 3.2.3, wonach weshalb zwei getrennte Einwilligungserklärungen, welche fast idente Datenkategorien ausweisen, kein höheres Maß an Transparenz ergeben. Aus diesen Gründen wurde Empfehlung 3.2.3 umgesetzt.

Hinsichtlich des bereits angeführten Kopplungsverbots nach Art 7 Abs 4 DSGVO, welches ein Abhängigmachen vertraglicher Leistungen von der Erteilung einer Einwilligung der betroffenen Person in eine (sachfremde) Datenverarbeitung untersagt, ist laut *Kastelitz* Folgendes zu prüfen:[38]

Ausgangspunkt einer Prüfung gem Art 7 Abs 4 DSGVO ist zuallererst, ob und wenn ja welche Verarbeitungen für die Vertragserfüllung erforderlich sind. Sowohl die Rechtfertigung gem Art 6 Abs 1 lit b DSGVO als auch das Kopplungsverbot in Art 7 Abs 4 DSGVO knüpfen daran an, ob die in Rede stehenden Datenverarbeitungsvorgänge für die Erfüllung eines Vertrags (einschließlich der Erbringung einer Dienstleistung) erforderlich sind. Vom Kopplungsverbot können daher nur Einwilligungen erfasst sein, die für den Vertragszweck nicht erforderlich sind. Umgekehrt formuliert ist Art 7 Abs 4 DSGVO auf all jene Fälle nicht anwendbar, in welchen die Datenverarbeitung für die Vertragserfüllung/Leistungserbringung erforderlich ist. Es liegt somit kein „absolutes Kopplungsverbot" vor, welches jede an einen Vertragsschluss gebundene Einwilligung untersagt.[39] Die Erforderlichkeit der Erteilung einer Einwilligung für die Vertragserfüllung setzt nach der Literatur an das Kriterium der Abhängigkeit der Leistungserbringung von der Erteilung der Einwilligung an, welche sodann zulässig ist, wenn *„diese Datenverarbeitung die notwendige Entscheidungs- und Kalkulationsgrundlage für das konkrete Rechtsgeschäft bietet."*[40]

Die betroffene Person, die die App in Anspruch nehmen will, entschließt sich freiwillig dazu, dies zu tun: Da das Wesen der App in der "personalisierten Benachrichtigung über Infektionsrisiken" zur Unterbrechung von COVID-19 Infektionsketten liegt, gibt es auch kein Angebot, welches unzulässigerweise an eine nicht notwendige Datenverarbeitung geknüpft ist. Vielmehr ist die Datenverarbeitung für die Erbringung der App-Funktionen erforderlich. Die Erforderlichkeit der Erteilung der ausdrücklichen Einwilligung für die Vertragserfüllung iSd Nutzung der Grundfunktionalität der Stopp Corona-App für die Verarbeitung durch den automatisierten Handshake liegt vor allem darin, dass dadurch der Verarbeitungszweck, welcher auf die Unterbrechung der COVID-19 Infektionsketten abzielt, am effizientesten verwirklicht werden kann. Denn durch die Verarbeitung

---

37 Technische und Rechtliche Analyse der Stopp Corona App des Österreichischen Roten Kreuzes, https://noyb.eu/de/bericht-corona-app-des-roten-kreuz-ueberprueft (abgerufen am 11.05.2020).

38 Vgl zum folgenden Absatz *Kastelitz* in *Knyrim*, DatKomm Art 7 DSGVO Rz 33 ff (Stand 1.10.2018, rdb.at).

39 Vgl *Heckmann/Paschke* in *Ehmann/Selmayr*, DS-GVO² Art 7 Rz 53; *Gierschmann* in *Gierschmann/Schlender/Stentzel/Veil*, DS-GVO Art 7 Rz 62.

40 Vgl *Buchner/Kühling* in *Kühling/Buchner*, DS-GVO² Art 7 Rz 47.

mittels automatisierten Handshake kann die Grundfunktionalität bestmöglich realisiert werden, indem ein möglichst lückenloses Kontakttagebuch von sämtlichen Stopp Corona-App Nutzern geführt werden kann. Um dies zu erreichen, umfasst die betreffende Einwilligung, welche mittels Opt-in-Verfahren zu Beginn der Erstinbetriebnahme der Stopp Corona-App eingeholt wird, auch die Verarbeitung durch den automatisierten Handshake. Dadurch, dass die Datenverarbeitung durch den automatisierten Handshake für den Verarbeitungszweck iSd Leistungserbringung der Grundfunktionalität zur Unterbrechung der COVID-19 Infektionsketten erforderlich ist und die Einwilligung auch nicht über das für die ordnungsgemäße Nutzung der App Erforderliche hinausgeht, liegt im Ergebnis kein Anwendungsfall von Art 7 Abs 4 DSGVO (Kopplungsverbot) vor.

Aus denselben Gründen liegt auch keine Verletzung des Grundsatzes „Datenschutz durch datenschutzfreundliche Voreinstellungen" vor. Mit „Voreinstellungen" ist nicht die primäre Funktionalität der Anwendung adressiert. Gemäß Art 25 Abs 2 DSGVO sollen „grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist". Als Voreinstellung sollen also nur solche Daten verarbeitete werden, die zur Erreichung der primären (legitimen) Ziele erforderlich sind. Das ist beim automatischen digitalen Handshake im Hinblick auf das Ziel der schnellstmöglichen Unterbrechung der Infektionskette wie soeben beschrieben der Fall. Weil die Rechtsgrundlage aber dennoch die Einwilligung ist, kann diese Einwilligung auch jederzeit widerrufen werden. Durch ein einfaches Ausschalten der Funktion in der App ist die informationelle Selbstbestimmung voll gewahrt.

Sofern der Stopp Corona-App Nutzer die Funktion des automatisierten Handshakes also nicht nutzen möchte, kann hierfür die ausdrückliche Einwilligung jederzeit widerrufen werden.Solange keine Krankmeldung geschickt wurde liegen anonyme Daten vor und kann das einfach über die Deinstallation bzw. Löschung der Stopp Corona App erfolgen. Damit werden keine personenbezogenen Daten des Nutzers mehr verarbeitet. Ein partieller Widerruf ist zudem dadurch möglich, dass der automatische „digitale Handshake" deaktiviert wird. Die Rechtmäßigkeit der Verarbeitung bis zum Widerruf wird dadurch nicht berührt.
Es wird somit jedem Stopp Corona-App Nutzer auch weiterhin die Möglichkeit der jederzeitigen Inanspruchnahme des Widerrufsrechts gem. Art 7 Abs 3 DSGVO bezüglich der Verarbeitung durch den automatisierten Handshake mittels Opt-out-Verfahren eingeräumt. Dies trägt maßgeblich zur Wahrung der informationellen Selbstbestimmung bei, welches sich aus dem Grundrecht auf Datenschutz gem. § 1 DSG ableiten lässt, denn dadurch wird dem Einzelnen zusätzlich ermöglicht, die Ausgestaltung der Verarbeitung seiner personenbezogenen Daten selbst zu bestimmen.

Daten, die zur technischen Bereitstellung der App erforderlich sind (berechtigtes Interesse):

Jede Kommunikation über das Internet erfordert bestimmte Daten, um den Informationsfluss zu ermöglichen. Im konkreten Fall sind folgende Daten für die Bereitstellung und Nutzung der App erforderlich für die Kommunikation zwischen Ihrem Endgerät (Handy) mit dem Server des ÖRK:

- IP-Adresse

- Datum und Uhrzeit der Anfrage

- Konfiguration (Spracheinstellungen, Gerätetyp und Version des Betriebssystems)

Die Verarbeitung dieser personenbezogenen Daten der Betroffenen erfolgt auf Basis des berechtigten Interesses(Art 6 Abs. 1 lit f DSGVO): die vorübergehende Verarbeitung der angeführten Daten durch das System ist notwendig, um eine Kommunikation zwischen Endgerät und Server zu ermöglichen. Eine Speicherung oder Zusammenführung dieser Daten mit anderen personenbezogenen Daten findet nicht statt. Die Erforderlichkeit der Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses ergibt sich aus den technischen Gegebenheiten, dass ohne Internetkonnektivität bereits das Herunterladen der App nicht möglich ist. Ein Überwiegen der Grundrechte und Grundfreiheiten der betroffenen Person ist nicht ersichtlich, da zum einen der

Betroffene die App freiwillig installiert und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass eine Verarbeitung für diesen Zweck erfolgen wird - die allermeisten Aktivitäten auf einem Smartphone (ein solches Endgerät ist zur Nutzung der App notwendig), erfordert eine Internetverbindung, um Daten abrufen und übertragen zu können. Jedem Nutzer wird aus objektiver Sicht bekannt sein, dass es bei der typischen Handynutzung zu einem Datenfluss ("Traffic") kommt.

Rechtsgrundlagen für die Verarbeitung ab der Krankmeldung/Verdachtsmeldung:

1. Für den Zweck Meldung an alle relevanten Kontakte: Art 6 Abs 1 lit a DSGVO und Art 9 Abs 2 lit a DSGVO
2. Für den Zweck Missbrauchsbekämpfung: Art 6 Abs 1 lit f und Art 9 Abs 2 lit f – mit Widerspruchsrecht auch für Art 9 Abs 2 lit f
3. Für den Zweck der Verpflichtung, behördlichen Auskunftsanfragen nachzukommen: Art 6 Abs 1 lit c iVm Art 9 Abs 2 lit i DSGVO

Die Verarbeitung der Bestätigung einer Krankmeldung bzw. einer ärztlich attestierten COVID-19 Infektion oder Verdachtsmeldung und die hierfür erhobenen persönlichen Daten iSv Telefonnummer stützt sich auch auf **Art 6 Abs 1 lit f iVm Art 9 Abs 2 lit f DSGVO** - zur Geltendmachung von Rechtsansprüchen, zum Zweck um etwaigen Missbrauchsfällen iSv absichtliche Falschmeldungen über das Vorliegen einer ärztlich attestierten COVID-19 Infektion zu verhindern, oder gegebenenfalls bei nachweisbarer Missbräuchlichkeit gegen jene betroffenen Personen rechtlich vorzugehen. Für den Zweck der Vorbeugung und Evaluierung von solchen Missbrauchsfällen wird die COVID-19 Krankmeldung samt den dafür verarbeiteten Daten für einen Zeitraum von 30 Tagen gespeichert und sofern kein Verdachtsfall auf Missbrauch vorliegt nach dem genannten Zeitraum gelöscht. Diese Speicherung erfolgt unabhängig von einem erfolgten Widerruf der Einwilligung. Sobald eine Krankmeldung/Verdachtsmeldung übermittelt wurde, werden die Daten für 30 Tage nach dem Absetzen dieser Meldung aufbewahrt. Wenn es zur Aufklärung einer rechtswidrigen bzw. missbräuchlichen Nutzung der App oder für die Rechtsverfolgung erforderlich ist und konkrete Anhaltspunkte für ein gesetzwidriges bzw. missbräuchliches Verhalten vorliegen, werden die Daten für einen Zeitraum von bis zu drei Jahren nach dem Absetzen der Krankmeldung/Verdachtsmeldung gespeichert.

Rechtsgrundlage für die Verarbeitung von aggregierten Daten zu statistischen Auswertungen:

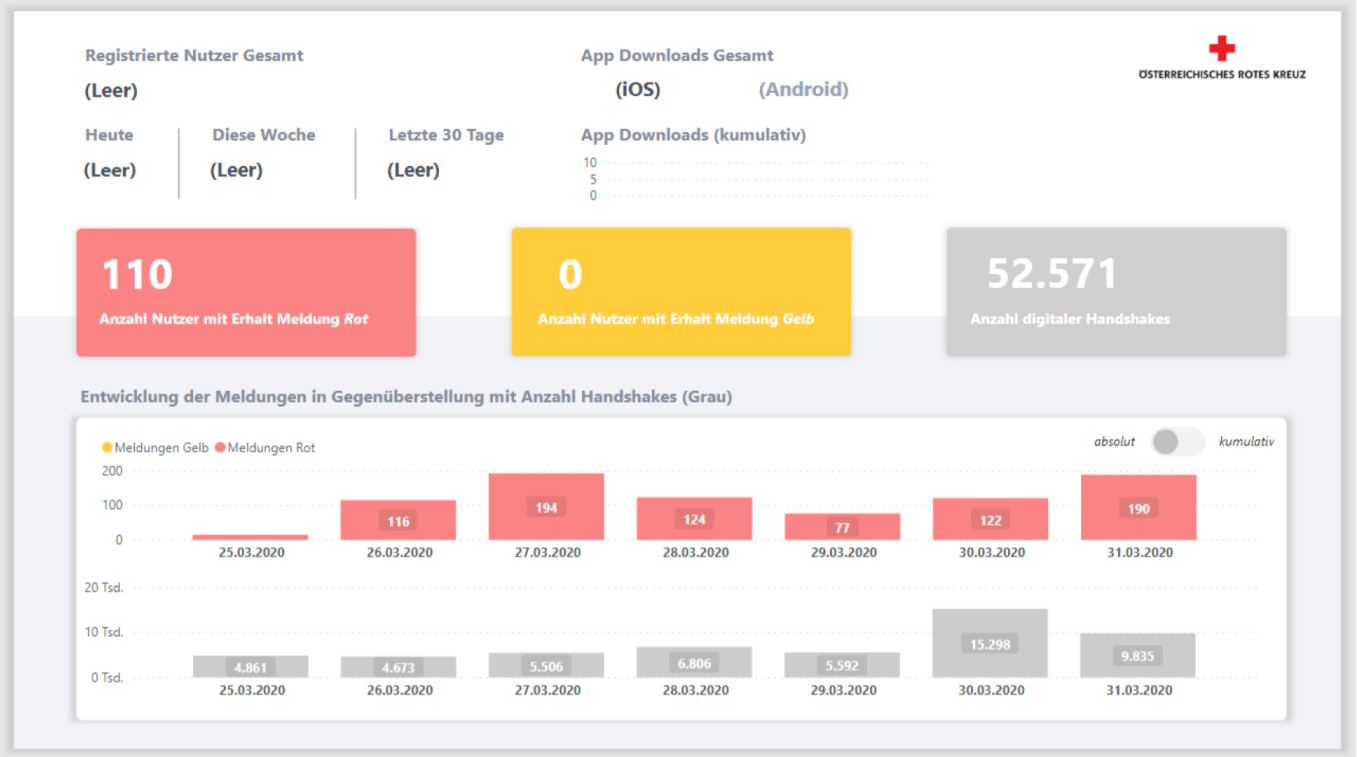
Seit der Stopp Corona App Version 1.1.3 vom 22.4.2020 werden keine Daten für Statistikzwecke erhoben. Für spätere Versionen sind statistische Auswertungen nach folgenden Maßgaben geplant. Die Datenverarbeitung im Rahmen der App ist nicht nur im Interesse der einzelnen natürlichen Person, sondern auch der Gesellschaft insgesamt. Es besteht daher auch ein klares öffentliches Interesse, aus den personenbezogenen Daten (aufgrund der Aggregation anonymisierte) statistische Informationen abzuleiten iSv die Anzahl der Installationen der Stopp Corona-App und die Anzahl der COVID-19 Krankmeldungen. **Die personenbezogenen Daten sowie besondere Kategorien personenbezogener Daten werden somit auch für statistische Zwecke auf der Rechtsgrundlage** § 7 Abs 1 Z 2 DSG iVm Art 9 Abs 2 lit j DSGVO **verarbeitet**, wofür jedoch ein Personenbezug nicht mehr erforderlich ist. Es handelt sich hierbei um rein statistische, nicht-personenbezogene Kennzahlen, die für die Ermittlung der gesellschaftlichen Akzeptanz der Stopp Corona-App sowie Anzahl von Krankmeldungen erforderlich sind. Die Daten wurden gemäß § 7 Abs 1 Z 2 DSG für andere Zwecke zulässigerweise (auf Basis von Art 6 Abs 1 lit a iVm Art 9 Abs 2 lit a DSGVO) ermittelt, zudem haben die Statistiken keine personenbezogenen Ergebnisse zum Ziel. Um die Identifizierbarkeit der betroffenen Person zu verhindern, werden der „Unique Identifier" (UUID) und die persönlichen Daten gelöscht, welche für

die Übermittlung der authentifizierten COVID-19 Krankmeldungen verarbeitet wurden. Dadurch kann es zu keinem personenbezogenen Ergebnis der statistischen Daten kommen und es können keine Rückschlüsse auf jene Daten gezogen werden.

Konkret zeigen die statistischen Auswertungen die Anzahl der Downloads und Handshakes sowie Anzahl der Krankmeldungen/Verdachtsmeldungen – in einer auf Österreich aggregierten Sicht der Nutzung der App in Bezug auf die Verteilung der Handshakes über den Tagesverlauf – aggregiertes Nutzungsverhalten der App Nutzer, zur Frage, ob die Nutzung der App (nicht nur die Installation) eine kritische Zahl erreicht und die App damit ihren Zweck erfüllt.

Erfasst wird auch die Anzahl der durchschnittlichen Handshakes nach Erhalt einer Warnung zur Frage, ob der durchschnittliche Nutzer auf Warnungen reagiert.

Nachfolgend ein schematischer Überblick der geplanten Statistiken:



Registrierte Nutzung der App im Falle einer Krankmeldung

Im Fall einer Krankmeldung, aufgrund eines vom Nutzer eingeholten ärztlichen Attests – werden Nutzer aufgefordert, ihre Mobiltelefonnummer bekannt zu geben. Diese Meldung lässt auf den Gesundheitsstatus und damit auf sensible personenbezogene Daten des Nutzers (= Daten besonderer Kategorie nach Art 9 DSGVO) schließen. Die Verarbeitung dieser Daten erfolgt auf der Rechtsgrundlage der Einwilligung (Art 6 Abs 1 lit a sowie Art 9 Abs 2 lit a DSGVO)

Wenn es zur Aufklärung einer rechtswidrigen bzw. missbräuchlichen Nutzung der App oder für die Rechtsverfolgung erforderlich ist die Datenverarbeitung dadurch gerechtfertigt, dass die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist (Art 6 Abs 1 lit f sowie 9 Abs 2 lit f DSGVO).

Sonstiges zu den geplanten Verarbeitungstätigkeiten

A. **Profiling**

a. Zur Einordnung des Profiling

Bei den geplanten Verarbeitungstätigkeiten könnte es sich rechtlich gesehen zudem tlw um Profiling im Sinne der DSGVO handeln.

Artikel 4 Z 4 DSGVO lautet: „*Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen*;

Artikel 22 DSGVO regelt zudem die Zulässigkeit von automatisierten Entscheidungen im Einzelfall einschließlich des Profilings.

Artikel 22 DSGVO (Automatisierte Entscheidungen im Einzelfall einschließlich Profiling) lautet:

(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr

- *gegenüber rechtliche Wirkung entfaltet oder*
- *sie in ähnlicher Weise erheblich beeinträchtigt.*

(2) Absatz 1 gilt nicht, wenn die Entscheidung
a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.
(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.
(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

b. Ist Art 22 DSGVO (automatisierte Einzelentscheidungen) berührt?

Art 22 DSGVO unterwirft nicht jedes Profiling per se seiner Rechtsfolge. Ein Profiling ist nur dann von Art 22 DSGVO erfasst, wenn alle konstitutiven Merkmal einer Automatisierten Entscheidung im

Einzelfall erfüllt sind. Die Profilbildung muss rechtlichen Wirkungen entfalten, oder die betroffene Person in ähnlich erheblicher Weise beeinträchtigen.[41]

Art 22 DSGVO regelt die Zulässigkeit von ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidungen die dem Betroffenen gegenüber rechtliche Wirkungen entfalten oder diesen in ähnlicher Weise erheblich beeinträchtigen. Zu differenzieren ist daher zwischen zwei Tatbestandselementen:

- Die Entscheidung muss rechtliche oder sonstige erhebliche Auswirkungen auf den Betroffenen haben?
- Es muss eine Entscheidung vorliegen, die ausschließlich auf einer automatisierten Verarbeitung beruht.

c. Bestehen rechtliche Wirkungen oder „ähnlich erhebliche Beeinträchtigungen“?

„Entscheidung mit rechtlicher Wirkung“

Eine rechtliche Wirkung verlangt, dass eine Entscheidung, die ausschließlich auf einer automatisierten Verarbeitung beruht, die Rechte einer Person betrifft, beispielsweise die Vereinigungsfreiheit, das Wahlrecht oder das Recht, rechtliche Schritte einzuleiten. Sie kann auch den rechtlichen Status einer Person oder deren Rechte aus einem Vertrag betreffen.

Beispiele für diese Art der Wirkung sind automatisierte Entscheidungen zu Personen, die zu Folgendem führen:

- der Auflösung eines Vertrags;
- dem Anspruch auf bzw. der Verweigerung einer bestimmten gesetzlichen Sozialleistung wie z. B. Kindergeld oder Wohngeld;
- der Einreiseverweigerung in ein Land oder der Ablehnung der Einbürgerung „sie in ähnlicher Weise erheblich beeinträchtigt“

Auch wenn eine Entscheidungsfindung sich nicht auf die Rechte einer Person auswirkt, kann sie dennoch in den Anwendungsbereich von Artikel 22 DSGVO fallen, wenn sie eine entsprechende Wirkung entfaltet oder die Person in ähnlicher Weise erheblich beeinträchtigt. Anders ausgedrückt, könnte die betroffene Person, selbst wenn sich ihre Rechte oder Pflichten nicht ändern, ausreichend beeinträchtigt werden, um den Schutz dieser Bestimmung zu benötigen. In der DSGVO wird die Formulierung „erheblich beeinträchtigt“ um „in ähnlicher Weise“ ergänzt (die es in Artikel 15 der Richtlinie 95/46/EG nicht gab). Daher muss die Grenze, ab der eine Beeinträchtigung als „erheblich“ anzusehen ist, ähnlich sein wie die Grenze, ab der eine Entscheidung rechtliche Wirkung entfaltet.

ErwGr 71 DSGVO enthält folgende typische Beispiele: „automatische Ablehnung eines Online-Kreditantrags“ oder „Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen“.

Damit die Datenverarbeitung eine Person erheblich beeinträchtigt, muss ihre Wirkung umfassend bzw. erwähnenswert sein. Es muss also die Möglichkeit bestehen, dass die Entscheidung

- die Umstände, das Verhalten oder die Entscheidungen der betroffenen Personen erheblich beeinträchtigt;

41 *Eckhardt* in *Rüpke*/*v. Lewinski*/*Eckhardt*, Datenschutzrecht, § 16, Rz 15.

- die betroffene Person über einen längeren Zeitraum oder dauerhaft beeinträchtigt oder
- im schlimmsten Fall zum Ausschluss oder zur Diskriminierung von Personen führt. Es lässt sich schwer genau definieren, was als erheblich genug einzustufen ist, damit die Grenze erreicht wird; in diese Kategorie könnten jedoch folgende Entscheidungen fallen:

Entscheidungen, die sich auf die finanzielle Lage einer Person auswirken, beispielsweise ihre Kreditwürdigkeit;

- Entscheidungen, die den Zugang zu Gesundheitsdienstleistungen betreffen;
- Entscheidungen, die den Zugang zu Arbeitsplätzen verwehren oder Personen ernsthaft benachteiligen;
- Entscheidungen, die sich auf den Zugang zu Bildung auswirken, beispielsweise Hochschulzulassungen.

5.3 Liegt eine Entscheidung vor, die ausschließlich auf einer automatisierten Verarbeitung beruht?

Bei den zu beurteilenden Verarbeitungstätigkeiten liegt jedoch keine Entscheidung vor, die **ausschließlich** auf einer automatisierten Verarbeitung beruht. Die Einstufung der Personen erfolgt hier nicht ausschließlich automatisiert, ohne jegliches menschliche Eingreifen (vgl ErwGr. 71 DSGVO).

Der EDSA bzw. die Artikel 29 Datenschutzgruppe hat diesbezüglich ausgeführt, dass der Verantwortliche die Bestimmungen von Artikel 22 DSGVO grundsätzlich nicht bereits dadurch umgehen kann, indem er eine Person in die Entscheidung einbezieht. Wenn jemand beispielsweise routinemäßig automatisch erstellte Profile auf Personen anwendet, die keinen tatsächlichen Einfluss auf das Ergebnis haben, wäre dies dennoch eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung. Eine direkte Einbeziehung von Personen ist erforderlich, wobei es sich nicht nur um eine symbolische Geste handeln dürfe. Im Rahmen der DSFA solle der Verantwortliche den Umfang der menschlichen Beteiligung an der Entscheidungsfindung und die Phase, in der sie erfolgt, ermitteln und aufzeichnen.[42]

Die menschliche Beteiligung erfolgt hier durch Einbeziehung der Betroffenen selbst.

Die Betroffenen stoßen aktiv die Verarbeitung ihrer personenbezogenen Daten an und entscheiden in weiterer Folge mittels bewusstem Willensakt über die Verständigung weiterer Intensivkontakte bzgl. des Vorliegens einer bestätigten COVID-19 Infektion bzw. der aus den Ergebnissen des Symptomcheckers/des Selbsttestes resultierenden Verdachtslage .

Hier ist darauf hinzuweisen, dass die Entscheidung über die Meldung von (möglichen) Infektionen gerade in der durch den Betroffenen ausgelösten Übermittlung der Infektions- bzw. Verdachtsmeldung liegt.

Es handelt sich bei den vorliegenden Verarbeitungstätigkeiten somit um keinen Anwendungsfall von Art 22 DSGVO.

[42] Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 17/DEWP251 rev. 01, S 22.

5.4 Angaben über die getroffenen bzw geplanten Maßnahmen zur Einhaltung der DSGVO

5.4.1 Zweckbindungsgrundsatz

Art 5 Abs 1 lit b DSGVO: Erhebung für festgelegte, eindeutige und legitime Zwecke; Weiterverwendung?[43]

Die Festlegung des oben angeführten Zwecks verhindert, dass einmal erhobene und gespeicherte Daten für andere beliebige Zwecke verwendet werden. Der Zweck muss bereits bei Erhebung der Daten festgelegt werden und es ist nicht möglich nach der Erhebung von personenbezogenen Daten andere Zwecke hinzuzufügen. Die strenge Bindung an die rechtmäßigen Tätigkeiten der Organisation, festgelegt durch gesetzliche und statutarische Regelungen[44] , gewährleisten eine enge Zweckbindung.

5.4.2 Grundsatz der Datenminimierung

Die verarbeiteten personenbezogenen Daten sind dem Zweck angemessen, erheblich und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt.

Der Grundsatz der Datenminimierung und das Prinzip Datenschutz durch Technikgestaltung gem Art 25 DSGVO („Privacy by Design“) wurden in der Gestaltung der App von vorn herein berücksichtigt. Dies äußert sich wie folgt:

- Bereits die Architektur der App ist anhand von Privacy by Design und mit dem Ziel der Datenminimierung gestaltet (Privacy by Architecture):
    - Es wird keine zentrale Kontaktdatenbank aller App-NutzerInnen aufgebaut, sondern die Kontakte der einzelnen App-NutzerInnen untereinander werden dezentral nur auf ihren jeweiligen Endgeräten gespeichert, die unter ihrer eigenen Kontrolle stehen.
    - Die App fungiert somit als lokales Kontakt-Tagebuch jedes/jeder Einzelnen.
    - Der zentrale Server dient im Kern nur der pseudonymen Propagierung von Meldungen über Infektionsfälle
- Auch diese Meldungen sind mittels Verschlüsselung datensparsam implementiert, sodass nur jene Apps eine solche Meldung entschlüsseln können, die tatsächlich bereits einen Kontakt mit der jeweiligen infizierten Person registriert haben.
- Die Kontakte werden zu jedem Zeitpunkt ausschließlich pseudonym verarbeitet.
- Generell wird nur ein Minimum an personenbezogenen Daten der Betroffenen verarbeitet; insbesondere wurde entschieden, den Namen und weitere Identifikationsdaten auch im Fall einer Krankmeldung nicht zu erfassen.
- Auch im Fall einer Krankmeldung/Verdachtsmeldung wird daher nur propagiert, dass ein Kontakt mit einem Infizierten bestanden hat, und nicht, um wen es sich dabei handelt.

---

43 Siehe dazu *Kastelitz*, Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Art 5-11 DSGVO), in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 99 (101 ff mwN).

44 Siehe dazu Aufgabenzuweisung in Satzung des Österreichischen Roten Kreuzes: *“1.4. die Organisation und Durchführung der Gesundheits- und Sozialen Dienste, wie insbesondere der Hauskrankenpflege, Heimhilfe und Altenbetreuung,(Hinweis: 17. IC/1948/R55; 19. IC/1957/R28; 23. IC/1977/R17; 24. IC/1981/R22; 25. IC/1986/R29, 30).”*

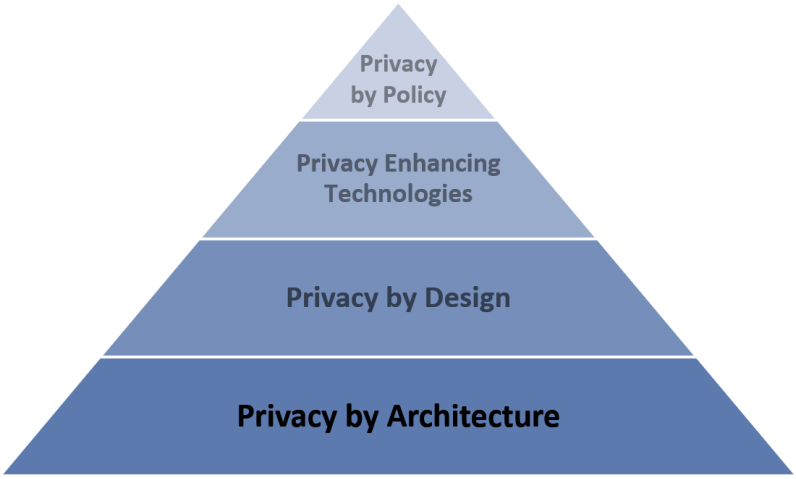


Abbildung: In der App werden nicht nur organisatorische Datenschutzmaßnahmen (Privacy by Policy) und Privacy Enhancing Technologies umgesetzt, wie z.B. Verschlüsselung, sondern der Datenschutz und die Datenminimierung wurden in der Gestaltung der App von Anfang an berücksichtigt (Privacy by Design), insbesondere auch bereits bei der Gestaltung der Architektur der App (Privacy by Architecture).[45]

5.4.3 Grundsatz der Speicherbegrenzung

Personenbezogene Daten werden nur so lange personenbezogen verarbeitet werden, wies es für die Zweckerreichung erforderlich ist. So weit wie möglich wird in den vorliegenden Verarbeitungsvorgängen auf Maßnahmen der Pseudonymisierung und Anonymisierung zurückgegriffen.

Gemäß Artikel 13 und 14 DSGVO informiert das Österreichische Rote Kreuz die Betroffenen über die Speicherdauer bzw. die Kriterien für die Festlegung der Speicherdauer.

Das ÖRK löscht oder anonymisiert die verarbeiteten personenbezogenen Daten, sobald sie für die Zwecke, für die sie erhoben oder verwendet wurden, nicht mehr erforderlich sind. In der Regel werden die personenbezogenen Daten für die Dauer der Nutzung nur in der App gespeichert. Diese können durch die Löschung der App jederzeit auf dem Endgerät durch die NutzerInnen selbst gelöscht werden. Daten auf dem Endgerät zum digitalen Handshake mit Intensivkontakten werden im Gerät jeweils nach 14 Tagen gelöscht. Solange Sie keine Verdachts- oder Infektionsmeldung abgeben, handelt es sich um anonyme Daten.

Sobald eine Krankmeldung/Verdachtsmeldung übermittelt wurde, erfolgt eine Speicherung für 30 Tage nach dem Absetzen dieser Meldung. Sofern und solange es zur Aufklärung einer rechtswidrigen bzw. missbräuchlichen Nutzung der App oder für die Rechtsverfolgung erforderlich ist und konkrete Anhaltspunkte für ein gesetzwidriges bzw. missbräuchliches Verhalten vorliegen, werden diese für einen Zeitraum von maximal drei Jahren nach dem Absetzen der Krankmeldung gespeichert. Bekannt gegebene private Kontaktdaten werden jedenfalls nach Ende der Epidemie gelöscht. Da ein Ende derzeit nicht absehbar ist, kann diesbezüglich aktuell kein konkreter Zeitpunkt der Löschung bekannt gegeben werden. Das Rote Kreuz ist Teil des österreichischen Krisenstabs und wird daher in enger Abstimmung mit den Behörden eine sachgerechte und transparente Entscheidung treffen und bekannt geben, wann der Zweck der Anwendung erfüllt ist.

---

45 Grafik entnommen aus *Hötzendorfer*, Zum Verhältnis von Recht und Technik: Rechtsdurchsetzung durch Technikgestaltung. In: *Hötzendorfer/Tschohl/Kummer* (Hrsg): International Trends in Legal Informatics, Festschrift for Erich Schweighofer, Editions Weblaw, Bern, 2020, 419–437, 435.

5.5 Angaben über die getroffenen bzw geplanten Maßnahmen zur Berücksichtigung der Rechte derbetroffenen Personen[46]

5.5.1 Vorbemerkung

Mit den im Rahmen der Stopp Corona-App verarbeiteten Daten, ausgenommen der Telefonnummer, die nur im Zuge einer Infektionsmeldung erhoben wird, können die Betroffenen durch das ÖRK nicht identifiziert werden. Daher können in Bezug auf diese Daten die Ansprüche aus den Artikeln 15 bis 20 nicht ohne weiteres erfüllt werden. Zur Erfüllung der Ansprüche aus den Artikeln 15 bis 20 wird es daher iSv Art 11 Abs 2 DSGVO in der Regel der Mitwirkung der betroffenen Person bedürfen.

5.5.2 Gewährleistung der Transparenz und Informationspflichten (Art 12-14)

Transparenz und genaue Information der Betroffenen über die Verarbeitungsvorgänge in Zusammenhang mit der App werden zum einen in der Datenschutzinformation sichergestellt, auf welche auch im Zuge der Einholung der Einwilligungserklärung explizit verwiesen wird. Die Datenschutzinformation ist über den Webauftritt des Verantwortlichen jederzeit abrufbar (zum Zeitpunkt der Erstellung des Berichts: https://www.roteskreuz.at/site/faq-app-stopp-corona/datenschutzinformation-zur-stopp-corona-app/), zudem werden oft gestellte Fragen der Betroffenen hinsichtlich der App auf einer speziell dafür eingerichteten Internetseite beantwortet (siehe https://www.roteskreuz.at/site/faq-app-stopp-corona/).

Bereits beim Start der App ("On-Boarding") erfolgen zudem erste Informationen betreffend die Funktionsweise der App:

Bei der Erteilung von Informationen an den Betroffenen gemäß Art 13 und 14 DSGVO, erfolgt eine Orientierung an den Leitlinien der Artikel 29 Datenschutzgruppe, WP 260 rev.01.

5.5.3 Recht auf Auskunft und Datenübertragbarkeit (Art 15, 20)

Recht auf Auskunft

Betroffene haben das Recht, vom ÖRK jederzeit auf Antrag eine Auskunft über die vom ÖRK verarbeiteten, sie betreffenden personenbezogenen Daten im Umfang des Art 15 DSGVO zu erhalten. Hierzu können sie einen Antrag postalisch oder per E-Mail an die angegebene Adresse stellen.

Recht auf Datenübertragbarkeit

Betroffene haben das Recht, vom ÖRK die sie betreffenden personenbezogenen Daten, die sie dem ÖRK bereitgestellt haben, in einem strukturierten, gängigen, maschinenlesbaren Format nach Maßgabe des Art 20 DSGVO zu erhalten. Für die Wahrnehmung dieses Rechtes wurden in der Datenschutzinformation mehrere Kontaktmöglichkeiten angegeben.

[46] Eine Dokumentation, wie die Betroffenenrechte erfüllt werden, sollte beim Verantwortlichen ohnehin vorliegen (Rechenschaftspflicht, Art 24 Abs 1). Diese kann hier übernommen werden.

5.5.4 Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung; Widerspruchsrecht (Art 16-19, Art 21)

Das Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung und das Widerspruchsrecht werden vollumfänglich gewährt.

Recht zur Berichtigung unrichtiger Daten

Betroffene haben das Recht, vom ÖRK die unverzügliche Berichtigung der sie betreffenden personenbezogenen Daten zu verlangen, sofern diese unrichtig sein sollten. Für die Wahrnehmung dieses Rechtes wurden in der Datenschutzinformation mehrere Kontaktmöglichkeiten angegeben.

Recht auf Löschung

Betroffene haben das Recht, unter den in Art 17 DSGVO beschriebenen Voraussetzungen vom ÖRK die Löschung der sie betreffenden personenbezogenen Daten zu verlangen. Diese Voraussetzungen sehen insbesondere ein Löschungsrecht vor, wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, sowie in Fällen der unrechtmäßigen Verarbeitung; auch wenn Betroffene ihre Einwilligung widerrufen und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt, besteht ein Recht auf Löschung. Für die Wahrnehmung dieses Rechtes wurden in der Datenschutzinformation mehrere Kontaktmöglichkeiten angegeben.

Recht auf Einschränkung der Verarbeitung

Betroffene haben das Recht, vom ÖRK die Einschränkung der Verarbeitung nach Maßgabe des Art 18 DSGVO zu verlangen. Dieses Recht besteht insbesondere, wenn die Richtigkeit der personenbezogenen Daten zwischen dem NutzerInnen und dem ÖRK umstritten ist, für die Dauer, welche die Überprüfung der Richtigkeit erfordert, sowie im Fall, dass der NutzerInnen bei einem bestehenden Recht auf Löschung anstelle der Löschung eine eingeschränkte Verarbeitung verlangt; ferner für den Fall, dass die Daten für die vom ÖRK verfolgten Zwecke nicht länger erforderlich sind, der NutzerInnen sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt. Für die Wahrnehmung dieses Rechtes wurden in der Datenschutzinformation mehrere Kontaktmöglichkeiten angegeben.

Recht auf Widerspruch

Das ÖRK verarbeitet private Kontaktdaten der Betroffenen auf Grundlage berechtigter Interessen gemäß Art 6 Abs 1 lit f und Art 9 Abs 2 lit f DSGVO. Das berechtigte Interesse liegt einerseits in der Reduzierung von Gesundheitsrisiken der Intensiv-Kontaktpersonen (berechtigtes Interesse) und andererseits allgemein in der Eindämmung der Infektionsverbreitung (berechtigtes Interesse der Allgemeinheit). Die Bereitstellung der Kontaktdaten (Telefonnummer) erfolgt auf freiwilliger Basis. Es bestehen für r Betroffene keine Konsequenzen für den Fall, dass sie diese nicht bereitstellen wollen. Allerdings können Betroffene diesfalls unter Umständen nicht zeitnah über Verdachtsfälle oder Infektionen ihrer Intensiv-Kontakte sowie über behördlich angeordnete Maßnahmen informiert werden.

Nachdem Betroffene die Kontaktdaten bekannt gegeben haben, kommt ihnen auch im Zeitraum der 30 Tage geplanten Speicherung ein Widerspruchsrecht gemäß Art 21 Abs 1 DSGVO zu. Das bedeutet die Betroffenenkönnen der Datenverarbeitung unter Angabe einer Begründung widersprechen. Ein Widerspruch führt jedoch nur dann zur Unterlassung der Verarbeitung, wenn der Widerspruch durch besondere Gründe gerechtfertigt ist. Dann verarbeitet das Rote Kreuz die personenbezogenen Daten nicht mehr, es sei denn, das Rote Kreuz könnte zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten des Betroffenen überwiegen, oder die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Für die

Wahrnehmung dieses Rechtes wurden in der Datenschutzinformation mehrere Kontaktmöglichkeiten angegeben.

Beschwerderecht

Betroffene haben ferner das Recht, sich bei Beschwerden an die zuständige Aufsichtsbehörde zu wenden. Die zuständige Aufsichtsbehörde ist:

Österreichische Datenschutzbehörde (DSB), Barichgasse 40-42, A-1030 Wien
Telefon: +43 1 52 152-0, E-Mail: dsb@dsb.gv.at, Web: https://www.dsb.gv.at

Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck

Die Stopp Corona-App dient der Frühwarnung und Information von Betroffenen, die möglicherweise infiziert sind. Sie leistet damit einen Beitrag zur Eindämmung der Infektionsverbreitung durch Unterbrechung von Infektionsketten. Dadurch, dass die App-NutzerInnen selbstbestimmt entscheiden, ob sie sich beteiligen wollen, ob sie via digitalem Handshake einen bestimmten Kontakt in die App eintragen wollen und ob sie Kontakte in weiterer Folge ggf über ihre eigene Infektion informieren wollen, behalten die Betroffenen die Kontrolle über die Verarbeitung ihrer personenbezogenen Daten und den Verständigungsprozess. Sie können damit einen aktiven Beitrag zur Eindämmung der Pandemie leisten.

Wie bereits dargestellt, wurde die App gesamtheitlich nach dem Grundsatz der Datenminimierung und dem Prinzip Datenschutz durch Technikgestaltung gestaltet. Dies äußert sich bereits in der Architektur der App, die eine dezentrale Speicherung die Kontakte der einzelnen App-NutzerInnen untereinander auf ihren jeweiligen Endgeräten vorsieht, und nicht etwa eine zentrale Kontaktdatenbank. Die Nutzung der App als Kontakttagebuch erfolgt anonym, die Meldung von Infektionsfällen erfolgt pseudonym und ebenfalls möglichst datensparsam. Der zentrale Server dient der pseudonymen Propagierung von Meldungen über Infektionsfälle und verarbeitet somit ebenfalls so wenige Daten wie möglich. Auch im Fall einer Krankmeldung wird nur an tatsächlich dokumentierte Kontaktpersonen gemeldet, dass ein Kontakt mit einem Infizierten bestanden hat. Dabei wird nicht gemeldet, um wen es sich dabei handelt. Anders als Systeme in anderen Staaten (z.B. Israel[47], Litauen[48], Polen[49]) setzt dieses System somit bewusst auf Freiwilligkeit, Selbstbestimmtheit und Datenminimierung. In Bezug auf die verfolgten Zwecke und deren enorme gesellschaftliche Bedeutung erscheint diese Form der Implementierung einer solchen App daher als notwendig und verhältnismäßig.

5.5.5 Angaben über die Einhaltung der Vorgaben der Datenübermittlung an Drittländer (oder internationale Organisationen)

Daten werden auch in Staaten außerhalb des Europäischen Wirtschaftsraumes (EWR) verarbeitet. Dies betrifft den oben genannten (Sub-)Auftragsverarbeiter Microsoft

Für die USA hat die Europäische Kommission mit Beschluss vom 12.7.2016 die Entscheidung getroffen, dass unter den Regelungen des EU-U.S.-Privacy Shields ein angemessenes Datenschutzniveau existiert (Angemessenheitsbeschluss, Art 45 Abs. 3 DSGVO). Microsoft ist ein nach dem EU-U.S.-Privacy Shield zertifiziertes Unternehmen.

47 https://www.heise.de/newsticker/meldung/Coronavirus-Oesterreich-und-Israel-setzen-auf-Handy-Tracking-4684339.html (zuletzt abgerufen am 08.04.2020).

48 https://www.spiegel.de/netzwelt/web/coronavirus-litauen-veroeffentlicht-bewegungsprofile-von-infizierten-a-58c16303-4616-4e05-91bc-10ac2b5659e6 (zuletzt abgerufen am 08.04.2020).

49 https://orf.at/stories/3158746/ (zuletzt abgerufen am 08.04.2020).

Der Europäische Gerichtshof hat am 16. Juli 2020 mit dem Urteil EuGH C-311/18 das „EU-US-Privacy-Shield“ für unwirksam erklärt. Das Urteil kennt keine Übergangsfrist.

In seinem Urteil prüfte das Gericht auch die Gültigkeit der Entscheidung 2010/87/EG der Europäischen Kommission über Standardvertragsklauseln (Standard Contractual Clauses, "SCC") und hielt diese für gültig. Datenübermittlungen in die Microsoft Azure Cloud sind derzeit durch Standardvertragsklauseln gedeckt.[50]

Allerdings weist der Gerichtshof insbesondere darauf hin, dass der Beschluss 2010/87/EG dem Datenexporteur und dem Empfänger der Daten (dem "Datenimporteur") die Verpflichtung auferlegt, vor jeder Übermittlung unter Berücksichtigung der Umstände der Übermittlung zu prüfen, ob dieses Schutzniveau in dem betreffenden Drittland eingehalten wird, und dass der Datenimporteur verpflichtet ist, den Datenexporteur über die Unfähigkeit zu informieren, die Standarddatenschutzklauseln und erforderlichenfalls zusätzliche Maßnahmen zu den durch diese Klauseln gebotenen zu erfüllen. Die Zulässigkeit der Übermittlung personenbezogener Daten in die USA auf der Basis von SCC hängt vom Ergebnis der Beurteilung im Einzelfall ab, wobei die Umstände der Übermittlung und zusätzlich ergriffene Maßnahmen, zu berücksichtigen sind.

In diesem Zusammenhang ist darauf hinzuweisen, dass aufgrund der vorgenommenen Verschlüsselung der Daten eine Identifizierung von betroffenen Personen durch die Auftragsverarbeiter nicht vorgenommen werden kann. Solche Informationen sind auch nicht aus dem Verarbeitungskontext ableitbar.

Die Schlüssel (TEK) jener Nutzer, die eine Infektion melden, werden auf dem Backend hinterlegt. Jede App holt einmal pro Tag die Liste aller Schlüssel von gemeldeten Infektionen vom Server ab. Diese Liste wird dann lokal auf dem Endgerät abgeglichen mit dem Schlüssel (TEK) der Intensivkontakte eines Nutzers. Sobald es eine Übereinstimmung gibt, erhält der Nutzer die Warnung.

5.5.6 Angaben über Datenübermittlungen innerhalb des EWR

- An die jeweilige Bezirksverwaltungsbehörde gemäß § 5 Abs 3 Epidemiegesetz 1950:

Auf Verlangen einer Bezirksverwaltungsbehörde besteht für den Verantwortlichen eine gesetzliche Pflicht zur Auskunftserteilung über Verdachtsfälle und Infektionen (und somit der Datenübermittlung) nach § 5 Abs 3 Epidemiegesetz 1950. Die Gesundheitsbehörden dürfen nach § 4 Abs 4 Epidemiegesetz 1950 jedenfalls folgende Datenkategorien von Erkrankten verarbeiten: Daten zur Identifikation von Erkrankten (Name, Geschlecht, Geburtsdatum, Sozialversicherungsnummer und bereichsspezifisches Personenkennzeichen gemäß § 9 EGovG), die für die anzeigepflichtige Krankheit relevanten klinischen Daten (Vorgeschichte und Krankheitsverlauf) und Labordaten, Daten zum Umfeld des Erkrankten, soweit sie in Bezug zur anzeigepflichtigen Erkrankung stehen, und Daten zu den getroffenen Vorkehrungsmaßnahmen. Zum Schutz der Daten sind in § 4 Epidemiegesetz 1950 Sicherheitsvorgaben normiert, die die Gesundheitsbehörden einzuhalten haben. Auch wenn eine solche Übermittlung von Daten (Telefonnummer) durch das Rote Kreuz an die zuständige Bezirksverwaltungsbehörde nicht beabsichtigt und auch technisch nicht implementiert ist, könnte das Rote Kreuz unter Umständen zur Herausgabe der Telefonnummer gezwungen werden. Sollte ein solcher Fall eintreten, ist die Rechtsgrundlage Art 6 Abs 1 lit c iVm Art 9 Abs 2 lit i DSGVO.

[50] https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-eu-model-clauses?view=o365-worldwide. (abgerufen am 04.08.2020).

5.6 Einholung des Standpunkts betroffener Personen (Art 35 Abs 9) oder ihrer Vertreter zu der beabsichtigten Verarbeitung

Aufgrund der großen Anzahl der möglichen App-NutzerInnen ist eine Einholung des Standpunktes aller künftigen Betroffenen im Vorfeld nur im Hinblick auf möglichst repräsentative Stichproben sinnvoll.

Der Standpunkt der Betroffenen wurde daher mittels einer Umfrage (Stichprobe 13 Personen, in der alle Altersgruppen vertreten waren) eingeholt. Die Ergebnisse der Umfrage liegen im Anhang bei. Eine größere Stichprobe war aufgrund der Dringlichkeit der Angelegenheit im Lichte der COVID-19-Pandemie nicht möglich. Zusätzlich wurden in den Sozialen Medien Reaktionen auf die öffentliche Ankündigung der App gesichtet und dort geäußerte Standpunkte berücksichtigt, wie zB das Risiko, dass sich Personen durch sozialen Druck dazu gedrängt fühlen könnten, die App zu verwenden und ihre Kontakte aufzuzeichnen. Relevante Bedenken der Betroffenen, auch aus dem öffentlichen Diskurs im Zuge der Ankündigung, wurden bei der Risikobewertung und den Maßnahmen der Risikominimierung entsprechend adressiert.

Nach Veröffentlichung der ersten Version der App wurden die öffentliche Debatte und die Bewertungen der App etc. detailliert verfolgt und dort geäußerte Standpunkte von Betroffenen aufgenommen und evaluiert.

Der häufigste geäußerte Kritikpunkt der Nutzer in den Stopp Corona-App Rezensionen innerhalb des Google Playstores war, dass der digitale Handshake manuell durchgeführt werden müsse und die App sohin unpraktikabel wäre. Diesem Kritikpunkt wurde bereits in vergangenen Releases durch die erweiterte Funktionalität Rechnung getragen. Im Rahmen des Release 2.0 werden die digitalen Handshakes künftig gänzlich automatisiert erfolgen, sofern die Nutzer die entsprechenden Funktionen freigeben.

6 Risikobeurteilung in Anlehnung an ISO 31000:2009, Kapitel 5 (Risk Assessment)[51]

6.1 Risikoidentifikation

Beschreibung von Risikoszenarien und daraus resultierender potenzieller Folgen. Es ist darauf hinzuweisen, dass die Risiken für die Rechte und Freiheiten von natürlichen Personen gemeint sind.

Folgende Fragen wurden im Zuge der Risikobehandlung abgearbeitet:

Im Zuge der Datenschutz-Folgenabschätzung wurden viele Fragen in dieser Liste vom Roten Kreuz, Accenture und dem Research Institute bearbeitet. Nachfolgend wird ein Auszug wiedergegeben, soweit die Fragen und deren Beantwortung für die Risikobehandlung relevant waren.[52]

Nr	Frage / Anmerkung	Antworten
Zur Systembeschreibung		

[51] Siehe dazu insb auch ErwGr 75 bis 78, 90. Die Risikobeurteilung kann hier nur schematisch wiedergegeben werden. Siehe dazu zB ISO 31000:2009 sowie eine Vielzahl weiterer Risikobeurteilungsmethoden.

[52] Seitenangaben in der nachfolgenden Tabelle beziehen sich auf eine ältere Entwurfsversion dieses Berichts.

Nr	Frage / Anmerkung	Antworten
S2	In der Systembeschreibung ist die Durchführung eines Handshakes zwischen zwei Endgeräten dargestellt, ohne auf den näheren Übertragungsweg bzw. die Funktionsweise dieses Datenaustausches einzugehen. In den rechtlichen Ausführungen (S. 26 der DSFA) ist diesbezüglich eine Standortdaten-Erfassung, eine Nutzung von QR-Codes oder aber eine Angabe von E-Mail-Adressen angeführt. Eine in der Systembeschreibung dargestellte Bildschirmmaske (S. 8) zeigt wiederum einen Dialog „Ihre Umgebung wird abgesucht“. Bitte um Information, auf welchem Weg bzw. welchen technischen Wegen ein solcher Handshake mit der App durchgeführt werden kann.	Die Erfassung der Endgeräte in der Umgebung erfolgt über die Nutzung von Google Nearby. Google Nearby nutzt die Sensoren des Mobiltelefons. und Bluetooth, um nahe Endgeräte zu finden. Google Nearby ist kein Auftragsverarbeiter von Accenture, sondern eine Funktion am Smartphone. Die betroffenen Personen entscheiden selbst, ob sie die Funktion zulassen oder nicht. Zur Beschreibung s. https://support.google.com/accounts/answer/6260286?hl=de Mit dem automatischen Handshake wurde auch p2pKIT als Auftragsverarbeiter eingeführt - siehe dazu unten.
S3	Im Zusammenhang mit der Speicherung von personenbezogenen Daten in der Azure Cloud wird in der Systembeschreibung (S. 15) unter dem Titel „Serverseitige Verschlüsselung“ darauf verwiesen, dass die Funktion "Encryption at rest" standardmäßig aktiv sei. Diese gewährleiste unter Verwendung eines symmetrischen Schlüssels einen Schutz vor unbefugten Datenzugriffen. Wie wird sichergestellt, dass bei einem allfälligen unberechtigten Zugriff auf die Daten nicht auch auf den symmetrischen Schlüssel unberechtigt zugegriffen wird?	In Azure, the default setting for transparent data encryption is that the database encryption key is protected by a built-in server certificate. The built-in server certificate is unique for each server and the encryption algorithm used is AES 256. If a database is in a geo-replication relationship, both the primary and geo-secondary database are protected by the primary database's parent server key. If two databases are connected to the same server, they also share the same built-in certificate. Microsoft automatically rotates these certificates in compliance with the internal security policy and the root

Nr	Frage / Anmerkung	Antworten
		key is protected by a Microsoft internal secret store.
S4	Anonymisierung von Statistikdaten: Aus den rechtlichen Ausführungen (S. 26) geht hervor, dass für statistische Zwecke eine Anonymisierung durch Löschung der UUID sowie der übermittelten Angaben zur Person (Name, Adresse etc.) erreicht werden soll. Aus den technischen Ausführungen zur API (S. 19) geht hervor, dass zu Statistikdaten Zeitstempel mit der Granularität Millisekunden gespeichert werden. Es erscheint fraglich, ob bei dieser Genauigkeit der Zeitangaben eine Zuordnung des Statistikwertes zu den Originaldaten tatsächlich wirksam unterbunden werden kann. Diesbezüglich wären nähere Ausführungen zu den gewählten Anonymisierungsschritten in der Systembeschreibung wünschenswert. Diese enthält dzt. keine näheren Angaben dazu.	Die Auswertungen dienen dazu, die Anzahl der Infizierten und die Anzahl ihrer Kontakte nachverfolgen zu können -> man will wissen, ob die Anzahl der Erkrankten und deren Kontakte sinken. Nach bisherigem Planungsstand werden im Backend ausschließlich die Nutzer IDs der App (nicht Geräte IDs) gespeichert. Bei der Krankmeldung wird zusätzlich die Handy Nummer erfasst für einen begrenzten Zeitraum. Die Auswertungen dienen dazu, die Anzahl der Infizierten und die Anzahl ihrer Kontakte nachverfolgen zu können. Die Zahlen werden voraussichtlich via PowerBI aggregiert werden für quantitative Statistik. Es sind keine Zeitstempel im Millisekundenbereich in den Auswertungen enthalten. Die Statistiken sind wie gesagt aggregierte Daten.
S5	Die Angaben zu den betroffenen Datenarten umfassen unter anderem das Geburtsdatum der jeweiligen Person. Zu welchem Zweck ist der genaue Geburtstag der Person erforderlich? Wäre das Jahr nicht ausreichend? In der Risikobewertung wird auf das Risiko des Identitätsdiebstahls eingegangen. Dieses könnte durch Datenreduktion auf das Geburtsjahr weiter verringert werden.	Mittlerweile ist nur noch die Angabe der Telefonnummer gefordert. Das Geburtsdatum wird bei der Krankmeldung nicht erfasst. Dass keine Daten von Kindern verarbeitet werden wird sichergestellt darüber, dass die Nutzungsbedingung für die App ist, mindestens 17 Jahre alt zu sein.
S6	In der DSFA werden unter "Betroffene Daten" (S. 12) "Standortdaten" angeführt. Bei welcher	Standortdaten werden nicht gespeichert. Zur Erkennung der

Nr	Frage / Anmerkung	Antworten
	Gelegenheit und zu welchem Zweck werden diese erfasst? Wie werden diese weiter verarbeitet? Um welche Art von Standortdaten handelt es sich (GPS-Positionen, ...)?	Personen in der Umgebung, um damit der Kontaktaufzeichnung im Endgerät der NutzerInnen, wird Google Nearby genutzt. Diese Daten werden allerdings nicht gespeichert.
S7	Im Rahmen der Selbstdiagnose werden Daten zum Gesundheitsempfinden der jeweiligen Person abgefragt und bewertet. Werden diese Daten an das Backend übertragen? Wenn ja: Erfolgt dies nur bei Vorliegen der Corona-Symptome oder betrifft dies jeden Selbsttest?	Die Antworten auf die Selbstdiagnosen erfolgen nicht persistent auf dem Endgerät der NutzerInnen. Die Daten werden nicht an das Backend übertragen. Eine Übertragung des Krankheitsstatus erfolgt erst bei der aktiven Krankmeldung der betroffenen Person/der App-Nutzerin. Dabei muss dann auch die Telefonnummer angegeben werden, die ans Backend übertragen wird. Weitere Daten werden nicht erfasst.
S8	Im Falle einer Infektionsmeldung werden an alle NutzerInnen der App verschlüsselte Infektionsnachrichten versandt, die nur von den Intensivkontakten der jeweiligen Person entschlüsselt werden können. Was ist der Dateninhalt dieser verschlüsselten Nachrichten?	Der Inhalt der verschlüsselten Nachricht ist die App-ID der NutzerInnen, die sich als krank gemeldet haben. Nur die Personen, die einen Kontakt mit einer als krank gemeldeten Person aufgezeichnet haben, können die ID entschlüsseln. Dies löst das Anzeigen der Warnmeldung auf dem Endgerät der NutzerInnen aus. Der Dateninhalt der Nachricht ist: ·Message UUID (Unique pro Message) ·Timestamp des Kontakts in 1h Auflösung ·Message type (z.Z. nur Ärztliche Diagnose)
S9	Die Infektionsnachrichten einer Person an die jeweiligen Intensivkontakte werden mit deren	Nein.

Nr	Frage / Anmerkung	Antworten
	öffentlichen Schlüsseln verschlüsselt, die im Rahmen des Handshakes erhalten wurden. Werden diese Infektionsnachrichten auch mit dem privaten Schlüssel der Person signiert?	Begründung: Auch der authentifizierte NutzerInnen selbst ist in der Lage, eine Falschmeldung abzugeben. Dieser Angriffsvektor ist viel größer als jener betreffend die Authentizität. Mit der Angabe der Mobiltelefonnummer mit der Krankmeldung, wurde ein datensparsamer Weg gewählt, dem zu begegnen
S10	An mehreren Stellen der DSFA wird erwähnt, dass über die App eine anonyme Information der Intensivkontakte einer Person erfolgt. Welche Anhaltspunkte sprechen dafür, dass insbesondere angesichts der derzeit geltenden Regeln zur sozialen Distanz tatsächlich keine Rückschlüsse auf die Identität der erkrankten Person gezogen werden können? Sofern diesbezüglich Unsicherheiten betreffend die Wirksamkeit der Anonymisierung bestehen sollte stattdessen der passendere Begriff der Pseudonymisierung verwendet werden, um allfälligen Missverständnissen vorzubeugen.	Diese Kritik trifft zu: Es wird die Uhrzeit angegeben, zu der man in Kontakt mit einer erkrankten Person war. Der Empfänger einer Meldung kann aus seinem Gedächtnis daher möglicherweise rückschließen, wer die infizierte Person ist. Das ist in der DSFA auch beschrieben. Mit Release 2 wird hier der Begriff anonymisiert durch pseudonymisiert ersetzt - begleitet durch eine gezielte Information zur sachlichen Verwendung dieser Begriffe und deren rechtlicher Bedeutung.
S11	Bei der Installation der App wird ein Unique Identifyer erzeugt. An mehreren Stellen der DSFA sind weiters eine oder unterschiedliche UUIDs erwähnt. Handelt es sich bei diesem Unique Identifyer oder anderen verwendeten Identifikationsnummern um die sogenannte Device-ID, die von Google und Apple den jeweiligen Endgeräten weltweit eindeutig zugeordnet werden? Wenn ja, in welchem Zusammenhang und für welche Zwecke wird diese verarbeitet?	Die Device ID wird im Rahmen der App nicht verwendet. Es werden folgende unabhängig voneinander generierte Random UUIDs verwendet: • Device UUID konstant über alle Tracking Calls • Message UUID Unique pro Message Device-IDs von Google und Apple werden von uns nicht direkt übertragen.

Nr	Frage / Anmerkung	Antworten
		Möglicherweise werden von Firebase Cloud Messaging intern weitere Identifier verwendet.
S12	Firebase Cloud Messaging: Welchen Inhalt haben die versendeten Push-Nachrichten? Handelt es sich dabei um eine Information über das Vorhandensein neuer Infektionsnachrichten, damit diese von der App abgeholt werden, oder werden die Infektionsnachrichten selbst gepusht?	Da das Backend nicht weiß, wer mit wem Kontakt hatte, werden alle App-NutzerInnen informiert, dass eine neue Krankmeldung vorliegt. Die Clients downloaden dann die relevanten Nachrichten. Für sie ist nur eine Nachricht relevant, wenn sie die ID des Kontaktes entschlüsseln können; das ist das Indiz dafür, dass sie in Kontakt waren.
Zu den rechtlichen Aspekten		
R1	In der DSFA werden die Begriffe Backend und Cloud synonym verwendet. Gemeint ist damit jeweils die Microsoft Azure Cloud mit Rechenzentrum in Frankfurt am Main. An diese Cloud werden durch die App Gesundheitsdaten iSd Art 9 DSGVO übermittelt. Manche Cloud-Anbieter schließen die Verarbeitung von Gesundheitsdaten in ihren Geschäfts- und Vertragsbedingungen ausdrücklich aus. Bitte um Information, ob geprüft wurde, ob dies bei der genutzten Cloud ebenfalls der Fall ist, und zu welchem Ergebnis diese Prüfung gelangt ist.	Die Prüfung seitens Accenture hat ergeben, dass die Verarbeitung von Gesundheitsdaten in der Azure Cloud rechtlich durch die Vertragsbedingungen nicht ausgeschlossen ist.
R2	Im Rahmen der Nutzung der Azure Cloud kann durch den Kunden gewählt werden, in welchen Rechenzentren bzw. Regionen die Daten gespeichert bzw. verarbeitet werden sollen. Bitte um Information welche Festlegungen für die gegenständliche Cloud getroffen wurden.	Wenn man eine Ressource anlegt, wählt man, welches Rechenzentrum genutzt wird. In diesem Fall wurde die Region EU West ausgewählt.
R3	Im Rahmen der Azure Cloud setzt Microsoft zahlreiche externe Dienstleister aus Drittstaaten ein. Bitte um Information, ob geprüft wurde auf welche Daten der App bzw. des Gesamtsystems	Der Cloud-Anbieter Microsoft erhält grundsätzlich keinen Zugriff auf die gespeicherten Daten. Der gesamte Datenbankserver wird verschlüsselt

Nr	Frage / Anmerkung	Antworten
	derartige Dienstleister zugreifen können und inwieweit dies mit den Anforderungen der DSGVO in Einklang steht. Alternativ bietet Microsoft auch die Möglichkeit an, Wartungszugriffe in jedem Einzelfall ausdrücklich durch den Kunden freigeben zu lassen. Bitte auch um Information darüber, ob diese Option gewählt wurde.	betrieben. Der ausgewählte Verschlüsselungsmodus ist RSA HSM 2048. Microsoft MitarbeiterInnen (und damit ihre potenziellen Dienstleister) haben auf die virtuellen Maschinen keinen direkten Zugriff bzw. keine Anmeldemöglichkeit.
R6	Bezüglich der eingesetzten Auftragsverarbeiter sollten in der DSFA Angaben zu den Rechtsgrundlagen derer Tätigkeit ergänzt werden (Vertragsstrukturen: Verantwortlicher – Auftragsverarbeiter – Sub-Auftragsverarbeiter, Bestehen von Auftragsverarbeitungsvereinbarungen zwischen diesen Parteien, ggf. Anwendbarkeit von Privacy Shield oder anderen Rechtsgrundlagen des Datenexports, …)	Ein AVV zwischen Accenture und dem ÖRK wurde abgeschlossen. Das ÖRK hat einen AVV mit Google betreffend den Einsatz von Firebase Cloud Messaging abgeschlossen. Es besteht eine AVV zwischen Accenture und Microsoft betreffend die Azure-Cloud. Allfällige Drittlandsübermittlungen in die USA sind durch das Privacy-Shield-Abkommen abgedeckt. Näheres ist in der Datenschutz-Folgenabschätzung dokumentiert.
R7	Bitte um Information, in welchem Verhältnis die gegenständliche Datenverarbeitung zu den Bestimmungen des Gesundheitstelematikgesetzes steht. Falls dieses anwendbar ist bitte um kurze Darstellung auf welche Art die entsprechenden Anforderungen erfüllt werden.	ÖRK ist als Betreiber der App (derzeit mit Release 1) KEIN Gesundheitsdiensteanbieter Die Verarbeitung von Gesundheitsdaten wird auf die Einwilligung (Art 9 Abs 2 lit a DSGVO) gestützt und bewusst nicht auf die Vertragserfüllung als GDA nach Art 9 Abs 2 lit h DSGVO - das wurde relativ ausführlich diskutiert. Dies gilt jedenfalls für die Release 1, bei der im Zuge der Folgenabschätzung die use-cases eingeschränkt wurden. Das Rote

Nr	Frage / Anmerkung	Antworten
		Kreuz wird also nicht als GDA tätig und agiert auch rechtlich - im Moment mit Release 1 - nicht als GDA, weshalb das GTelG nicht anwendbar ist. Erst mit Release 2 ist geplant, die Funktionalitäten so auszubauen, dass im Roten Kreuz im Hintergrund auch die medizinischen/organisatorischen Kapazitäten aufgebaut werden. Dazu würde die Anwendbarkeit des GTelG neu geprüft. Näheres ist in der Datenschutz-Folgenabschätzung dokumentiert.
R8	Bitte um Information, zu welchem Zweck die personenbezogenen Daten (Name, Adresse, …) einer Infektionsmeldung verarbeitet werden. Werden diese Daten an Dritte übermittelt? Wenn ja: an wen (Gesundheitsbehörden, etc) und auf Basis welcher Rechtsgrundlagen erfolgt diese Übermittlung? Wenn nein: zu welchen legitimen Zwecken des Auftraggebers werden die Daten verarbeitet? Dies geht aus den Ausführungen der DSFA nicht schlüssig hervor.	Dies wurde nun eingeschränkt und in der DSFA näher ausgeführt. Kurzfassung: Es wird nur die Telefonnummer erhoben und diese dient der Missbrauchsbekämpfung. Näheres siehe insbesondere in der Datenschutz-Information.
R9	Rechtsgrundlagen: Art 9 (2) lit a (Einwilligung): Auf welche Weise wird diese eingeholt und dokumentiert? Wie erfolgt die vorherige Information der NutzerInnen über die Umstände der Verarbeitung? In welcher Weise kann die Einwilligung widerrufen werden? Auf welche Verarbeitungsschritte ist die Einwilligung anwendbar? Wie wirkt sich die Kopplung der Einwilligung an die Vertragserfüllung aus, wenn die Einwilligung widerrufen wird?	Dies ist nunmehr in der Datenschutz-Information und in der DSFA dokumentiert.
R10	Die Datenschutzerklärung enthält keinen klar erkennbaren Hinweis auf die Verarbeitung auf	Dies wurde aktualisiert und ist nunmehr in der Datenschutz-

Nr	Frage / Anmerkung	Antworten
	Basis einer Einwilligung gem. Art 9 Abs 2 lit a. Weiters ist eine entsprechende Widerrufsbelehrung nicht enthalten. Bitte um Übermittlung des konkreten Einwilligungstextes sowie einer Beschreibung der Art der Einholung dieser Einwilligung und insbesondere der eindeutigen bestätigenden Handlung der NutzerInnen.	Information und in der DSFA dokumentiert.
R11	Hinsichtlich der Verarbeitung von Daten auf Grundlage des Art 9 Abs 2 lit f DSGVO (Geltendmachung von Rechtsansprüchen) sollte näher ausgeführt werden, welche Rechtsansprüche des Verantwortlichen durch allfällige Falschmeldungen ggf. entstehen könnten. Ebenso sollten die NutzerInnen präventiv auf die möglichen Rechtsfolgen von Falschmeldungen hingewiesen werden. Datenschutzerklärung: Im Punkt "Weitergabe von Daten" ist iZm der missbräuchlichen Nutzung der App eine Weitergabe von Daten an geschädigte Dritte vorgesehen. (Warum) Ist es als rechtlich gesichert anzusehen, dass Art 9-Daten für Rechtsansprüche Dritter verarbeitet und übermittelt werden dürfen und sich dies nicht nur auf Rechtsansprüche des Verantwortlichen bezieht?	Dies wurde aktualisiert und ist nunmehr in der Datenschutz-Information und in der DSFA dokumentiert.
R12	Die Datenschutzerklärung gibt die Speicherdauer von Krankmeldungen mit 30 Tagen an. Die DSFA enthält dazu derzeit keine Angaben. Bitte um Erläuterung der Gründe für den gewählten Zeitraum und eine Bewertung im Sinne der Verpflichtung zur Speicherbegrenzung in der DSFA.	30-Tage-Speicherung der Krankmeldungstransaktion um in diesem Zeitraum evaluieren zu können ob ein Missbrauchsfall von den NutzerInnen ausgeht. Ist in der Datenschutz-Information vermerkt.
R13	Punkt 3.1 der DSFA enthält eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung. Deren letzter Absatz lautet *„In Anbetracht von in anderen Staaten (Israel, Litauen, Polen) aktuell eingesetzten Überwachungs- bzw.*	Wurde nunmehr in der DSFA umgesetzt.

Nr	Frage / Anmerkung	Antworten
	Kontrolltechnologien, ist ein System das bewusst auf Selbstbestimmtheit, freiwillige Nutzung und eigenverantwortlicher Steuerung durch die Nutzer abzielt, in Bezug auf den verfolgten Zweck/die verfolgten Zwecke als verhältnismäßig und notwendig zu betrachten.“ In Anbetracht der geplanten Veröffentlichung des Berichts wird angeregt, die Argumentationskette zur Begründung der Verhältnismäßigkeit und Notwendigkeit des Systems evtl. nochmals zu überdenken. Ausführungen zur datenschonenden Verarbeitung, geringer Speicherdauer, strikter Zweckbindung, etc. wären im Rahmen der öffentlichen Kommunikation evtl. besser geeignet das Vertrauen der Bevölkerung in die Wahrung des Grundrechts auf Datenschutz zu gewinnen.	

Für die geplanten Verarbeitungsvorgänge lassen sich unterschiedliche Risiken identifizieren.

Zu den Risiken wird in ErwGr 75 der DSGVO Folgendes ausgeführt:

> „Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem **physischen, materiellen oder immateriellen Schaden** führen könnte, insbesondere wenn die Verarbeitung zu einer **Diskriminierung**, einem **Identitätsdiebstahl oder -betrug**, einem **finanziellen Verlust**, einer **Rufschädigung**, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen **erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen** führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn **personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet** werden, **wenn persönliche Aspekte bewertet werden**, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit**, persönliche Vorlieben oder Interessen**, die Zuverlässigkeit oder das **Verhalten**, den Aufenthaltsort oder Ortswechsel betreffen, **analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen**, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von **Kindern**, verarbeitet werden oder wenn die Verarbeitung eine **große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen** betrifft.“

Zu den möglichen physischen, materiellen oder immateriellen Schäden, die aus den geplanten Verarbeitungstätigkeiten folgen können, zählen insbesondere:

- **Rufschädigung**: Szenarien einer Rufschädigung sind denkbar, wenn bestimmte Informationen aus der Datenverarbeitung an unbefugte Personen geraten. Das Bekanntwerden des Umstands, dass eine Person infiziert ist/ sein könnte, kann für diesen Betroffenen nachteilige Folgen haben und zu einer rechtlich relevanten Rufschädigung führen, wenn dieser Umstand bekannt wird
- **Finanzieller Verlust**: Das Bekanntwerden einer (möglichen) Infektion, könnte, je nach beruflicher Tätigkeit, ggf den Verlust des Arbeitsplatzes zur Folge haben.
- **Kontrollverlust** bzgl. der personenbezogenen Daten des Betroffenen, ist denkbar, wenn kein Berechtigungskonzept besteht, beliebige Mitarbeiter des Roten Kreuzes Zugriff haben und die Datenbank gegen Angriffe unzureichend abgesichert ist.
- **Verlust der Vertraulichkeit:** Unberechtigte Personen könnten Zugriff auf die Daten der App-NutzerInnen erhalten. Dabei kann es sich entweder um unternehmensinterne Personen handeln (MitarbeiterInnen, oder aber um unberechtigte Zugriffe von außen, die Zugriff auf die Daten durch Hackerangriffe erhalten/erlangen).
- **Diskriminierung**: In Frage kommt eine Diskriminierung aufgrund der ausgewerteten Daten insbesondere aufgrund von Aspekten, die die gesundheitliche Lage betreffen (diese können analysiert oder prognostiziert werden, um persönliche Profile zu erstellen bzw. zu nutzen).Da es ein Aufgabengebiet des ÖRK ist, erkrankte Personen zu unterstützen, ist der Eintritt dieses Schadens nur dann möglich, wenn personenbezogene Daten der Betroffenen in die Hände von Unbefugten gelangen bzw. von Mitarbeitern missbräuchlich verwendet werden. Das Datenschutz-Management System stellt sicher, dass jeder Änderungsprozess einem organisatorisch abgesicherten Kontrollprozess unterliegt. Das Management ist dabei softwareunterstützt, sodass die Kontrollmechanismen im Rahmen der Freigabeprozesse technisch abgesichert sind.
  Identitätsdiebstahl oder -betrug: Es bestehen umfassende technisch-organisatorische Maßnahmen (verschlüsselte Verbindungen etc., siehe Anhang), die nicht nur einem (externen bzw. internen) Datenmissbrauch bzw. -diebstahl wirksam entgegenwirken (z.B. durch eine Firewall und abgestufte Berechtigungen). In einer Gesamtbetrachtung besteht kein hohes Risiko, dass jemand die Identität des Unterstützers annimmt und ein Missbrauch stattfindet. Aus der Sicht der Betroffenen liegt das Risiko eines Identitätsdiebstahls aber nicht ausschließlich in den Auswirkungen auf die vorliegende Anwendung begraben. Vielmehr geht es darum, dass in der vorliegenden Anwendung eine große Zahl an Informationen zu Personen vorliegen, die es einem böswilligen Täter ermöglichen würden, in Verbindung mit anderen Informationen und Tathandlungen einen schweren Identitätsdiebstahl zu begehen. Die besonders schwerwiegenden Cyberdelikte sind typischerweise komplexe, über längere Zeiträume verteilte und oft für sich genommen unscheinbare einzelne Angriffe, die in Summe schwere Schäden mit sich bringen können (sog. Advanced Persistent Threats, APT). In dieser Hinsicht ist der wichtigste und effektivste Grundsatz der Datenminimierung in der Umsetzung der vorliegenden Anwendung optimiert. Initial sowie bei jeder künftigen Ergänzung wird genau geprüft, ob ein Datum notwendig ist und die Pseudonymisierung optimiert ist. Dem Verlust der Datenverfügbarkeit wird durch die TOMs wirksam entgegengewirkt, es erfolgt u.a. ein regelmäßiges Backup der Daten.

- **Unbefugte Aufhebung der Pseudonymisierung:** Werden im Zusammenhang mit der geplanten Verarbeitungsvorgängen unzureichende technische und oder organisatorische Maßnahmen getroffen, könnte es zu einer unbefugten Aufhebung der Pseudonymisierung kommen.

- **Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile:** Es erfolgt keine Entscheidung die rechtliche Wirkung entfaltet oder den Betroffenen in ähnlicher Weise erheblich beeinträchtigt (siehe dazu oben).

Mögliche Gründe für diese Schäden sind:

- **Einschränkung der Rechte**: Es erfolgt keine Entscheidung, die den Betroffenen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

- **Verarbeitung von Daten besonders schutzbedürftiger Personen:** Erkrankte Personen sind als besonderes schutzbedürftige Personen zu betrachten.

- **Verarbeitung sensibler (besondere Kategorien personenbezogener) Daten:** Es erfolgt eine Verarbeitung von sensiblen Daten (siehe oben).

- **Profilerstellung (Bewertung persönlicher Aspekte):** Es erfolgt eine Profilerstellung auf Basis von sensiblen Daten (die jedoch nicht unter Artikel 22 DSGVO fällt).

- **Große Reichweite (große Datenmenge, große Anzahl Betroffener):** Eine große Reichweite liegt vor und bildet ein Kriterium für die Durchführung der vorliegenden Datenschutz-Folgenabschätzung.

Risiken für die Rechte und Freiheiten von natürlichen Personen

Hinzuweisen ist darauf, dass der Wortlaut des Art 35 Abs 1 DSGVO auf die Risiken für die Rechte und Freiheiten von **„natürlichen"** Personen abstellt, diese also nicht auf die von der Datenverarbeitung betroffenen Personen einschränkt. Daraus könnte der Schluss gezogen werden, dass bei der Beurteilung der mit der Datenverarbeitung verbundenen Risiken auch solche miteinbezogen werden müssen, die sich für Personen ergeben könnten, auf die sich die verarbeiteten Daten gar nicht beziehen. Da eine entsprechende Unterscheidung aber auch in Art 35 Abs 7 lit d DSGVO gemacht wird, ist von einem bewussten Abstellen auf „natürliche Personen" (und nicht von einem Redaktionsfehler) auszugehen.[53] Auch wenn die Leitlinien der *Artikel-29-Datenschutzgruppe* diesem scheinbar keine Bedeutung beimessen[54] und lediglich Risiken für „betroffene" Personen behandeln, sollen – gerade aufgrund der aktuellen angespannten Lage, nachfolgend sowohl die oben angeführten Risiken für betroffene Personen als auch Risiken für natürliche Personen (=die Bevölkerung) berücksichtigt werden.

Risiken des Konterkarierens des Social-distancing-Gedankens bzw. der gesetzlichen Maßnahmen

Aktuell sollte man so wenige Kontakte haben, dass man darüber den Überblick behält (siehe dazu auch Bedenken aus der Umfrage, „App bringt mir nichts, ich reduziere Kontakte sowieso"). Jede/r sollte sich prophylaktisch so verhalten, als wäre er infiziert, um seine Mitmenschen optimal zu schützen (nicht hinausgehen, Abstand halten etc.) Der Grundgedanke der App steht mit dem in gewissem Widerspruch.

Gerade bei jüngerer Personen ist es schwierig diese von der Notwendigkeit der social distancing Maßnahmen zu überzeugen (siehe dazu auch Bedenken aus der Umfrage, „Jüngere wollen nicht so viel am Handy sein, keine Angst vor Virus"). Die App könnte eine falsche Botschaft aussenden bzw. dazu führen, dass sich insbesondere jüngerer Personen noch sicherer fühlen und letztendlich die gesetzlichen Maßnahmen gegen die Ausbreitung konterkarieren.

Risiko der intransparenten Verarbeitung personenbezogener Daten durch unzureichend beschriebene Datenschutzinformationen der App

Aufgrund der Komplexität der datenschutzrechtlichen Materie in Kombination mit der hohen gesellschaftlichen Akzeptanz diverser Applikationen gegenüber besteht generell meist ein hohes Risiko der intransparenten Verarbeitung.

Risiken aus der Erstellung einer umfangreichen Datenbank mit sensiblen Daten, sozialer Interaktionen und Bewegungsprofilen

Es ist zu beachten, dass eine sehr große und damit auch kritische Datenbank aller Bewegungen und sozialen Interaktionen potenziell hunderttausender NutzerInnen aufgebaut, die nicht vollständig anonym, sondern und potenziell Personenbezogen ist und auch missbraucht werden könnte (siehe dazu auch Bedenken aus der Umfrage, „Anonymität kommt noch nicht genug raus" und "Behörden nutzen Corona-Krise aus um Daten zu sammeln").

Es erfolgt grundsätzlich keine Weiterleitung von Daten an Behörden, unter Umständen können Behörden aber nach dem Epidemiegesetz personenbezogene Daten über Erkrankungen anfordern. Folgendes wird den Nutzern im Rahmen der Datenschutz-Information hierzu mitgeteilt:

---

53 *Trieb* in *Knyrim*, DatKomm Art 35 DSGVO, Rz 2.

54 *Trieb* in *Knyrim*, DatKomm Art 35 DSGVO, Rz 2 mwN.

Missbrauch und Strafverfolgung

Wenn es zur Aufklärung einer rechtswidrigen bzw. missbräuchlichen Nutzung der App oder für die Rechtsverfolgung erforderlich ist, werden personenbezogene Daten an die Strafverfolgungsbehörden oder an österreichische Gerichte weitergeleitet. Dies geschieht jedoch nur, wenn Anhaltspunkte für ein gesetzwidriges bzw. missbräuchliches Verhalten vorliegen; in der Abwehr eines solchen Verhaltens liegt auch unser berechtigtes Interesse. Das Rote Kreuz stützt sich hierfür auf Art 6 Abs 1 lit f DSGVO iVm Art 9 Abs 2 lit f DSGVO.

Epidemiegesetz

Gemäß § 5 Abs. 3 Epidemiegesetz sind **auf Verlangen** einer Bezirksverwaltungsbehörde (https://www.help.gv.at/Portal.Node/hlpd/public/content/behoerden.html) alle Personen, wie insbesondere behandelnde Ärzte, Labors, Arbeitgeber, Familienangehörige und Personal von Gemeinschaftseinrichtungen, die zu den Erhebungen einen Beitrag leisten könnten, zur Auskunftserteilung verpflichtet. Auch wenn eine solche Übermittlung von Daten (hier kommt insbesondere die Telefonnummer in Betracht, sofern vorhanden) durch das Rote Kreuz an die zuständige Bezirksverwaltungsbehörde nicht beabsichtigt und auch technisch nicht implementiert ist, könnte das ÖRK unter Umständen zur Herausgabe dieser Daten gezwungen werden. Sollte ein solcher Fall auftreten, ist die Rechtsgrundlage für die Übermittlung Art 6 Abs. 1 lit c iVm Art 9 Abs. 2 lit i DSGVO.

Risiko, dass aus den Statistikdaten individuelle Bewegungsprofile abgeleitet werden

Es könnte versucht werden, aus ermittelten Statistikdaten individuelle Bewegungsprofile abzuleiten.

Risiko, dass Personen fälschlicherweise glauben, sie wären infiziert, weil sich jemand mutwillig fälschlicherweise als infiziert gemeldet hat

App-User könnten mutwillig Kontakte über eine COVID-19 Infektion verständigen, obwohl diese nicht vorliegt. Dieses Risiko kann insbesondere beim automatisierten Handshake (bei der vorher keine aktive Kontaktaufnahme mit dem anderen App-User erfolgt ist) bestehen.

Risiko, dass Personen fälschlicherweise glauben, sie wären infiziert, weil ihre Symptome den Symptomen des Fragebogens entsprechen

Die Symptome einer COVID-19 Erkrankung sind häufig schwer zuzuordnen, die häufigsten Symptome, mit denen die Betroffenen auffällig werden sind: Husten (55 Prozent), Fieber (39 Prozent), Schnupfen (28 Prozent), Halsschmerzen (23 Prozent), und Atemnot (drei Prozent).[55]

Derzeit befindet sich Österreich nicht nur in der Phase der abklingende Grippesaison, sondern auch in einer „starken" Allergiesaison, da die Änderungen des Klimawandels dazu einer stärkeren Birkenpollenbelastung als üblich geführt hat. Tlw. besteht hier eine ähnliche Symptomatik. Die bereits bekannten Allergien ist dies für den Betroffenen erklärbar, Allergien treten jedoch grundsätzlich irgendwann das erste Mal auf und es ist denkbar, dass Personen bei denen Allergien das erste Mal auftreten, vermuten an COVID-19 erkrankt zu sein.

[55] Siehe dazu etwa folgenden Beitrag unter https://www.diepresse.com/5792524/coronavirus-schnupfen-und-halsweh-bei-knapp-einem-drittel-auffallig#kommentare (zuletzt abgerufen am 08.04.2020).

Die Lenkung der Aufmerksamkeit auf die augenscheinlichen Symptome, welche jedoch auch gänzlich andere Ursachen (Allergie, Psychosomatik, etc) haben können, erinnert darüber hinaus an das Lehrbuchbeispiel von Paul Watzlawick hinsichtlich der zerkratzten Windschutzscheiben in Seattle (siehe *Paul Watzlawick*, Wie wirklich ist die Wirklichkeit)

Risiko, dass verständigte Personen glauben, sie wären infiziert, weil eine andere Person fälschlicherweise (jedoch nicht böswillig) aufgrund des Fragebogens angenommen hat, infiziert zu sein

Die Symptome sind einer COVID-19 Erkrankung sind häufig schwer zuzuordnen, die häufigsten Symptome, mit denen die Betroffenen auffällig werden sind: Husten (55 Prozent), Fieber (39 Prozent), Schnupfen (28 Prozent), Halsschmerzen (23 Prozent), und Atemnot (drei Prozent).[56]

Derzeit befindet sich Österreich nicht nur in der Phase der abklingende Grippesaison, sondern auch in einer „starken" Allergiesaison, da die Änderungen des Klimawandels dazu einer stärkeren Birkenpollenbelastung als üblich geführt hat. Teilweise besteht hier eine ähnliche Symptomatik. Die bereits bekannten Allergien ist dies für den Betroffenen erklärbar, Allergien treten jedoch grundsätzlich irgendwann das erste Mal auf und es ist denkbar, dass Personen bei denen Allergien das erste Mal auftreten, vermuten an COVID-19 erkrankt zu sein.

Diese Personen könnten weitere Kontaktpersonen über eine tatsächlich nicht vorliegende Infektion verständigen.

Risiko, dass Personen aufgrund des Fragebogens annehmen, sie wären nicht infiziert, obwohl sie es tatsächlich sind

Asymptomatische Verläufe können häufig sein. Laut Wikipedia waren dies gut die Hälfte der Fälle auf der Diamond Princess.[57] Auch nach einer isländischen Studie, besteht ein hoher Anteil an asymptomatischen Verläufen.[58] Wie hoch die Anzahl der asymptomatischen Verläufe in Österreich vermutlich ist, ist derzeit unklar. Die Ergebnisse der österreichischen Dunkelzifferstudie in Form eines wissenschaftlichen Methodenberichts des Sora-Institutes, wurde im April 2020 präsentiert.[59] Diese Studie erlaubt es, die Prävalenz akuter Infektionen mit COVID-19 („Corona-Virus") unter in Österreich lebenden, nicht hospitalisierten Menschen für den Zeitraum Anfang April 2020 abzuschätzen: Der Anteil der positiv Getesteten beträgt in der gewichteten Stichprobe 0,33 %, umgelegt auf die Bevölkerung sind das ca. 28.500 Personen.[60] Eine Einschätzung des Anteils der asymptomatischen Verläufe erfolgte im Rahmen dieser Studie jedoch nicht.

Schätzungen zu Folge, handelt es sich dabei jedoch um einen Anteil von mind. 50 %[61], tlw wird auch

---

56 Siehe dazu folgenden Beitrag https://www.diepresse.com/5792524/coronavirus-schnupfen-und-halsweh-bei-knapp-einem-drittel-auffallig#kommentare, (zuletzt abgerufen am 08.04.2020)

57 https://de.wikipedia.org/wiki/COVID-19#cite_note-Diamond-epi-10 ; https://cmmid.github.io/topics/covid19/severity/diamond_cruise_cfr_estimates.html (zuletzt abgerufen am 08.04.2020).

58 https://orf.at/stories/3159008/ (zuletzt abgerufen am 08.04.2020).

59 https://www.sora.at/nc//news-presse/news/news-einzelansicht/news/halbzeit-bei-der-dunkelzifferstudie-1005.html (zuletzt abgerufen am 08.04.2020).

60 https://www.sora.at/nc/news-presse/news/news-einzelansicht/news/covid-19-praevalenz-1006.html (zuletzt abgerufen am 21.04.2020).

61 Siehe, Aigner Florian, Covid-19: Ein simulierter Blick zurück, April 2020, abrufbar unter https://www.tuwien.at/tu-wien/aktuelles/news/news/covid-19-ein-simulierter-blick-zurueck/ (zuletzt abgerufen am 11.05.2020).

von 75 bis 80 %[62] ausgegangen.

Risiko, dass Personen fälschlicherweise glauben, sie wären infiziert, weil der Prozess der Meldung fehlerhaft implementiert ist oder manipuliert wird

Wenn der Prozess der Meldung fehlerhaft implementiert wurde oder manipuliert wird, könnten Personen fälschlicherweise davon ausgehen, dass sie infiziert sein könnten.

Risiko, dass Personen fälschlicherweise eine Infektion durch Angabe ihrer Telefonnummer melden

Es besteht das Risiko, dass Personen fälschlicherweise angeben infiziert zu sein und ihre Telefonnummer angeben weil sie glauben es ist für den Registrierungsprozess notwendig.

Risiko, dass die informierten Kontakte aus ihrer Erinnerung Rückschlüsse ziehen können, wer die infizierte Person ist, obwohl die Meldung pseudonym erfolgt

Unmittelbar nach einer Krankmeldung werden die Kontakte der letzten 3 Tage darüber informiert, dass einer der Intensiv-Kontakte als infiziert gilt, sowie wann der Kontakt stattgefunden hat. Dies gibt den Kontakten die Möglichkeit, weitere Personen im Umfeld, zu denen diese nach diesem Zeitpunkt Kontakt hatten, zu warnen Durch die Angabe, wann der Kontakt stattgefunden hat, könnten Rückschlüsse die auf Infizierte Person erfolgen.

Risiko, dass über die Endgeräte ein Personenbezug zu den pseudonymen Kontakten hergestellt werden kann

Für den Handybesitzer könnte potentiell auslesbar sein, welchen konkreten Personen IDs zuordenbar sind.

Risiko, dass Personen mit mangelnden Deutschkenntnissen nicht verstehen in was sie einwilligen

Die APP kann in deutscher und englischer Sprache heruntergeladen werden.

Die in der App zugänglichen Datenschutzinformation sind jedoch nur in deutscher Sprache verfügbar. Dies kann dazu führen, dass Personen die nicht die erforderlichen Deutschkenntnisse aufweisen, die datenschutzrechtlich relevanten Informationen nicht ausreichend verstehen. Gerade vor dem Hintergrund, dass die App von einer kritischen Masse verwendet werden sollte, ist dies als Risiko einzustufen.

Risiko, der fehlenden Barrierefreiheit der App

Die Verwendungsmöglichkeit der App durch Menschen mit besonderen Bedürfnissen ist aktuell eingeschränkt. Somit ist keine vollständige Barrierefreiheit gegeben und sind bestimmte Personengruppen von der Verwendung der App ausgeschlossen.

---

62 Siehe Interview mit Johan Giesecke, abrufbar auf der Rechereplattform Addendum unter https://www.addendum.org/coronavirus/interview-johan-giesecke/ (zuletzt abgerufen am 11.05.2020).

Risiko, dass sich Personen durch sozialen Druck dazu gedrängt fühlen könnten, die App zu verwenden und entgegen ihre eigentliche Überzeugung Daten aufzuzeichnen

Damit die Infektionen eingedämmt werden können, ist es erforderlich, dass möglichst viele Menschen die App verwenden um die Infektionsketten nachzuvollziehen und andere Personen zu warnen. Dies könnte dazu führen, dass ein sozialer Druck zur Verwendung der App entsteht.

Risiko, dass bei einem allfällig unberechtigten Zugriff auf die Daten in der Azure-Cloud auf den symmetrischen Schlüssel unberechtigt zugegriffen wird

Im Zusammenhang mit der Speicherung von personenbezogenen Daten in der Azure Cloud besteht eine Serverseitige Verschlüsselung, in welcher die Funktion "Encryption at rest" standardmäßig aktiv ist. Bei einem allfälligen unberechtigten Zugriff auf die Daten könnte jedoch auch auf den symmetrischen Schlüssel unberechtigt zugegriffen werden.

Risiken aus häufiger Quarantäne

Auf dem Weg zur Herdenimmunität bzw. bis zur Verfügbarkeit einer Impfung werden sich ggf hohe Infektionszahlen ergeben. Dies kann bei Betroffenen zu einer häufigen Quarantäne führen.

Beispiel: Der Betroffene erfährt durch die App, dass man Kontakt zu einem nachgewiesenen Infizierten hatte und begibt sich in Selbstisolation und erhält) Entwarnung. Dasselbe könnte nach Beendigung der Selbstisolation (und ohne entsprechende Virus-Tests die dem Betroffenen „Immunität" bestätigt) nach kurzer Zeit wieder geschehen. Seit Lockerung der Ausgehbeschränkungen könnten gehäufte Selbstisolationen einer Person ggf zu Jobverlust führen.

Risiko aus möglicher Ungenauigkeit von Bluetooth

Bluetooth kann sich je nach nach Umgebung als unzuverlässig erweisen. So kann die Technologie eine zu geringe Reichweite aufweisen oder aber eine zu weite Reichweite aufweisen **um realistische Angaben zu Infektionsrisiken daraus ableiten zu können.** Zudem können beim Einsatz praktische Probleme bestehen (ein **Smartphone in der hinteren Hosentasche könnte anders abstrahlen als ein Smartphone in der Hand.**)

Risiko, dass infizierte NutzerInnen nicht bekannt geben positiv getestet worden zu sein, weil sie Angst haben, dass versucht wird mithilfe der pseudonymisierten Daten einen Personenbezug herzustellen

Unabhängig davon, dass dieser Rückschluss nicht (oder nur sehr schwer) möglich ist, reicht die unbegründete Angst um den Nutzen der App zu untergraben.

Risiko, dass auch kürzere Kontakte, als Intensivkontakte erfasst werden

Es ist denkbar, dass aufgrund der Ungenauigkeit der eingesetzten Technologie, auch kürzere Kontakte, als Intensivkontakte erfasst werde.

Risiko, dass Daten an den Uniqa-Konzern verkauft werden

In den (sozialen) Medien wurde die Befürchtung geäußert, dass Daten von App-Usern an den Uniqa-

Konzern verkauft werden könnten, da die Entwicklung der App mit einer Uniqa Spende finanziert wurde.

Risiko, dass Google und Apple die Daten für kommerzielle Zwecke weiterverwenden

Google und Apple könnten die Daten für andere (eigene kommerzielle) Zwecke weiterverwenden.

Risiko, dass es eine Überwachungsapp für den Staat ist/werden kann (etwa durch rechtliche Änderungen)

In den Medien wurde über die Diskussion betreffend einen verpflichtenden Einsatz der Stopp Corona-App berichtet. Es wäre denkbar, die App für staatliche Überwachungszwecke zur Kontrolle der Pandemie einzusetzen.

Risiko, dass beim Prüfen der Infektionsmeldungen unbeabsichtigt eine Nachricht als „Positivnachricht" gewertet wird

Meldet eine Person eine Infektion, verschlüsselt sie die Nachricht *IN* mit den Public Keys jener Personen, mit denen ein Kontakt bestanden hat. Die Personen werden dadurch über die Infektion informiert, dass sie versuchen alle Infektionsnachrichten zu entschlüsseln. Gelingt das, geht die App davon aus, dass mit einer infektiösen Person Kontakt bestanden hat.

In Abhängigkeit der Länge der Nachricht *IN* besteht eine bestimmte Wahrscheinlichkeit, dass eine Nachricht bei der Entschlüsselung unbeabsichtigt den Wert von *IN* liefert. Eine Person würde in diesem Fall davon ausgehen, dass sie mit einem Infizierten Kontakt hatte, obwohl dies nicht zutrifft.

Die Wahrscheinlichkeit für diesen Fall kann mit der Formel

$$P(m,n) = 1 - e^{-\left(\frac{n^2}{2m}\right)}$$

berechnet werden, wobei *m* die Anzahl der möglichen Nachrichten *IN* darstellt und *n* die Anzahl der verwendeten Schlüsselpaare.[63]

Beispiel: Beträgt die Länge der Nachricht *IN* lediglich 6 Byte, gibt es insgesamt $m = 256^6$ mögliche Kombinationen. Geht man davon aus, dass alle Einwohner in Österreich die App installieren beträgt $n = 8.837.707$.[64] Unter Anwendung der oben angeführten Formel tritt mit einer Wahrscheinlichkeit von 12,95 Prozent das geschilderte Szenario ein.

63 Vgl. *Menezes/v. Oorschot/Vanstone*, Handbook of Applied Cryptography (1997), S 53.

64 Einwohneranzahl laut https://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/bevoelkerung/index.html (zuletzt abgerufen am 08.04.2020).

6.2 Risikoanalyse

Auf Grundlage der bereits bestehenden rechtlichen, technischen und organisatorischen (bereits unter Beachtung der umgesetzten, aktuellen) Maßnahmen kommen die Verfasser zur folgenden Risikoanalyse:

Ad Rufschädigung

Schwere: Schwer

Eintrittswahrscheinlichkeit: Mittel

Ad finanzieller Verlust

Schwere: Schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Kontrollverlust

Schwere: Sehr schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Verlust der Vertraulichkeit

Schwere: Sehr schwer

Eintrittswahrscheinlichkeit: Gering

Ad Diskriminierung

Schwere: Sehr schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Identitätsdiebstahl- oder Betrug

Schwere: Schwer

Eintrittswahrscheinlichkeit: Gering

Ad unbefugte Aufhebung der Pseudonymisierung

Schwere: Mittel

Eintrittswahrscheinlichkeit: Gering

Ad Risiken des Konterkarierens des social distancing Gedankens bzw. der gesetzlichen Maßnahmen

Schwere: Sehr Schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko der intransparenten Verarbeitung personenbezogener Daten durch unzureichend beschriebene Datenschutzinformationen der App

Schwere: Schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiken aus der Erstellung einer umfangreichen Datenbank mit sensiblen Daten, sozialer Interaktionen und Bewegungsprofilen

Schwere: Sehr Schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko: Aus den erhobenen Statistikdaten werden individuelle Bewegungsprofile abgeleitet

Schwere: Sehr Schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko, dass Personen fälschlicherweise glauben, sie wären infiziert, weil sich jemand mutwillig fälschlicherweise als infiziert gemeldet hat

Schwere: Sehr schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko, dass Personen fälschlicherweise glauben, sie wären infiziert, weil ihre Symptome den Symptomen des Fragebogens entsprechen

Schwere: Sehr schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko, dass verständigte Personen glauben, sie wären infiziert, weil eine andere Personen fälschlicherweise (jedoch nicht böswillig) aufgrund des Fragebogens angenommen hat, infiziert zu sein

Schwere: Sehr schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko, dass Personen aufgrund des Fragebogens annehmen, sie wären nicht infiziert, obwohl sie es tatsächlich sind

Schwere: Sehr schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko, dass Personen fälschlicherweise glauben, sie wären infiziert, weil der Prozess der Meldung fehlerhaft implementiert ist oder manipuliert wird

Schwere: Sehr schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko, dass Personen fälschlicherweise angeben infiziert zu sein und ihre Telefonnummer angeben weil sie glauben es ist für den Registrierungsprozess notwendig

Schwere: Sehr schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko, dass die informierten Kontakte aus ihrer Erinnerung Rückschlüsse ziehen können, wer die infizierte Person ist, obwohl die Meldung pseudonym erfolgt

Schwere: Schwer

Eintrittswahrscheinlichkeit: Gering

Ad Risiko, dass über die Endgeräte ein Personenbezug zu den pseudonymen Kontakten hergestellt werden kann

Schwere: Schwer

Eintrittswahrscheinlichkeit: Gering

Ad Risiko, dass Personen mit mangelnden Deutschkenntnissen nicht verstehen in was sie einwilligen

Schwere: Schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko der fehlenden Barrierefreiheit

Schwere: Schwer

Eintrittswahrscheinlichkeit: Hoch

Ad Risiko, dass sich Personen durch sozialen Druck dazu gedrängt fühlen könnten, die App zu verwenden und entgegen ihre eigentliche Überzeugung Daten aufzuzeichnen

Schwere: Sehr schwer

Eintrittswahrscheinlichkeit: Hoch

Ad Risiko, dass bei einem allfällig unberechtigten Zugriff auf die Daten in der Azure-Cloud auf den symmetrischen Schlüssel unberechtigt zugegriffen wird

Schwere: Sehr Schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiken aus häufiger Quarantäne

Schwere: Schwer

Eintrittswahrscheinlichkeit: Hoch

Ad Risiko aus möglicher Ungenauigkeit von Bluetooth

Schwere: Schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko, dass infizierte NutzerInnen nicht bekannt geben positiv getestet worden zu sein weil sie Angst haben, dass versucht wird mithilfe der pseudonymisierten Daten einen Personenbezug herzustellen

Schwere: Schwer

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko, dass auch kürzere als Intensivkontakte erfasst werden

Schwere: Mittel

Eintrittswahrscheinlichkeit: Mittel

Ad Risiko, dass Daten an Uniqa verkauft werden

Schwere: Sehr schwer

Eintrittswahrscheinlichkeit: Gering

Ad Risiko, dass Google und Apple die Daten für kommerzielle Zwecke verwenden

Schwere: Sehr schwer

Eintrittswahrscheinlichkeit: Gering

Ad Risiko, dass es eine Überwachungsapp für den Staat ist/werden kann (etwa durch rechtliche Änderungen)

Schwere: Schwer

Eintrittswahrscheinlichkeit: Gering

Ad Risiko, dass beim Prüfen der Infektionsmeldungen unbeabsichtigt eine Nachricht als „Positivnachricht“ gewertet wird

Schwere: Schwer

Eintrittswahrscheinlichkeit: Mittel

6.3 Risikobewertung

Der Risikograd (hier dreistufig dargestellt: gering, mittel, hoch) ergibt aus der Kombination von Eintrittswahrscheinlichkeit und Schwere des Risikos bestimmt. Das kann in Form einer Risikomatrix dargestellt werden.[65]

Ad Rufschädigung

Risikograd: Mittel

Ad finanzieller Verlust

Risikograd: Mittel

Ad Kontrollverlust

Risikograd: Mittel

Ad Verlust der Vertraulichkeit

[65] Vgl *Kranig/Sachs/Gierschmann*, Datenschutz-Compliance nach der DS-GVO (2017) 102 ff.

Risikograd: Mittel

Ad Diskriminierung

Risikograd: Hoch

Ad Identitätsdiebstahl

Risikograd: Mittel

Ad unbefugte Aufhebung der Pseudonymisierung

Risikograd: Gering

Ad Risiken des Konterkarierens des social distancing Gedankens bzw. der gesetzlichen Maßnahmen

Risikograd: Hoch

Ad Risiko der intransparenten Verarbeitung personenbezogener Daten durch unzureichend beschriebene Datenschutzinformationen der App

Risikograd: Mittel

Ad Risiken aus der Erstellung einer umfangreichen Datenbank mit sensiblen Daten, sozialer Interaktionen und Bewegungsprofilen

Risikograd: Hoch

Ad Risiko: Aus den erhobenen Statistikdaten werden individuelle Bewegungsprofile abgeleitet

Risikograd: Hoch

Ad Risiko, dass Personen fälschlicherweise glauben, sie wären infiziert, weil sich jemand mutwillig fälschlicherweise als infiziert gemeldet hat

Risikograd: Hoch

Ad Risiko, dass Personen fälschlicherweise glauben, sie wären infiziert, weil sie ihre Symptome den Symptomen des Fragebogens entsprechen

Risikograd: Hoch

Ad Risiko, dass verständigte Personen glauben, sie wären infiziert, weil eine andere Personen fälschlicherweise (jedoch nicht böswillig) aufgrund des Fragebogens angenommen hat, infiziert zu sein

Risikograd: Hoch

Risiko, dass Personen aufgrund des Fragebogens annehmen, sie wären nicht infiziert, obwohl sie es tatsächlich sind

Risikograd: Hoch

Ad Risiko, dass Personen fälschlicherweise glauben, sie wären infiziert, weil der Prozess der Meldung fehlerhaft implementiert ist oder manipuliert wird

Risikograd**:** Hoch

Ad Risiko, dass Personen fälschlicherweise angeben infiziert zu sein und ihre Telefonnummer angeben weil sie glauben es ist für den Registrierungsprozess notwendig

Risikograd: Hoch

Ad Risiko, dass die informierten Kontakte aus ihrer Erinnerung Rückschlüsse ziehen können, wer die infizierte Person ist, obwohl die Meldung pseudonym erfolgt

Risikograd: Mittel

Ad Risiko, dass über die Endgeräte ein Personenbezug zu den pseudonymen Kontakten hergestellt werden kann

Risikograd: Mittel

Ad Risiko, dass Personen mit mangelnden Deutschkenntnissen nicht verstehen in was sie einwilligen

Risikograd:Mittel

Ad Risiko der fehlenden Barrierefreiheit

Risikograd: Hoch

Ad Risiko, dass sich Personen durch sozialen Druck dazu gedrängt fühlen könnten, die App zu verwenden und entgegen ihre eigentliche Überzeugung Daten aufzuzeichnen

Risikograd: Hoch

Ad Risiko, dass bei einem allfällig unberechtigten Zugriff auf die Daten in der Azure-Cloud auf den symmetrischen Schlüssel unberechtigt zugegriffen wird

Risikograd: Hoch

Ad Risiken aus häufiger Quarantäne

Risikograd: Hoch

Ad Risiko aus möglicher Ungenauigkeit von Bluetooth

Risikograd: Mittel

Ad Risiko, dass infizierte NutzerInnen nicht bekannt geben positiv getestet worden zu sein weil sie Angst haben, dass versucht wird mithilfe der pseudonymisierten Daten einen Personenbezug herzustellen

Risikograd: Mittel

Ad Risiko, dass auch kürzere als Intensivkontakte erfasst werden

Risikograd: Mittel

Ad Risiko, dass Daten an die Uniqa verkauft werden

Risikograd: Mittel

Ad Risiko, dass Google und Apple die Daten für kommerzielle Zwecke weiterverwenden

Risikograd: Mittel

Ad Risiko, dass es eine Überwachungsapp für den Staat ist/werden kann (etwa durch rechtliche Änderungen)

Risikograd: Mittel

Ad Risiko, dass beim Prüfen der Infektionsmeldungen unbeabsichtigt eine Nachricht als „Positivnachricht“ gewertet wird

Risikograd: Mittel

6.4 Maßnahmenplan zur Risikobehandlung

Zur Minimierung der nicht als tragbar einzustufenden Risiken und in Bezug auf die verfügbaren Technologien und Implementierungskosten wurden folgende geeignete **technische und organisatorische Maßnahmen** (TOM) zur Risikoreduktion identifiziert und getroffen.

Die allgemeinen technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit sind in Anhang A dokumentiert.

[Details zu den getroffenen Datensicherheitsmaßnahmen werden aus Sicherheitsgründen nicht veröffentlicht und wurden daher in der veröffentlichten Version entfernt.]

Die Ergebnisse der Schritte zur Risikobeurteilung in diesem Abschnitt sind in folgender Tabelle zusammengefasst:

Identifiziertes Risiko (Beschreibung)	Auswirkungen (Schwere)	Eintrittswahrscheinlichkeit	Risikograd	Maßnahmen (TOM)	Finaler Risikograd
Rufschädigung: durch Bekanntwerden von Erkrankungsdaten die von unbefugten Personen an die Öffentlichkeit kommuniziert werden	Schwer	Mittel	Hoch	• Datenminimierung: Krankmeldungen werden nicht namentlich erfasst. Nur die Mobilfunknummer wird zur Missbrauchsbekämpfung abgefragt. • Berechtigungskonzept: Nur berechtigte Mitarbeiter*innen haben Zugriff auf die Datenbank (Need-to-Know-Prinzip). • Schulung jener Mitarbeiter*innen die mit den Daten arbeiten.	Mittel
Finanzieller Verlust	Schwer	Mittel	Mittel	Es ist davon auszugehen, dass ohne Impfstoff langfristig ca 60 % (ungefähre Schwelle zur Herdenimmunität) der österreichischen Bevölkerung infiziert sein werden. Dies kann insbesondere im heurigen Jahr in Österreich mit vielen Krankenständen bzw. verpflichtenden Phasen der Selbstisolation verbunden sein. Der österreichische Gesetzgeber hat umfangreiche Maßnahmen zur Abfederung dieser Auswirkungen geschaffen.	Gering
Kontrollverlust: beliebige Mitarbeiter*innen haben Zugriff auf Kontaktdaten oder Erkrankungsdaten	Sehr schwer	Mittel	Hoch	• Dezentralisierung: Die Kontakte werden bis zur Krank- oder Verdachtsmeldung anonym und nur jeweils lokal am Endgerät in der App gespeichert. Serverseitig besteht darauf kein Zugriff. Die Daten am Endgerät liegen in der App-Sandbox und sind damit auch vor lokalen Zugriffen geschützt. • Datenminimierung: Krankmeldungen werden nicht namentlich erfasst. Nur die Mobilfunknummer wird zur Missbrauchsbekämpfung abgefragt.	Mittel

				• Berechtigungskonzept: Nur berechtigte Mitarbeiter*innen haben Zugriff auf die Datenbank (Need-to-Know-Prinzip). • Schulung jener Mitarbeiter*innen die mit den Daten arbeiten.	
Verlust der Vertraulichkeit: Es ist nicht eindeutig, wer auf die Daten zugreift bzw. könnten Unbefugte auf die Daten zugreifen	Sehr schwer	Mittel	Hoch	• Dezentralisierung: Die Kontakte werden nur anonym und nur jeweils lokal am Endgerät in der App gespeichert. Serverseitig besteht darauf kein Zugriff. Die Daten am Endgerät liegen in der App-Sandbox und sind damit auch vor lokalen Zugriffen geschützt. • Datenminimierung: Krankmeldungen werden nicht namentlich erfasst. Nur die Mobilfunknummer wird zur Missbrauchsbekämpfung abgefragt. • Protokollierung um eine Nachvollziehbarkeit zu gewährleisten. • In Azure ist die Standardeinstellung für die transparente Datenverschlüsselung, dass der Datenbank-Verschlüsselungsschlüssel durch ein eingebautes Server-Zertifikat geschützt ist. Das integrierte Server-Zertifikat ist für jeden Server einzigartig, und der verwendete Verschlüsselungsalgorithmus ist AES 256. Wenn sich eine Datenbank in einer Georeplikationsbeziehung befindet, werden sowohl die primäre als auch die geosekundäre Datenbank durch den Schlüssel des übergeordneten Servers der primären Datenbank geschützt. Wenn zwei Datenbanken mit demselben Server verbunden sind, teilen sie auch dasselbe integrierte Zertifikat. Microsoft rotiert diese Zertifikate automatisch in Übereinstimmung mit der internen Sicherheitsrichtlinie, und der Stammschlüssel wird durch einen internen Microsoft-Geheimspeicher geschützt.	Mittel

				• Datenminimierung: Der Server weiß nicht, wer mit wem Kontakt hatte. Alle App-NutzerInnen werden informiert, dass eine neue Krankmeldung vorliegt. Die Clients downloaden die relevanten Nachrichten. Für sie ist nur eine Nachricht relevant, wenn sie die ID des Kontaktes entschlüsseln können -> das ist das Indiz dafür, dass sie in Kontakt waren.	
Diskriminierung aufgrund der verarbeiteten Daten insbesondere aufgrund von Aspekten, die die gesundheitliche Lage bzw. das Verhalten betreffen	Sehr schwer	Mittel	Hoch	• Das Backend weiß nicht, wer mit wem Kontakt hatte. Alle App NutzerInnen werden informiert, dass eine neue Krankmeldung vorliegt. Die Clients downloaden die relevanten Nachrichten. Für sie ist nur eine Nachricht relevant, wenn sie die ID des Kontaktes entschlüsseln können -> das ist das Indiz dafür, dass sie in Kontakt waren • Nur berechtigte Mitarbeiter*innen haben Zugriff auf die Datenbank (Need-to-Know-Prinzip)	Mittel
Identitätsdiebstahl	Schwer	Gering	Mittel	• Es bestehen umfassende technisch-organisatorische Maßnahmen (verschlüsselte Verbindungen etc., siehe Anhang), die nicht nur einem (externen bzw. internen) Datenmissbrauch bzw. -diebstahl wirksam entgegenwirken (z.B. durch eine Firewall und abgestufte Berechtigungen)	Gering
Unbefugte Aufhebung der Pseudonymisierung: (etwa wenn die DB gehackt wird)	Mittel	Gering	Gering	• Dezentralisierung: Die Kontakte werden nur anonym und nur jeweils lokal am Endgerät in der App gespeichert. Serverseitig besteht darauf kein Zugriff. Die Daten am Endgerät liegen in der App-Sandbox und sind damit auch vor lokalen Zugriffen geschützt. • Datenminimierung: Krankmeldungen werden nicht namentlich erfasst. Nur die Mobilfunknummer wird zur Missbrauchsbekämpfung abgefragt.	Gering

				• Sicherheitsvorkehrungen des Rechenzentrums (siehe TOMS) • Sicherheitsvorkehrungen des Österreichischen Roten Kreuzes, Passwörter werden regelmäßig gewechselt, Firewall	
Konterkarieren der Social Distancing Maßnahmen/der gesetzlichen Regelungen	Sehr schwer	Mittel	Hoch	• Aufklärung und gute Kommunikation als mitigierende Maßnahmen. • Vor allem: Alternativen zur App werden auf der Website des Roten Kreuzes, welche über die App abrufbar ist, in den Vordergrund gerückt und auf das Abstandhalten/Social Distancing hingewiesen: BLEIBEN SIE ZUHAUSE! dann brauchen Sie die App gar nicht. (Beispiele, wo die App zB sehr viel Sinn macht, ist etwa das - zB Personal in Gesundheitseinrichtungen, oder etwa Geschäftsreisen in öffentlichen Verkehrsmitteln (Zügen)). • Es wird gezeigt, dass es sich bei der App nicht um die einzige Alternative handelt, sondern diese eine Entlastung des Systems bringen soll. Alternativen: Persönliches offline-Quarantäne-Tagebuch. Führen Sie ein handschriftliches Logbuch ihrer potentiellen Infektionskontakte.	Mittel
Risiko der intransparenten Verarbeitung	Schwer	Mittel	Mittel	• Umfangreiche Datenschutzinformationen und FAQs werden den Betroffenen zur Verfügung gestellt. • Der Source Code wird grundrechtsaffinen NGOs in künftigen Updates zur Verfügung gestellt (siehe dazu weiter unten) • Die Datenschutz-Folgenabschätzung wird der Öffentlichkeit auszugsweise zur Verfügung gestellt	Gering
Risiken aus der Erstellung einer umfangreichen Datenbank mit sensiblen Daten,	Sehr schwer	Mittel	Hoch	• Die Kontakte werden nur anonym und nur jeweils lokal am Endgerät in der App gespeichert. Serverseitig	Mittel

sozialer Interaktionen und Bewegungsprofilen				besteht darauf kein Zugriff. Die Daten am Endgerät liegen in der App-Sandbox und sind damit auch vor lokalen Zugriffen geschützt. Es ist daher von zentraler Stelle aus nicht möglich, eine solche Datenbank zu erstellen. • Zur Erkennung der Personen in der Umgebung, um damit der Kontaktaufzeichnung im Endgerät der NutzerInnen, wird BLE Technolgie genutzt. Diese Daten werden allerdings nicht gespeichert. • Durch Verschlüsselung wird sichergestellt dass die Nutzer möglichst lange die- "Datenhoheit" behalten. Jeder muss App installiert haben, aktiv in die Verarbeitung einwilligen und die Verständigung von weiteren Personen aktiv anstoßen). • Verschlüsselungstechniken. • Penetration-Tests. • Es wird keine Device ID im Rahmen der App verwendet, sondern unabhängig voneinander generierte Zufalls-IDs verwendet:	
Risiko: Aus den erhobenen Statistikdaten werden individuelle Bewegungsprofile abgeleitet.	Schwer	Mittel	Mittel	• Die Kontakte werden nur pseudonym und nur jeweils lokal am Endgerät in der App gespeichert. • In der Statistik werden nur aggregierte Daten erhoben, wie die Anzahl der Infizierten und die Anzahl ihrer Kontakte. • Es sind auch keine Zeitstempel im Millisekundenbereich in den statistischen Daten enthalten, die es eventuell ermöglichen würden, einen Personenbezug herzustellen.	Gering
Risiko, dass Personen fälschlicherweise glauben, sie wären infiziert, weil sich jemand mutwillig	Schwer	Hoch	Hoch	• Die NutzerInnen werden vor Abgabe der Meldung ausdrücklich darauf hingewiesen, dass sie nur	Mittel

fälschlicherweise als infiziert gemeldet hat.				medizinisch nachgewiesene Infektionen melden dürfen. • Sie müssen vor Abgabe der Meldung ein Feld ankreuzen, um zu bestätigen, dass sie die Angaben wahrheitsgemäß gemacht haben. • Bei der Abgabe der Meldung wird die Mobilfunknummer des Meldenden erfasst und verifiziert. Die Meldenden wissen, sie sind mit der Mobilfunknummer eindeutig identifiziert und können verfolgt werden, wenn sie schuldhaft einen Schaden verursachen.	
Risiko, dass Personen fälschlicherweise glauben, sie wären infiziert, weil ihre Symptome den Symptomen des Fragebogens entsprechen	Sehr schwer	Mittel	Hoch	• Die Qualitätssicherung bzgl. der Inhalte und der Logik des Fragebogens erfolgte durch Abstimmung zwischen dem ÖRK und der zuständigen Abteilung des Gesundheitsministeriums. • Neue wissenschaftliche Erkenntnisse werden durch zeitnahe Releases berücksichtigt • Infotexte sind so ausgestaltet, dass die User darauf hingewiesen werden, dass die Symptome einer Covid-19-Erkrankung entsprechen können (jedoch nicht müssen). Die Betroffenen werden über die weitere Vorgehensweise informiert/angeleitet. • Am Beginn des Symptom-Checkers erfolgt der Hinweis, dass dieser Fragebogen keine ärztliche Diagnose ersetzt.	Mittel
Risiko, dass verständigte Personen glauben, sie wären infiziert, weil eine andere Person fälschlicherweise (jedoch nicht böswillig) aufgrund des Fragebogens angenommen hat, infiziert zu sein.	Sehr schwer	Mittel	Hoch	• Die Qualitätssicherung bzgl. der Inhalte und der Logik des Fragebogens erfolgte durch Abstimmung zwischen dem ÖRK und der zuständigen Abteilung des Gesundheitsministeriums. • Neue wissenschaftliche Erkenntnisse werden durch zeitnahe Releases berücksichtigt • Infotexte sind so ausgestaltet, dass die User darauf hingewiesen werden, dass die Symptome einer Covid-19-	Mittel

				Erkrankung entsprechen können (jedoch nicht müssen). Die Betroffenen werden über die weitere Vorgehensweise informiert/angeleitet.	
Risiko, dass Personen aufgrund des Fragebogens annehmen, sie wären nicht infiziert, obwohl sie es tatsächlich sind	Sehr schwer	Mittel	Hoch	• Die Qualitätssicherung bzgl. der Inhalte und der Logik des Fragebogens erfolgte durch Abstimmung zwischen dem ÖRK und der zuständigen Abteilung des Gesundheitsministeriums. • Neue wissenschaftliche Erkenntnisse werden durch zeitnahe Releases berücksichtigt • Infotexte sind so ausgestaltet, dass die User darauf hingewiesen werden, dass die Symptome einer Covid-19-Erkrankung entsprechen können (jedoch nicht müssen). Die Betroffenen werden über die weitere Vorgehensweise informiert/angeleitet. • Am Beginn des Symptom-Checkers erfolgt der Hinweis, dass dieser Fragebogen keine ärztliche Diagnose ersetzt.	Mittel
Risiko, dass Personen fälschlicherweise glauben, sie wären infiziert, weil der Prozess der Meldung fehlerhaft implementiert ist oder manipuliert wird.	Schwer	Mittel	Mittel	• Der Prozess der Meldung an die Kontakte ist, wie oben beschrieben, mittels Verschlüsselung implementiert, sodass nur die tatsächlich gespeicherten Kontakte die Meldung eines Infizierten verschlüsseln können.	Mittel
Risiko, dass Personen fälschlicherweise angeben infiziert zu sein und ihre Telefonnummer angeben weil sie glauben es ist für den Registrierungsprozess notwendig.	Sehr schwer	Mittel	Hoch	• Dieses Risiko wurde durch eine Umgestaltung im Bedienungsablauf der App mitigiert.	Mittel
Risiko, dass die informierten Kontakte aus ihrer Erinnerung Rückschlüsse ziehen können, wer die infizierte Person ist, obwohl die Meldung pseudonym erfolgt.	Schwer	Hoch	Hoch	• Die App protokolliert Begegnungen mit anderen Mobiltelefonen mit, diese werden jedoch aus Gründen des Datenschutzes nicht mehr in der App angezeigt.	Gering

Risiko, dass über die Endgeräte ein Personenbezug zu den Kontakten hergestellt werden kann.	Schwer	Mittel	Mittel	• Dies wird durch die verwendeten Pseudonyme wirksam unterbunden. Die Device ID des Endgeräts wird im Rahmen der App nicht verwendet. Die Pseudonyme werden zufällig generiert. • Protokollierte Begegnungen mit anderen Mobiltelefonen werden aus Gründen des Datenschutzes künftig nicht mehr angezeigt.	Niedrig
Risiko, dass Personen mit mangelnden Deutschkenntnissen nicht verstehen in was sie einwilligen	Schwer	Mittel	Mittel	• Aufgrund des hohen Zeitdrucks konnten die Datenschutzinformationen noch nicht mehrsprachig erstellt werden. Dieses Problem wird in weiteren Releases adressiert.	Mittel
Risiko der fehlenden Barrierefreiheit	Sehr schwer	Hoch	Hoch	• Einbindung der von Interessenvertretungen für Menschen mit besonderen Bedürfnissen um die bestmögliche Barrierefreiheit der App zu gewährleisten.	Mittel
Risiko, dass sich Personen durch sozialen Druck dazu gedrängt fühlen könnten, die App zu verwenden und entgegen ihre eigentliche Überzeugung Daten aufzuzeichnen.	Schwer	Hoch	Hoch	• Aufklärung und gute Kommunikation als mitigierende Maßnahmen. • Alternativen zur App werden auf der Website des Roten Kreuzes, welche über die App abrufbar ist, in den Vordergrund gerückt und auf das Abstandhalten/Social Distancing hingewiesen (Beispiele, wo es sehr viel Sinn macht, ist etwa das - zB Personal in Gesundheitseinrichtungen, oder etwa Geschäftsreisen in öffentlichen Verkehrsmitteln (Zügen). • Alternativen: Persönliches offline-Quarantäne-Tagebuch. Führen Sie ein handschriftliches Logbuch ihrer potentiellen Infektionskontakte. • Statistisch möglichst viele, einzelne die mitmachen sind aber keine „Spielverderber".	Mittel
Risiko, dass bei einem allfällig unberechtigten Zugriff auf die Daten in der Azure-Cloud auf	Sehr schwer	Mittel	Hoch	• Der Cloud-Anbieter Microsoft erhält grundsätzlich keinen Zugriff auf die gespeicherten	Mittel

den symmetrischen Schlüssel unberechtigt zugegriffen wird				Daten. Der gesamte Datenbankserver wird verschlüsselt betrieben. Der ausgewählte Verschlüsselungsmodus ist RSA HSM 2048. • Microsoft MitarbeiterInnen (und damit ihre potenziellen Dienstleister) haben auf die virtuellen Maschinen keinen direkten Zugriff bzw. keine Anmeldemöglichkeit.	
Risiken aus häufiger Quarantäne	Schwer	Hoch	Mittel	• Nach vermehrter Ausrollung von Corona-Anti-Körper-Tests (diese werden ab Ende April ausgerollt)[66], kann die abgelaufene Infektion/Immunität der Betroffenen festgestellt werden, und es ist keine weitere Quarantäne erforderlich.	Gering
Risiko aus möglicher Ungenauigkeit von Bluetooth	Schwer	Mittel	Mittel	• Unwägbarkeiten des Bluetooth-Einsatzes werden durch Signalstärkemessungen abgefangen	Gering
Risiko, dass infizierte NutzerInnen nicht bekannt geben positiv getestet worden zu sein weil sie Angst haben, dass versucht wird mithilfe der pseudonymisierten Daten einen Personenbezug herzustellen.	Schwer	Mittel	Mittel	• Dieses “Risiko” ist der informationellen Selbstbestimmung und Freiwilligkeit der App-Nutzung des Betroffenen geschuldet und soll nicht mitigiert werden.	Gering
Risiko, dass auch kürzere als Intensivkontakte erfasst werden	Mittel	Mittel	Mittel	• Stetige Verbesserung des Handshake-Algorithmus	Mittel
Risiko, dass Daten an Uniqa verkauft werden	Sehr schwer	Gering	Mittel	• striktes “Datenschutz durch Technik” Konzept, insbesondere Datenvermeidung • eindeutige Klarstellung, dass mit der Spende keine Ansprüche in welcher Hinsicht auch immer bestehen • Offene und transparente Kommunikation, den Punkt offen ansprechen	Gering
Risiko, dass Google und Apple die Daten	Sehr schwer	Gering	Mittel	• Das System vermeidet „by design“ die Entstehung	

66 https://orf.at/stories/3161054/ (zuletzt abgerufen am 08.04.2020).

für kommerzielle Zwecke weiterverwenden				personenbezogener Daten, die durch Apple oder Google missbraucht werden könnten • Die App führt in dieser Hinsicht nicht zu einer Risikoerhöhung im Vergleich zur sonstigen Nutzung eines Smartphones	
Risiko, dass es eine Überwachungsapp für den Staat ist/werden kann (etwa durch rechtliche Änderungen)	Schwer	Gering	Mittel	• striktes "Datenschutz durch Technik" Konzept, insbesondere Datenvermeidung • stetige Kommunikation mit politischen Entscheidungsträgern. Klarstellung, dass das Rote Kreuz die App dann einstellen müsste	Gering
Risiko, dass beim Prüfen der Infektionsmeldungen unbeabsichtigt eine Nachricht als „Positivnachricht" gewertet wird	Schwer	Mittel	Mittel	• Die Nachricht *IN* hat zumindest 10 Byte.	Gering
Risiko, dass Angreifer erkennt, dass eine Person mehrere infizierte Kontakte hatte	Mittel	Gering	Gering	• Ergänzen einer kryptographisch generierten Zufallszahl bei der Nachricht/*N*, sodass jede Infektionsmeldung ein anderes Chiffrat hat	Gering

6.5 Weitere Maßnahme der Risikobeurteilung: Code-Analyse

Im Zuge der Datenschutz-Folgenabschätzung wurde in Bezug auf Version 1.1 der App eine Analyse des Source-Code durch die Organisationen epicenter.works, noyb und SBA Research sowie durch Armin Ronacher (unabhängig) durchgeführt.

Diese Analyse führte zu folgenden Empfehlungen, auf die wie folgt eingegangen wurde - was zu einer weiteren Risikominimierung beiträgt:

Technische Analyse

Kapitel	Empfehlung
2.2.2.	Die vom Co-Epi-Projekt vorgestellten Sicherheitseigenschaften für Contact-Tracing-Apps stellen aus der Sicht des Datenschutzes wichtige Empfehlungen dar. Wir empfehlen, dass die gewählte Architektur diese empfohlenen Sicherheitseigenschaften berücksichtigt.
	Rückmeldung ÖRK
	Die erstrebenswerten Sicherheitseigenschaften von Contact-Tracing-Apps sind ein Grundpfeiler in der Gestaltung solcher Apps. Wir finden diese Eigenschaften wichtig und versuchen in der Umsetzung uns bestmöglich daran zu orientieren.
2.2.3.	**Empfehlung**
	Zum Entwicklungsstart der ÖRK-App standen keine architekturellen Ansätze zur Verfügung, wodurch das ÖRK und Accenture gezwungen waren, eine eigene Architektur zu entwerfen und zu implementieren. Mittlerweile werden in der Fachwelt unterschiedliche Ansätze (z.B. DP-3T, Co-Epi/CovidWatch) diskutiert. Wir empfehlen mittel- bis langfristig den Umstieg auf eine dezentrale Architektur, welche von internationalen Experten aus unterschiedlichen wissenschaftlichen Disziplinen empfohlen wird.
	Rückmeldung ÖRK
	Lösung mit Umsetzung von DP-3T Wir bevorzugen weiterhin klar einen dezentralen Architekturansatz. Daher sind im engen Austausch mit DP-3T[1)] und Google&Apple[2)] damit deren Ansätze unsere Anforderungen erfüllen, und haben dazu sehr positive Rückmeldungen erhalten. Sobald der Ansatz eine praxistaugliche Reife und Verfügbarkeit erreicht, werden wir die Architektur auf DP-3T umstellen und auf Interoperabilität mit anderen Ländern achten. (1) DP-3T: regelmäßige Abstimmungsmeetings mit Prof. Capkun (ETH Zürich) sowie Prof. Bugnion (EPFL) um unsere Anforderungen verschiedene Warntypen, manuelle Handshakes, Tokens etc. in die DP-3T Umsetzung aufzunehmen. (2) Google und Apple GF in Österreich, der globalen Partnerschaft des Umsetzungspartners Accenture mit Google&Apple bezüglich early adopter Zugänge der angekündigten Lösung; dem technischen 3rd Level Support von

Technische Analyse

Kapitel	Empfehlung
2.2.2.	Die vom Co-Epi-Projekt vorgestellten Sicherheitseigenschaften für Contact-Tracing-Apps stellen aus der Sicht des Datenschutzes wichtige Empfehlungen dar. Wir empfehlen, dass die gewählte Architektur diese empfohlenen Sicherheitseigenschaften berücksichtigt.
	Rückmeldung ÖRK
	Die erstrebenswerten Sicherheitseigenschaften von Contact-Tracing-Apps sind ein Grundpfeiler in der Gestaltung solcher Apps. Wir finden diese Eigenschaften wichtig und versuchen in der Umsetzung uns bestmöglich daran zu orientieren.
2.2.3.	**Empfehlung**
	Zum Entwicklungsstart der ÖRK-App standen keine architekturellen Ansätze zur Verfügung, wodurch das ÖRK und Accenture gezwungen waren, eine eigene Architektur zu entwerfen und zu implementieren. Mittlerweile werden in der Fachwelt unterschiedliche Ansätze (z.B. DP-3T, Co-Epi/CovidWatch) diskutiert. Wir empfehlen mittel- bis langfristig den Umstieg auf eine dezentrale Architektur, welche von internationalen Experten aus unterschiedlichen wissenschaftlichen Disziplinen empfohlen wird.
	Rückmeldung ÖRK
	Lösung mit Umsetzung von DP-3T Wir bevorzugen weiterhin klar einen dezentralen Architekturansatz. Daher sind im engen Austausch mit DP-3T[1)] und Google&Apple[2)] damit deren Ansätze unsere Anforderungen erfüllen, und haben dazu sehr positive Rückmeldungen erhalten. Sobald der Ansatz eine praxistaugliche Reife und Verfügbarkeit erreicht, werden wir die Architektur auf DP-3T umstellen und auf Interoperabilität mit anderen Ländern achten. (1) DP-3T: regelmäßige Abstimmungsmeetings mit Prof. Capkun (ETH Zürich) sowie Prof. Bugnion (EPFL) um unsere Anforderungen verschiedene Warntypen, manuelle Handshakes, Tokens etc. in die DP-3T Umsetzung aufzunehmen. (2) Google und Apple GF in Österreich, der globalen Partnerschaft des Umsetzungspartners Accenture mit Google&Apple bezüglich early adopter Zugänge der angekündigten Lösung; dem technischen 3rd Level Support von

	Wie bei 2.2.3 beschrieben lösen wir mit der Umsetzung von DP-3T und dem Google&Apple Mechanismus zum direkten Austausch der Handshake-Informationen zwischen zwei Geräten die bisher dafür genutzen Mechanismen ab.
2.3.4.	**Empfehlung**
	Wir empfehlen, dass keine Kommunikation mit dem Server des ÖRK oder einem Drittdienst stattfindet, bevor die User*innen der Datenverarbeitung zugestimmt haben.
	Rückmeldung ÖRK
	Lösung umgesetzt in Release 22.4.2020 Die Empfehlung wurde aufgegriffen und im aktuellen Release bereits umgesetzt.
2.3.5.	**Empfehlung**
	Es muss soweit als möglich ausgeschlossen werden, dass Infektionsnachrichten an bekannte öffentliche Schlüssel von Dritten zuordenbar sind.
	Rückmeldung ÖRK
	Lösung geplant für Release 30.4.2020 und DP-3T Umstellung Der Empfehlung wird gefolgt. Es ist krimineller Energie kombiniert mit technischer Expertise erforderlich, trotz bestehender Sicherheitsvorkehrungen die Informationen analysieren zu können. Um den Angriffsvektor für theoretisch bestehende statistische Rückschlüsse weiter zu minimieren, werden bis zum Release am 30.4.2020 rotierende Schlüssel eingesetzt. Mit der Umstellung auf DP-3T werden statistische Störmeldungen eingebaut um eine mögliche Zuordnung zu öffentlichen Schlüsseln zu unterbinden.
2.4.4.1.	**Empfehlung**
	Beim Einsatz von kryptografischen Algorithmen empfehlen wir die Beachtung von Best-Practice-Empfehlungen bezüglich Mindestschlüssellängen und Padding-Verfahren.
	Rückmeldung ÖRK
	Lösung mit Umsetzung von DP-3T

	Die Empfehlung wird gerne aufgegriffen und eine Umsetzung mit auch für iOS verfügbaren, besser geeigneten Padding Schemes wird gerade analysiert. Mit Umstellung auf DP-3T ist das Thema jedenfalls adressiert.
2.4.5.1.	**Empfehlung**
	In Bezug auf die Abhörsicherheit ist es eine sinnvolle Maßnahme, für eine weitere Erhöhung der Sicherheit das Vertrauen im Zusammenhang mit der Zertifikatsausstellung auf nur eine CA zu beschränken („Certificate Pinning"). Wir empfehlen diese Maßnahme in die nächste Version einzubauen.
	Rückmeldung ÖRK
	Lösung umgesetzt in Release 22.4.2020 Die Empfehlung wurde aufgegriffen und im aktuellen Release bereits umgesetzt.

Rechtliche Analyse

In einer kurzen juristischen Analyse nach der DSGVO (mit Fokus auf Artikel 5, 6 und 13 DSGVO) sind folgende Probleme und offene Punkte identifiziert worden.

Kapitel	Empfehlung
3.1.2	Eine klare Benennung aller Sub-(Sub-) Auftragsverarbeiter in der Datenschutzinformation ist nachzuholen.
	Rückmeldung ÖRK
	Anmerkung wird aufgenommen.
3.1.2	**Empfehlung**
	Angleichung der Zwecke der Datenverarbeitung zwischen AVV und Datenschutzrichtlinie.
	Rückmeldung ÖRK
	Anmerkung wird aufgenommen.
3.1.2	**Empfehlung**
	Klare Trennung der beiden Google-Dienste (Nearby und Firebase) und der jeweils Verantwortlichen in der Datenschutzinformation ist sicherzustellen.
	Rückmeldung ÖRK
	Anmerkung wird aufgenommen.
3.1.2	**Empfehlung**
	Klarstellung in der Datenschutzinformation zur Verwendung von Apple Push Notification Service ist erforderlich.
	Rückmeldung ÖRK
	Anmerkung wird aufgenommen.
3.1.2	**Empfehlung**
	Die Verwendung alternativer Auftragsverarbeiter, die nicht unter US-Gesetze fallen, wird empfohlen.
	Rückmeldung ÖRK
	Anmerkung wird für Telefonnummern (TAN) in der aktuellen Release umgesetzt. Für pseudonymisierte Daten wird an einer Umsetzung gearbeitet.

3.1.4	**Empfehlung**
	Es wäre wünschenswert, jene Daten, die konkret technisch an Gesundheits- und Bezirksverwaltungsbehörden beauskunftet werden können, sowie die im österreichischen Recht bekannten Fälle der Beauskunftung klar zu benennen.
	Rückmeldung ÖRK
	Bisher gab es keine Beauskunftungsanfrage oder Anstrebungen hierzu. Wurde in der Datenschutzinformation klargestellt.
3.2.1	**Empfehlung**
	Es ist klarzustellen, zu welchem Zweck IP-Adressen verarbeitet werden und auf welche Rechtsgrundlage jene Datenverarbeitungen gestützt werden, die bereits vor Erteilung der Einwilligung erfolgen.
	Rückmeldung ÖRK
	IP-Adressen werden nicht gespeichert. Die Aufrufe vor Einwilligung wurden korrigiert.
3.2.1	**Empfehlung**
	Die Speicherdauer von IP-Adressen ist unklar. Auch ist die Speicherdauer der „digitalen Handshakes" in der Datenschutzinformation auszuweisen.
	Rückmeldung ÖRK
	IP-Adressen werde nicht gespeichert, Information werden ergänzt wenn nicht bereits klargestellt.
3.2.3	**Empfehlung**
	Die Notwendigkeit einer zweiten, gesonderten Einwilligung für den Symptom-Checker ist zu überdenken.
	Rückmeldung ÖRK
	Dies wurde nach sorgfältiger Beratung in Hinblick auf Artikel 7(2) DSGVO für notwendig erachtet.
3.2.3	**Empfehlung**
	Der Benachrichtigungszeitraum (54 Stunden) sollte in allen Dokumenten einheitlich aufscheinen.
	Rückmeldung ÖRK
	Der Benachrichtigungszeitraum ist im Sinne des Containment 2.0 je nach Stand der Wissenschaft konfigurierbar.. Die Datenschutzinformation wurde angepasst.

3.2.4	**Empfehlung**
	Es bestehen massive Bedenken, ob die Statistik-Funktion dem Gebote der Datenminimierung entspricht.
	Rückmeldung ÖRK
	Die Anregung wurde aufgegriffen und im aktuellen Release bereits umgesetzt.
3.4.1	**Empfehlung**
	Modalitäten und Auswirkungen eines Widerrufs der erteilten Einwilligungen sollten verständlich dargestellt werden. Einzelne Handshakes sollen vom Gerät gelöscht werden können.
	Rückmeldung ÖRK
	Anregung wird gerne aufgegriffen und zur Priorisierung in den Backlog möglicher Erweiterungen gestellt.
3.4.2.	**Empfehlung**
	Die App muss die Handshakes umgehend nach der Löschfrist auch tatsächlich löschen.
	Rückmeldung ÖRK
	Die Anregung wurde aufgegriffen und befindet sich in Umsetzung.
3.4.2.	**Empfehlung**
	Die Speicherdauer von IP-Adressen muss angegeben werden.
	Rückmeldung ÖRK
	IP-Adressen werde nicht gespeichert, Information muss ergänzt werden wenn nicht bereits klargestellt.
3.5.5	**Empfehlung**
	Es scheinen weitere „angemessen Maßnahmen“ (im Sinne des Artikel 5(1)(c) DSGVO) zu bestehen, um falsche Informationen soweit wie möglich zu vermeiden.
	Rückmeldung ÖRK
	Aus fachlicher Sicht (siehe epidemologische Erläuterungen) werden grundsätzlich falsch-positive Meldungen akzeptiert oder antizipiert. Die ist ident zur analogen Welt, wo ebenfalls viele falsch-positive Fälle getestet werden um dann ein negatives Testergebnis zu erhalten.

3.5.6	**Empfehlung**
	Es ist zu empfehlen, die Übermittlungszeiten in der Datenschutzrichtlinie oder in den FAQs anzuführen.
	Rückmeldung ÖRK
	Aktuell wird die Meldung mit einem maximalen Verzug von einer Stunde übermittelt. Verbesserungen können gerne aufgenommen werden. Hinweis zur Einordnung: Der aktuell behördliche Informationsfluss „Symptom > Testung > Ergebnis > Ausforschung der Sozialkontakte > Benachrichtigung" benötigt typischerweise Tage – gegenüber 1 Stunde in der App.
3.6	**Empfehlung**
	Zumindest die eigene UUID ist dem User ersichtlich zu machen oder eine alternative Möglichkeit der eindeutigen Identifizierung zu schaffen, um die Ausübung von Betroffenenrechten zu ermöglichen.
	Rückmeldung ÖRK
	Dieser Verbesserungswunsch kann gerne aufgenommen und gemeinsam priorisiert werden. Faktisch wird die UUID nach dem Ausbau der Statistikmeldung nicht weiter verwendet.

6.6 Benennung der verbleibenden hohen Risiken

Wie in der Tabelle in Kapitel 6.4 oben ersichtlich, verbleiben keine hohen Risiken für die Betroffenen.

7 Fazit und getroffene Entscheidungen

7.1 Entscheidung zur weiteren Vorgehensweise V1.0

Im Zuge der Erstellung der Datenschutz-Folgenabschätzung Version 1.0 wurde vom Projektteam in Abstimmung mit der Geschäftsleitung entschieden, dass aufgrund der gesetzten Maßnahmen zwar kein hohes Risiko für die Betroffenen besteht, jedoch folgende weitere technische und organisatorische Maßnahmen umgesetzt werden.

Allerdings werden folgende Empfehlungen an den Verantwortlichen im Bericht des Datenschutzbeauftragten an die Geschäftsleitung des Verantwortlichen formuliert. Es handelt sich dabei um wesentliche Empfehlungen und Bedingungen, welche weiteren Maßnahmen zeitnah, spätestens mit der nächsten Ausbaustufe (Release 1.1) umzusetzen sind:

1. Die ständige und zeitkritische Einbindung des Datenschutzbeauftragten muss gewährleistet sein. Insbesondere ist der DSBA frühestmöglich in die Prozesse zur Erweiterung des Funktionsumfangs einzubinden. Entsprechende Ressourcen auch für externe Beratung müssen sichergestellt sein und nicht das ordentliche Budget für den Datenschutz im Roten Kreuz belasten (Schaffung eines gesonderten Budgets).
2. Die Bereitschaft zur Datenminimierung und zur Einhaltung der Datenschutz-Grundsätze als oberstes Gebot der weiteren Entwicklung ist weiterhin beizubehalten. Insbesondere sind Verbesserungen zum Datenschutz und zur Datensicherheit auch unabhängig von Funktionserweiterungen auf technischer Ebene in zumutbaren Abständen umzusetzen. Ein detaillierter Plan hierzu wird zwischen dem Verantwortlichen und dem Auftragsverarbeiter Accenture anhand der obenstehenden Risiko-Maßnahmen-Tabelle fortlaufend entwickelt.
3. Der Quellcode der App ist offen zu legen. Bisher war noch nicht genügend Zeit, die Dokumentation zur Entwicklung so aufzubereiten, wie das bei einem open source Projekt nicht nur üblich, sondern notwendig ist, um den Code einer unbestimmten Öffentlichkeit verständlich zu machen. Bis zur baldigen Fertigstellung der Dokumentation und der Veröffentlichung des Source-Codes sollte aber dennoch bereits Feedback zum Source-Code eingeholt werden. Der DSBA hat hierzu eine short-list von Organisationen (zB epicenter.works, noyb.eu) empfohlen. Die ersten Auslieferungen des Source-Codes auf dieser Basis sind am 9.4.2020 erfolgt.
4. Die Kommunikation über die Funktionen und Leistungen der App ist stetig zu verbessern. Die Menschen dürfen sich nicht in falscher Sicherheit wiegen – die App ist kein Ersatz für alle anderen Maßnahmen gegen die Pandemie und das muss ordentlich kommuniziert werden!
5. Die App sollte so bald wie möglich in Österreich oder zumindest innerhalb der EU gehostet werden, ohne auf die Infrastruktur amerikanischer Konzerne angewiesen zu sein. Allerdings zeigt sich hier eine seit langem gewachsene Abhängigkeit selbst der kritischen Infrastrukturen in sämtlichen EU Staaten von US-amerikanischen Tech-Diensten. Vielleicht führt die Corona-Krise dazu, sich des Problems weit über die App hinaus bewusst zu werden und als Rotes Kreuz hier neue europäische und österreichische Lösungen einzufordern und zu befördern.
6. Die App und die Server-Komponenten müssen möglichst bald einer professionellen IT-Security-Überprüfung (Audit) unterzogen werden. Der Audit-Bericht muss veröffentlicht werden.
7. Der Bericht zur Datenschutzfolgen-Abschätzung sollte so rasch wie möglich veröffentlicht werden.
8. Eine DSFA muss immer vor der „Ausrollung“ der Datenverarbeitung (=App) erfolgen, muss aber auch immer aktuell gehalten werden. Das heißt, dass bei Änderungen an der App-Funktionalität oder dem Backend die DSFA zu aktualisieren ist (wie auch die anderen datenschutzrelevanten Dokumente, insbesondere Datenschutz-Information und Einwilligungserklärung).

Für jene Risikominimierungsmaßnahmen, die aus unterschiedlichen Gründen nicht sofort umsetzbar sind, wurde ein entsprechender Zeitplan erstellt und laufend erweitert:

Release 1:
Inhalt: nur mit Meldung über das Vorliegen einer ärztlich bestätigten Infektion (ohne Symptom-Checker und Verdachtsmeldung); nur mit HandyNr ohne zusätzliche Attribute (Name, GebDat, Adresse); Freigabe Datenschutzbeauftragter: Dienstagabend 24.3.

Datum: Freigabe der Release, Mittwoch 25.3. in den Appstores verfügbar.

Release 1.1:
Inhalt: Digitaler Handshake und Symptom-Checker und Verdachtsmeldung mit Bestätigung oder Entwarnung
Datum: Donnerstag 9.4.2020

Release 1.1.3:
Inhalt: Deaktivierung der Statistik-Funktion und Umsetzung der weiteren Empfehlungen aus der Code-Analyse, wie in Kapitel 6.5 ersichtlich.
Datum: Mittwoch 22.4.2020

Release 1.2:

Inhalt: Widerruf der Krankmeldung, Empfehlungsfunktion, Verarbeitung der Telefonnummern bei einem österreichischen Anbieter
Datum: Dienstag 12.5.2020

Release 2.0:

Inhalt: Austausch des Technologie-Stacks für den automatischen „peer2peer-Handshake“
Der automatische digitale Handshake zwischen Geräten mit aktivierter Stopp Corona-App funktioniert nun durch das neue Google und Apple Framework auf allen Smartphones mit den Betriebssystemen Android (ab Version 6 mit Bluetooth Low Energy (BLE) von Google und iOS (ab Version 13.5.) von Apple.

Datum: 26.6.2020

Nächste geplante Release:
Inhalt Implementierung von DP-3T
Datum: offen, abhängig von der Entwicklung)

Die Datenschutz-Folgenabschätzung wird mit weiteren Versionierungen des DSFA-Berichts im Zuge der fortlaufenden Arbeit um diese weiteren risikominimierenden Maßnahmen ergänzt.

7.2 Entscheidung zur Konsultationspflicht (Art 36)

Aufgrund der getroffenen Maßnahmen besteht kein hohes Risiko und es erfolgt keine Konsultation nach Artikel 36 DSGVO.

7.3 Gegebenenfalls Entscheidungen zur Position des Datenschutzbeauftragten

Falls der Verantwortliche mit dem gemäß Art 35 Abs 2 DSGVO vom Datenschutzbeauftragten eingeholten Rat (oder Teilen davon) nicht einverstanden ist, sollte (Anm: durch den Verantwortlichen) eine (nachvollziehbare) Begründung für die mangelnde Beachtung des Ratschlags/der Ratschläge des

Datenschutzbeauftragten in den Bericht aufgenommen werden (so die Art-29-Datenschutzgruppe, WP 243 rev. 01, 17 unter Hinweis auf Art 24 Abs 1 DSGVO).[67]

Es gab keine wesentlichen Diskrepanzen zum Rat des Datenschutzbeauftragten, die Geschäftsleitung hat diesen bislang im vollen Umfang Folge geleistet. Einige ungelöste Probleme (zB Hosting ohne US-amerikanischen Tech-Anbieter) liegen nicht in der simplen Entscheidungssphäre des Verantwortlichen, sondern sind vielmehr Probleme, die der europäische Datenschutz in der Praxis noch gar nicht bewältigt hat. Die Gelegenheit wird aber genutzt, um europäischen Lösungen Vorschub zu leisten.

7.4 Feststellung künftiger Überprüfungen

Risikomanagement ist als Plan-Do-Check-Act-Zyklus anzusehen (in Anlehnung an ISO 31000), sodass künftige Überprüfungen auch eine Neuevaluation der relevanten Risiken beinhalten sollten. In diesem Zusammenhang ist auf Art 35 Abs 11 hinzuweisen. Erforderlichenfalls stößt der Verantwortliche eine Überprüfung an, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird. Die Bewertung und rechtliche Beurteilung erfolgt durch das Datenschutzteam in enger Abstimmung mit dem Verantwortlichen. Eine Bewertung ist jedenfalls anzustoßen, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Die App soll mit der Corona-Krise befristet sein und unterliegt derzeit einer ständigen Weiterentwicklung mit einer begleitenden Datenschutz-Folgenabschätzung. Eine Festlegung von Review-Zyklen im klassischen Sinn ist daher zu diesem Zeitpunkt nicht sinnvoll. Dies wird sich aber voraussichtlich und Erfahrungsgemäß aus einem zeitnahen professionellen und unabhängigen IT-Sicherheits-Audit ergeben. Festzuhalten ist, dass die Leistungen des Teams des hinzugezogenen Beratungsunternehmens Research Institute AG & Co KG (RI) keinesfalls als Audit darzustellen sind. RI ist in der Rolle des Beraters, die mit einer unabhängigen Auditierung unvereinbar ist. Es sind daher jedenfalls andere qualifizierte Organisationen oder Personen zu beauftragen.

8 Anlagen

Sämtliche Anlagen sind in der Datenschutz-Dokumentation des Österreichischen Roten Kreuzes, Generalsekretariat, abgelegt und dem ÖRK-Datenschutzteam zugänglich. Dies beinhaltet insbesondere technische Dokumentation, Spezifikationen, Produktbeschreibungen, Auftragsverarbeitungsverträge mit angeschlossenen Technisch- organisatorischen Maßnahmen. Bei der Übermittlung dieses Berichts wird nur der Bericht des Datenschutzbeauftragten angefügt. Die weitere Dokumentation ist auf Anfrage beim Datenschutz-Team (datenschutz@roteskreuz.at) jederzeit kurzfristig erhältlich. Im Zuge der weiteren Aufarbeitung mit den folgenden Releases wird auch trotz allen Zeitdrucks in der Krise die Dokumentation stetig verbessert. Eine strukturierte Auflistung der vorhandenen Dokumentation wird in einer späteren Version nachgeliefert.

[67] Stellungnahme liegt bei.

Quelle: Stopp_Corona_Sicherheitskonzept_v0R3 von Accenture vom 8.4.2020

1. ***Informationssicherheit in der Entwicklung***

Um **Informationssicherheit in der Entwicklung** zu gewährleisten, werden folgenden Maßnahmen durchgeführt:

- Die Accenture Entwicklungsrichtlinien für Web Entwicklung kommen zur Anwendung.
- Die Entwicklungs- und Testumgebung wird von der Produktionsumgebung **strikt getrennt**.
- Anwendung einer strikten **Versionskontrolle** der zu entwickelnden Software. Der Quellcode wird mit allen Änderungen und Ergänzungen in einem Versionskontrollsystem archiviert. Zu jedem Zeitpunkt kann jeder ausgelieferte Softwarestand rekonstruiert werden.
- Ablage der System- und Applikationskonfiguration im **Konfigurations-Management-System**. Durchgehende Verwendung von **Virenschutzsoftware** in der Entwicklungsumgebung.
- **Ein Architektur Review** beinhaltet die Überprüfung der geplanten Systemarchitektur der Stopp Corona-App bezüglich der Umsetzung der Sicherheitsprinzipien (Least Privilege, Need-to-Know, Redundanz, Defense in Depth, Vertraulichkeit, Integrität, Verfügbarkeit), der Korrektur bei Fehlern und der abschließenden Dokumentation des Ergebnisses.
- Festlegung von **Secure Coding Guidelines** zur sicheren Entwicklung. Die Richtlinien werden spezifisch für die Entwicklungssprache ausgewählt. Mithilfe einer **Secure Source Code Analyse** (SSCA) wird der Quellcode manuell bzw. maschinell auf sicherheitsrelevante Schwachstellen z.B. XSS, SQL Injection überprüft. Die SSCA ermöglicht frühzeitig die Erkennung einer unsicheren Programmierpraxis. Bei unzureichender Implementierung wird dem Entwickler dies als Fehler gemeldet.
- Anhand der geplanten Architektur werden **Security Testfälle** entwickelt und dokumentiert, die gezielt die Sicherheit der Komponenten der Stopp Corona-App überprüfen. Dabei werden sowohl für die implementierten Sicherheitsfunktionen als auch für das System selbst Testfälle erstellt, die vor allem nicht-systemkonforme Abläufe und Angriffe auf die IT-Systeme beinhalten. Diese Testfälle werden im Testplan dokumentiert.

2. ***Integrations- und Testphase***

- **Systemhärtung:**

  Für die gesamte „Stopp CoronaApp wird ein **Hardening Konzept** erstellt, durch welches Plattformkomponenten wie Betriebssysteme, Datenbanken, Applikationen, Webserver und weitere Komponenten einem entsprechenden Prozess der **Systemhärtung** unterzogen werden. Dies beinhaltet unter anderem die Deaktivierung von nicht verwendeten Diensten und Benutzerkennungen, die sichere Konfiguration der Web Services, der Einsatz von sicheren Kommunikationsprotokollen und weitere Maßnahmen zur Härtung der „Stopp Corona-App. Diese Maßnahmen werden dokumentiert und später als Teil der Installations-, Administrations- und Benutzer-Handbücher zur Verfügung gestellt.

- **Sicherheitstest:**

  Zur Überprüfung der korrekten Umsetzung der Sicherheitsanforderungen, Sicherheitsfunktionen und der Sicherheitsarchitektur werden **dezidierte Sicherheitstests**

durchgeführt. Diese Tests werden basierend auf den bestehenden Durchführungsunterlagen und dem Testplan zu abgestimmten Zeiten auf der Testanlage durchgeführt.

- **Last Test:**

  Es werden Last Tests vor den Livebetrieb geplant und durchgeführt.

- **PEN Test:**

  Es werden PEN Tests vor den Livebetrieb geplant und durchgeführt.

3. *Richtlinien in der Entwicklung*

In der Entwicklung bei Accenture kommen unter anderem die relevanten Accenture Richtlinien zu folgenden Themenbereichen zur Anwendung:

- Backup / Recovery
- Mobile Device Management
- Verhütung von Schadsoftware
- Protokollierung (SIEM)
- Zugriffsberechtigungen
- Klassifizierung von Daten
- Data Leakage Prevention (DLP)
- Virus Detektion
- Integrität und Vertraulichkeit von Daten
- Verschlüsselung der externen Kommunikation
- Business Continuity Management (BCM)

4. *Patch Management*

In Bezug auf das Backend entfällt, aufgrund des eingesetzten Plattform-as-a-Service Models, ein Großteil der Patch Management Aktivitäten auf den Zuständigkeitsbereich des Cloud Service Anbieters. Des Weiteren werden von den Herstellern der eigesetzten mobilen Betriebssysteme entsprechende Patches zur Verfügung gestellt. Das Entwicklungs- bzw. Betriebsteam hat die Aufgabe publizierte sicherheitsrelevante Patches zu evaluieren und bei Bedarf die einwandfreie Funktion der Applikation nach erfolgter Installation des Patches zu verifizieren. Außerdem werden gemäß den angeführten Richtlinien, im Zuge von regelmäßigen Wartungsarbeiten sicherheitsrelevante Patches für die Applikation selbst entwickelt, verifiziert und bereitgestellt. Die folgende Tabelle gibt einen Überblick über die Verantwortlichkeiten in Bezug auf die Entwicklung und Bereitstellung von sicherheitsrelevanten Patches.

Gegenstand	**Patch**			
	Entwicklung	**Bereitstellung**	**Auswirkungsanalyse**	**Beschreibung**
Applikation Source Code	Entwicklungsteam	Entwicklungsteam	Entwicklungsteam	Sicherheitsrelevante Patches werden

				vom internen Entwicklungsteam entwickelt, getestet und in regelmäßigen Abständen bereitgestellt (im Rahmen der angebotenen Leistungen).
Mobiles Betriebssystem	Google / Apple	Google / Apple		Neue, stabile Versionen der Betriebssysteme werden regelmäßig vom Hersteller entwickelt und bereitgestellt. Je nach Art der Änderungen wird ein Patch entweder als zusätzliche Version bereitgestellt oder es wird die nicht mehr aktuelle Version überschrieben. Details zu den jeweiligen Patches werden vom Hersteller frühzeitig kommuniziert. Das Betriebs- bzw. Entwicklungsteam ist dafür verantwortlich die Änderungen der kommunizierten Patches zu evaluieren und wenn nötig zu testen. Sollten Änderungen an der Applikation notwendig sein werden diese durch das Entwicklungsteam umgesetzt.
Backend	Microsoft	Microsoft		

SMS Gateway	Österreichisches Rotes Kreuz	Österreichisches Rotes Kreuz		Die Wartung des SMS Gateways obliegt der zuständigen Stelle des ÖRK. Sollten allfällige Änderungen die Kommunikation zwischen Backend und SMS Gateway beeinträchtigen ist das Betriebs- bzw. Entwicklungsteam darüber in Kenntnis zu setzen.

Tabelle: Sicherheitsrelevanten Patches: Verantwortlichkeiten und Bereitstellung

5. ***Aufbewahrungsfristen / Löschen von Daten***

Die Aufbewahrungsfristen und das Löschen von Daten wird separat für extern gespeicherte Daten in der mobilen Umgebung und die zentral im Backend gehaltenen Daten ausgeführt.

Stopp Corona-App:

- Eine Aufhebung von nicht bestätigten Verdachtsmeldungen ist durch den Benutzer möglich. Die Aufhebung der Verdachtsmeldung in der App führt ebenso zur Aufhebung der entsprechenden Meldung im Backend und bei den entsprechenden Kontakten.
- Eine Deinstallation der Stopp Corona-App durch den Benutzer entfernt alle Daten auf dem Mobilgerät. Dies betrifft digitale Handshakes, Zufalls-IDs und ebenso erzeugte Schlüssel (privater und öffentlicher).
- Die digitalen Handshakes des Benutzers sind für die letzten 14 Tage verfügbar und werden danach automatisch gelöscht.

Backend:

- Im Backend bereinigen „Clean Jobs“ Kontakte und Meldungsdaten, welche älter als 8 Wochen sind.
  Hinweis: Diese Daten stehen dann nur mehr in aggregierter Form (ohne APP-UUID) als Statistik zur Verfügung.
- Für Telefonnummern, welche zur Meldung einer Erkrankung (Verdacht auf Infektion oder bestätigte Infektion) angegeben wurden, erfolgt die Löschung nach einer Frist von 30 Tagen.

6. ***Zugriffsberechtigung***

Die Passwortvergabe folgt den Accenture Richtlinien definiert in *Identification and Authentication Standard Version 6.9*.

Folgende Rollen sind in der Entwicklung und im Betrieb vorgesehen.

Stopp Corona-App-Entwicklung/Test:

Rolle	Entwicklungs- /Test Umgebung	AppStores	Info
App Entwicklung	X		
App Lead Entwickler	X	X	Deployment
App Test	(X)		Eingeschränkter Zugriff auf Entwicklungssystem

Tabelle: Rollen und Berechtigungen App-Entwicklung

Stopp Corona **Backend** Entwicklung/Test:

Rolle	Entwicklungs- /Test System	Produktivsystem	Info
Backend Entwicklung	X		
Backend Lead Entwickler	X	X	Deployment, Unterstützung des Betriebes bei Fehler und Last Analyse
Backend Test	(X)		Eingeschränkter Zugriff auf Entwicklungssystem
Backend Betrieb	(X)	X	Eingeschränkter Zugriff auf Entwicklungssystem für Rücksicherung (Test der Sicherungen)

Tabelle: Rollen und Berechtigungen Backend Entwicklung

Stopp Corona **Statistik** Entwicklung/Test:

Rolle	Statistik Entwicklungs- /Test System	Statistik Produktivsystem	Info
Statistik Entwicklung	X		
Statistik Lead Entwickler	X	X	Deployment, Unterstützung des Betriebes bei Fehler und Last Analyse
Statistik Test	(X)		Eingeschränkter Zugriff auf das Statistik - Entwicklungssystem
Statistik Betrieb	(X)	X	Eingeschränkter Zugriff auf Entwicklungssystem für Rücksicherung (Test der Sicherungen)

Tabelle: Rollen und Berechtigungen Statistik Entwicklung

7. ***Protokollierung***

Plattformprotokolle liefern detaillierte Diagnose- und Überwachungsinformationen für Azure-Ressourcen bzw. die Azure-Plattform und werden automatisch generiert. Aus sicherheitsrelevanter Sicht werden drei verschiedene Logkategorien protokolliert:

Log	**BESCHREIBUNG**
Ressourcenprotokolle	Sie bieten einen Einblick in Vorgänge, die innerhalb einer Azure-Ressource (der Datenebene) ausgeführt wurden, z.B. das Abrufen eines Geheimnisses aus einem Key Vault oder die Ausgabe einer Anforderung an eine Datenbank. Der Inhalt dieser Protokolle variiert je nach Azure-Dienst und -Ressourcentyp.
Aktivitätsprotokoll	Bietet Einblicke in die Vorgänge für jede Azure-Ressource im Abonnement von außen (die Verwaltungsebene) sowie Aktualisierungen zu Service Health-Ereignissen. Das Aktivitätsprotokoll dient zur Ermittelung der Antworten auf die Fragen Was, Wer und Wann für alle Schreibvorgänge (PUT, POST, DELETE), die für die Ressourcen des Abonnements durchgeführt wurden. Es gibt jeweils ein Aktivitätsprotokoll für jedes Azure-Abonnement.
Azure Active Directory-Protokolle	Enthält den Verlauf der Anmeldeaktivität und das Überwachungsprotokoll der Änderungen, die in Azure Active Directory für einen bestimmten Mandanten vorgenommen wurden.

Die Überwachung der Azure Functions, über welche die zentrale Logik im Backend implementiert ist, wird mit Hilfe der verfügbaren Integration von **Azure Applikation Insights** realisiert. Es werden Protokoll-, Leistungs- und Fehlerdaten erfasst.

Die Protokolle sind gegen Veränderung (verschlüsselt abgelegt), unberechtigten Zugriff (Anzeige über eingeschränkte Benutzerberechtigungen) und gegen Löschen geschützt.

8. ***Backup / Recovery***

Das regelmäßige Backup der Applikationsdaten (Konfiguration) und der Stopp Corona Daten (Datenbank) erfolgt aufgrund des eingesetzten Plattform-as-a-Service Models durch den Cloud Service Anbietern.

Es erfolgt eine tägliche Sicherung der Konfigurations- und Logdaten und alle 12 Stunden eine Delta Sicherung der Datenbank. Das Transaktionsprotokoll der Datenbank wird alle 10 Minuten gesichert.
Für die Datenbank erfolgt eine wöchentliche Vollsicherung welche 3 Wochen vorgehalten wird.

Das Backup wird regelmäßig durch das Betriebsteam mittels Rücksicherung auf das Entwicklungssystem überprüft.
Die Durchführung der Rücksicherungstests wird vermerkt.

9. ***Dienstleister / Services***

- Neben dem primären Auftragsverarbeiter Accenture bestehen folgende weitere Dienstleister:

- **Microsoft Corporation**

  Hosting der Dienste: Microsoft Azure Cloud (Region EU West)
  Dept. 551, Volume Licensing
  6100 Neil Road, Suite 210
  Reno, Nevada 89511-1137
  USA

- **World-Direct eBusiness solutions GmbH**
  Hosting der Dienste zur Ansteuerung des SMS Gateways mittels Telefonnummer & TAN, TAN Erzeugung und Validierung
  Lassallestrasse 9
  1020 Wien

- **Rotes Kreuz**

  SMS Gateway: Österreichisches Rote Kreuz (ÖRK), Wiedner Hauptstraße 32,
  A-1040 Wien