

Datenschutzerklärung

In dieser Datenschutzerklärung erfahren Sie, wie Ihre Daten verarbeitet werden und welche Datenschutzrechte Sie haben, wenn Sie die offizielle Corona-Warn-App der deutschen Bundesregierung nutzen.

Folgende Themen werden behandelt:

1. Wer ist Herausgeber der Corona-Warn-App?
2. Ist die Nutzung der App freiwillig?
3. Auf welcher Rechtsgrundlage werden Ihre Daten verarbeitet?
4. An wen richtet sich die App?
5. Welche Daten werden verarbeitet?
6. Wofür werden Ihre Daten verarbeitet?
7. Wie funktioniert das länderübergreifende Warnsystem?
8. Welche Berechtigungen benötigt die App?
9. Wann werden Ihre Daten gelöscht?
10. An wen werden Ihre Daten weitergegeben?
11. Werden Ihre Daten in Länder außerhalb der EU übermittelt?
12. Wie können Sie Ihr Einverständnis zurücknehmen?
13. Welche weiteren Datenschutzrechte haben Sie?
14. Datenschutzbeauftragte und Kontakt

Damit dieser Text für alle Nutzer verständlich ist, bemühen wir uns um eine einfache und möglichst untechnische Darstellung.

1. Wer ist Herausgeber der Corona-Warn-App?

Diese App wird vom Robert Koch-Institut (**RKI**) für die deutsche Bundesregierung herausgegeben. Das RKI ist auch dafür verantwortlich, dass Ihre personenbezogenen Daten in Übereinstimmung mit den Vorschriften über den Datenschutz verarbeitet werden.

Wenn Sie nach einem positiven Corona-Test per App eine länderübergreifende Warnung auslösen, können auch die Nutzer von offiziellen Corona-Apps anderer Länder, denen Sie begegnet sind, gewarnt werden. In diesem Fall sind das RKI und die zuständigen Gesundheitsbehörden der an den jeweiligen länderübergreifenden Warnsystemen

teilnehmenden Länder für die Datenverarbeitung gemeinsam verantwortlich. Einzelheiten erfahren Sie unter Punkt 7.

2. Ist die Nutzung der App freiwillig?

Die Nutzung der App ist freiwillig. Es ist allein Ihre Entscheidung, ob Sie die App installieren, welche App-Funktionen Sie nutzen und ob Sie Daten mit anderen teilen. Grundsätzlich holen die Haupt-Funktionen der App, die eine Weitergabe Ihrer personenbezogenen Daten erfordern, vorher Ihr ausdrückliches Einverständnis ein.

Im Zusammenhang mit den offiziellen digitalen COVID-Zertifikaten (COVID-Testzertifikat, COVID-Impfzertifikat und COVID-Genesenenenzertifikat) gibt es neue gesetzliche Grundlagen für die Erstellung der Nachweise. In diesem Zusammenhang ist daher keine zusätzliche Einwilligung erforderlich. Die Zertifikate werden aber nur erstellt, wenn Sie dies wünschen. Die Anforderung und Verwendung der digitalen COVID-Zertifikate ist freiwillig.

Falls Sie ein Einverständnis nicht erteilen oder nachträglich zurücknehmen oder keine digitalen COVID-Zertifikate anfordern, entstehen Ihnen keine Nachteile.

3. Auf welcher Rechtsgrundlage werden Ihre Daten verarbeitet?

Ihre Daten werden im Zusammenhang mit den Funktionen der App grundsätzlich nur auf Grundlage Ihres Einverständnisses verarbeitet. Dies umfasst z. B. die Datenverarbeitung zur Risiko-Ermittlung und der Warnung Anderer, die Überprüfung von COVID-Zertifikaten bei Ticketbuchungen sowie die Verarbeitung von Daten in COVID-Zertifikaten bei der Aktualisierung von Zertifikaten (siehe 6 o.). Die Rechtsgrundlage ist jeweils Art. 6 Abs. 1 S. 1 lit. a DSGVO sowie im Falle von Gesundheitsdaten Art. 9 Abs. 2 lit. a DSGVO. Informationen zu Ihrem Widerrufsrecht finden Sie unter Punkt 12.

Im Zusammenhang mit den offiziellen digitalen COVID-Zertifikaten (COVID-Testzertifikat, COVID-Impfzertifikat und COVID-Genesenenenzertifikat) ist die Datenverarbeitung überwiegend gesetzlich geregelt. Die Erstellung und Bescheinigung von Impfzertifikaten erfolgt auf Basis von Art. 9 Abs. 2 lit. g DSGVO i.V.m § 22a Abs. 5 IfSG. Die Erstellung und Bescheinigung von Testzertifikaten erfolgt auf Basis von Art. 9 Abs. 2 lit. g DSGVO i.V.m § 22a Abs. 7 IfSG. Die Erstellung und Bescheinigung von Genesenenenzertifikaten erfolgt auf Basis von Art. 9 Abs. 2 lit. g DSGVO i.V.m § 22a Abs. 6 IfSG. Die Verarbeitung von Zugriffsdaten in Zusammenhang mit der Funktion „Gültigkeit prüfen“, der Prüfung der Regeln für die Empfehlungen für Auffrischungsimpfungen sowie der Bereitstellung von Informationen zur Aktualisierung von Zertifikaten erfolgt auf Basis von Art. 6 Abs. 1 lit. e DSGVO i.V.m § 3 BDSG. Die vorübergehende Speicherung der Hash-Werte der Signatur bei der Aktualisierung von Zertifikaten (siehe Punkt 6.o.) erfolgt auf Grundlage von § 22 Abs. 1 lit. c BDSG und Art. 9 Abs. 2 lit. i DSGVO.

Die Verarbeitung von Zugriffsdaten für die Bereitstellung der täglichen Statistiken (siehe hierzu Punkt 6.f.) erfolgt im Rahmen der Information der Öffentlichkeit durch das RKI gem. § 4 Abs. 4 BGA-NachfG auf Basis von Art. 6 Abs. 1 lit. e. DSGVO i.V.m § 3 BDSG.

4. An wen richtet sich die App?

Die App richtet sich an Personen, die sich in Deutschland aufhalten und mindestens 16 Jahre alt sind.

5. Welche Daten werden verarbeitet?

Das gesamte System der App ist so programmiert, dass für die Kernfunktionen so wenig personenbezogene Daten wie möglich verarbeitet werden. Das bedeutet, dass das System bei der Risiko-Ermittlung, der Warnung anderer und dem Abruf des Testergebnisses keine Daten erfassen muss, die es dem RKI oder anderen Nutzern ermöglichen, auf Ihre Identität, Ihren Namen, Ihren Standort oder andere persönliche Details zu schließen.

Ausnahmen gelten für die ergänzenden Funktionen „Schnelltest-Ergebnis nachweisen“, mit der Sie eine auf Ihren Namen ausgestellte Bestätigung für negative Schnelltest-Ergebnisse anzeigen lassen können (siehe hierzu Punkt 6.c.), die Funktion zum Anlegen eines „Schnelltest-Profiles“, mit der Sie einer Teststelle die zur Durchführung eines Schnelltests erforderlichen Daten bereitstellen können (siehe hierzu Punkt 6.d.) und wenn Sie digitale COVID-Zertifikate in der App hinzufügen (siehe hierzu Punkt 6.h.) oder aktualisieren (siehe hierzu Punkt 6.o.) oder im Rahmen einer Ticketbuchung überprüfen lassen (siehe hierzu Punkt 6.k.).

Die App verzichtet standardmäßig auf die Auswertung Ihres Nutzungsverhaltens durch Analyse-Tools. Nur wenn Sie ausdrücklich der freiwilligen Datenspende zustimmen oder einen Fehlerbericht aufzeichnen und mit dem RKI teilen, werden bestimmte Daten über Ihre Nutzung der App an das RKI übermittelt (siehe hierzu Punkt 5.j. und Punkt 5.m.).

Die von der App verarbeiteten Daten lassen sich den folgenden Kategorien zuordnen:

a. Zugriffsdaten

Bei jedem Internet-Datenaustausch der App mit dem Serversystem des RKI (im Folgenden: **Serversystem**) werden vom Serversystem sogenannte Zugriffsdaten verarbeitet. Dies ist erforderlich, damit die App aktuelle Daten (z. B. für Warnungen) abrufen oder bestimmte auf dem Smartphone gespeicherte Daten an das Serversystem übermitteln kann. Die Zugriffsdaten umfassen folgende Daten:

- IP-Adresse
- Datum und Uhrzeit des Abrufs
- übertragene Datenmenge (bzw. Paketlänge)
- Meldung, ob der Datenaustausch erfolgreich war

Diese Zugriffsdaten werden verarbeitet, um den technischen Betrieb der App und des Serversystems aufrechtzuerhalten und abzusichern. Sie werden dabei nicht als Nutzer der App persönlich identifiziert und es wird kein Nutzungsprofil erstellt. Eine Speicherung der IP-Adresse über das Ende des Nutzungsvorgangs hinaus erfolgt nicht.

Um eine unbefugte Zuordnung Ihrer Daten anhand Ihrer IP-Adresse schon während eines Nutzungsvorgangs zu verhindern, greift die App nur über einen speziellen Eingangsserver auf das Serversystem zu. Der Eingangsserver leitet die von der App angeforderten oder übermittelten Daten dann ohne die IP-Adresse an den jeweils zuständigen Server weiter, so dass die IP-Adresse innerhalb des Serversystems nicht verarbeitet wird.

b. Begegnungsdaten

Sobald Sie das COVID-19-Benachrichtigungssystem Ihres iPhones (dort „Begegnungsmittelungen“ genannt) oder Ihres Android-Smartphones (dort „COVID-19-Benachrichtigungen“ genannt) aktivieren, sendet Ihr Smartphone per Bluetooth sogenannte

Begegnungsdaten aus, die von anderen Smartphones in Ihrer Nähe aufgezeichnet werden können. Umgekehrt empfängt Ihr Smartphone auch die Begegnungsdaten von anderen Smartphones. Die ausgesendeten Begegnungsdaten umfassen:

- zufällige Kennnummern (im Folgenden: **Zufalls-IDs**)
- Bluetooth-Protokollversion
- Bluetooth-Sendeleistung in Dezibel Milliwatt (dBm)

Bei aufgezeichneten Begegnungen umfassen die Begegnungsdaten zusätzlich:

- Tag, Zeitpunkt und Dauer der Begegnung
- Bluetooth-Empfangsstärke in dBm

Die Zufalls-IDs werden regelmäßig geändert. Dies trägt dazu bei, dass Ihr Smartphone nicht über diese Zufalls-IDs identifiziert werden kann. Die von Ihrem Smartphone ausgesendeten eigenen Begegnungsdaten und die aufgezeichneten Begegnungsdaten der Personen, mit denen Sie Kontakt hatten, werden auf Ihrem Smartphone gespeichert und jeweils nach 14 Tagen gelöscht. Auf die gleiche Weise werden Ihre ausgesendeten Begegnungsdaten verarbeitet, wenn sie von den Smartphones anderer App-Nutzer aufgezeichnet werden.

Bitte beachten Sie: Das COVID-19-Benachrichtigungssystem ist eine Funktion Ihres Betriebssystems. Anbieter und Verantwortliche für dieses System sind daher Apple (wenn Sie ein iPhone haben) und Google (wenn Sie ein Android-Smartphone haben). Insoweit unterliegt die Datenverarbeitung den Datenschutzbestimmungen dieser Unternehmen und liegt außerhalb des Verantwortungs- und Einflussbereichs des RKI. Die tatsächlichen Bezeichnungen, Bedienschritte und Einstellmöglichkeiten können je nach Version und Einstellung Ihres Betriebssystems von der Darstellung in dieser Datenschutzerklärung abweichen. Weitere Informationen stellen Ihnen die jeweiligen Hersteller zur Verfügung:

- Informationen von Google für Android-Smartphones finden Sie auf Ihrem Gerät unter „Einstellungen“ > Google > COVID-19-Benachrichtigungen unter dem Link „Weitere Informationen“
- Informationen von Apple für iPhones finden Sie auf Ihrem Gerät unter „Einstellungen“ > "Begegnungsmitteilungen" unter dem Link „So funktionieren Begegnungsmitteilungen ...“.

c. Schnelltestdaten

Sie können die Ergebnisse der von Ihnen bei einer Teststelle durchgeführten Antigen-Schnelltests über die App abrufen. Sollten Sie dieses Angebot wahrnehmen, wird Ihre Teststelle einen individuellen QR-Code für Sie erzeugen, den Sie mit der App scannen müssen. Der QR-Code enthält in kodierter Form eine eindeutige Kennzahl für Ihren Schnelltest sowie den Testzeitpunkt. Sofern Sie im Fall eines negativen Schnelltest-Befunds zu Nachweiszwecken eine namentliche Darstellung des Testergebnisses in der App wünschen (siehe zu dieser Funktion Punkt 6 c.), enthält der QR-Code in kodierter Form weitere von Ihnen angegebene Daten. Sie können die App auch verwenden, um die Testergebnisse von Familienmitgliedern abzurufen. Der Name des Familienmitglieds, den Sie hierbei in der App angeben, wird nur lokal auf Ihrem Smartphone gespeichert. Anhand eines positiven Testergebnisses eines Familienmitgliedes können Sie nicht andere warnen.

d. Schnelltest-Profil

Sie können Angaben zu Ihrer Person in Ihrem Schnelltest-Profil in der App speichern. Das Schnelltest-Profil umfasst folgende Felder: Vorname, Nachname, Geburtsdatum, Straße und Hausnummer, PLZ, Stadt, Telefonnummer, E-Mail-Adresse. Die App wandelt Ihre Daten dann in Ihren persönlichen QR-Code um, der alle von Ihnen eingegebenen Daten enthält. Das Anlegen eines Schnelltest-Profiles in der App und dessen Verwendung in einer Teststelle sind freiwillig. Sie entscheiden selbst, welche Daten Sie in Ihrem Schnelltest-Profil eintragen. Nur diese Daten sind im QR-Code enthalten. Sollte die Teststelle weitere Angaben benötigen, die nicht im QR-Code enthalten sind, können Sie diese der Teststelle auch auf andere Weise mitteilen.

e. Event-Daten

Wenn Sie ein Event (beispielsweise eine Feier oder ein Konzert) oder einen Ort (beispielsweise ein Geschäft oder ein Restaurant) besuchen, können Sie Ihren Aufenthalt in der App erfassen. Hierfür können Veranstalter von Events oder Inhaber eines Geschäfts den Gästen einen QR-Code zur Verfügung stellen.

Als Gast können Sie diesen QR-Code beim Ankommen mit der App einfach einscannen und sich so „einchecken“. Beim Verlassen des Events oder Ortes können Sie sich in der App wieder „auschecken“. Die App merkt sich dann, dass und wann Sie bei dem betreffenden Event oder Ort gewesen sind. Sollte ein Gast später Corona-positiv getestet werden und über die App eine Warnung auslösen, werden alle Gäste gewarnt, die zeitgleich eingeklickt waren.

Wenn Sie als Gast einen QR-Code scannen, werden die vom Gastgeber angegebenen Event-Details (Bezeichnung des Events/Ortes, Adresse/Ort, typische Aufenthaltsdauer und ggf. Startzeit des Events) sowie die Check-in-Zeit auf Ihrem Smartphone gespeichert. Zudem leitet Ihre App anhand der im QR-Code enthaltenen Informationen eine dem Event eindeutig zuordenbare verschlüsselte Kennung (im Folgenden: **Event-ID**) ab. Aus der Event-ID ergeben sich keine Rückschlüsse auf das Event oder den Ort. Wenn Sie sich in der App auschecken oder nach Ablauf der vom Gastgeber voreingestellten Zeit automatisch ausgecheckt werden, wird der Auscheck-Zeitpunkt auf Ihrem Smartphone gespeichert.

Außerdem wird standardmäßig ein Eintrag in Ihrem Kontakt-Tagebuch angelegt. Die Einzelheiten hierzu werden unter Punkt 5 g. und 6 g. erläutert. Wenn Sie für ein Event oder Ort keinen Eintrag in Ihrem Kontakt-Tagebuch anlegen möchten, können Sie diese Funktion einfach über den entsprechenden Schieberegler ausschalten.

Sie können Ihre bisherigen Check-ins unter „Meine Check-ins“ überprüfen, löschen und den Auscheck-Zeitpunkt anpassen.

Als Gastgeber können Sie einen QR-Code für Ihre Gäste erstellen, damit diese sich bei Ihrem Event oder Ort einchecken können.

In dem QR-Code zu dem Event oder Ort werden die von Ihnen angegebenen Event-Details sowie eine zufällige Kennzahl gespeichert. Die zufällige Kennzahl gewährleistet, dass unterschiedliche Orte und Events, für die dieselben Event-Details festgelegt wurden, später über unterschiedliche Event-IDs verfügen. Die von Ihnen erstellten QR-Codes sind auf Ihrem Smartphone gespeichert. Sie können Ihre selbst erstellten QR-Codes unter „Meine QR-Codes“ jederzeit löschen. Bedenken Sie jedoch, dass Sie einen QR-Code benötigen, um Ihre Gäste zu warnen, die bei dem Event oder Ort eingeklickt waren.

f. Gesundheitsdaten

Gesundheitsdaten sind alle Daten, die Informationen zum Gesundheitszustand einer Person enthalten. Dazu gehören nicht nur Angaben zu früheren und aktuellen Krankheiten, sondern auch zu Krankheitsrisiken einer Person (z. B. das Risiko, dass eine Person sich mit dem Coronavirus angesteckt hat). Die App verarbeitet Gesundheitsdaten in folgenden Fällen:

- wenn eine Risiko-Begegnung erkannt wird
- wenn Sie über die App ein Testergebnis abrufen
- wenn Sie Ihre Begegnungen und Gäste von zeitgleich besuchten Events oder Orten über die App vor einer möglichen Infektion warnen
- wenn Sie Angaben zum Beginn von eventuellen Corona-Symptomen machen oder
- wenn Sie digitale COVID-Zertifikate (Impfzertifikate, Testzertifikate oder Genesenzertifikate) in der App hinzufügen.

Die Einzelheiten werden unter Punkt 6 erläutert.

g. Einträge im Kontakt-Tagebuch

Wenn Sie im Kontakt-Tagebuch notieren, wann und wo Sie welche Personen getroffen haben und Umstände der Begegnung oder Kontaktdaten zu Personen und Orten vermerken, werden diese Angaben verschlüsselt auf Ihrem Smartphone gespeichert. Die Kontakt-Tagebuch-Einträge dienen nur Ihnen als Gedächtnisstütze. Das RKI oder andere Stellen können auf die Einträge im Kontakt-Tagebuch nicht zugreifen. Das Kontakt-Tagebuch kann Ihnen helfen, Ihre persönlichen Kontakte der letzten 14 Tage nachzuvollziehen. Falls Sie Corona-positiv getestet werden sollten und das Gesundheitsamt Ihre Mithilfe bei der Kontaktnachverfolgung erbittet, können Sie dem Gesundheitsamt somit schnell die benötigten Informationen mitteilen.

Die Nutzung des Kontakt-Tagebuchs ist freiwillig. Sie entscheiden selbst über die Speicherung der Einträge im Kontakt-Tagebuch. Sie sind insofern auch selbst für Ihre Einträge verantwortlich. Respektieren Sie daher bitte die Privatsphäre der Personen, die Sie in Ihr Kontakt-Tagebuch aufnehmen. Die Einträge sollen nicht an Dritte und nicht über unsichere Kommunikationskanäle weitergegeben werden. Das zuständige Gesundheitsamt wird Ihnen mitteilen, welche Informationen es für die Kontaktnachverfolgung von Ihnen benötigt und wie Sie diese zur Verfügung stellen können.

h. Daten über Ihre Corona-Impfung (Daten im COVID-Impfzertifikat)

Sie können Ihre offiziellen Impfzertifikate (digitale COVID-Impfzertifikate) in der App hinzufügen. Die Anforderung des digitalen Impfzertifikats ist freiwillig. Sollten Sie dieses Angebot wahrnehmen, erhalten Sie bei der Impfung einen Ausdruck mit einem QR-Code. In diesem sind die folgenden Daten zu Ihrer Corona-Impfung kodiert:

- Daten zu Ihrer Person (Name, Vorname, Geburtsdatum)
- Informationen zum Impfstoff (Krankheit, Impfstoff, Produkt, Hersteller)
- Informationen zur Impfung (Dosennummer, Gesamtdosen, Impfdatum, Land, Aussteller)
- Elektronische Signatur des RKI
- Eindeutige Kennung des Impfzertifikats.

Die Daten werden in der App gespeichert, sobald Sie den QR-Code zum digitalen Impfzertifikat scannen. Diese Daten wurden zuvor bei Ihrer Impfung erhoben.

i. Daten über Ihre Genesung (Daten im COVID-Genesenenzertifikat)

Sie können Ihre offiziellen Genesenenzertifikate (digitale COVID-Genesenenzertifikate) in der App hinzufügen. Die Anforderung des digitalen Genesenenzertifikats ist freiwillig. Nach Anforderung des Genesenenzertifikats, erhalten Sie von dem Arzt einen Ausdruck mit einem QR-Code. In diesem sind die folgenden Daten zu Ihrer Genesung kodiert:

- Daten zu Ihrer Person (Name, Vorname, Geburtsdatum)
- das Datum der Testung
- Angaben zur Testung, einschließlich der Art der Testung, und zum Aussteller
- Elektronische Signatur des RKI
- Eindeutige Kennung des Genesenenzertifikats.

Die Daten werden in der App gespeichert, sobald Sie den QR-Code des digitalen Genesenenzertifikats scannen. Diese Daten hat der Arzt bei Anforderung des Zertifikats von Ihnen erhoben.

j. Daten im COVID-Testzertifikat

Sie können über die App offizielle Testzertifikate (digitale COVID-Testzertifikate) anfordern. Die Anforderung eines digitalen Testzertifikats ist freiwillig und erfolgt nur, wenn ein negatives Testergebnis vorliegt. Sie erhalten dann ihr Testzertifikat mit einem QR-Code in der App. In diesem sind die folgenden Daten zu Ihrem Testergebnis enthalten:

- Daten zu Ihrer Person (Name, Vorname, Geburtsdatum)
- Informationen zum Test (Krankheit, Art des Tests, Produkt, Hersteller)
- Informationen zur Testdurchführung (Datum und Uhrzeit des Tests, Ort an dem sich das Testzentrum befindet)
- Testergebnis
- Elektronische Signatur des RKI
- Eindeutige Kennung des Testzertifikats.

Die Daten werden in der App gespeichert, sobald Ihr Testergebnis vorliegt.

k. Buchungsdaten

Wenn Sie über das Internet bei einem Reise- oder Veranstaltungsunternehmen oder einem sonstigen Anbieter eine Buchung vornehmen, können Sie die App zum Nachweis eines gültigen digitalen COVID-Zertifikats gegenüber dem jeweiligen Anbieter nutzen (Zertifikatsprüfung bei Ticketbuchungen). Voraussetzung hierfür ist, dass Sie in der App ein digitales COVID-Zertifikat hinzugefügt haben. Zudem muss der jeweilige Anbieter an einen Überprüfungs-service angebunden sein.

Zur Zertifikatsprüfung benötigen Sie einen speziellen QR-Code, den Sie im Rahmen des Buchungsvorgangs von dem jeweiligen Anbieter erhalten. Dieser QR-Code enthält eine eindeutige Transaktions-ID, eine kurze Beschreibung des Buchungsvorgangs (z. B. „Buchungsnummer 1234“) und eine Internetadresse (URL).

Die App nutzt diese Informationen, um beim Anbieter technische Spezifikationen sowie die folgenden Details zur Buchung abzurufen, die für die Überprüfung des COVID-Zertifikats berücksichtigt werden sollen:

- Ihren Namen
- Ihr Geburtsdatum
- Angaben zum Datum der erforderlichen Gültigkeit des COVID-Zertifikats (Reisedatum oder Veranstaltungsdatum)
- Bei Reisen: Ausgangsland und Zielland
- Nachweisanforderungen, insbesondere also die zum Nachweis geeigneten Zertifikatstypen, wie z.B. Impfzertifikat (bei grenzüberschreitenden Reisen auch die Anforderungen des Ziellandes)
- Bei bestimmten Buchungen werden zusätzlich auch Angaben zur Veranstaltungsart mitgeteilt (z. B. Konzert oder Großveranstaltung).

Welche konkreten Informationen für die Überprüfung des COVID-Zertifikats verwendet werden sollen und welche COVID-Zertifikate als Nachweis zugelassen sind, wird vom jeweiligen Anbieter individuell festgelegt.

I. Nutzungsdaten (Datenspende)

Wenn Sie die Datenspende aktivieren, übermittelt die App bestimmte Daten über Ihre App-Nutzung einmal täglich an das RKI (im Folgenden: **Nutzungsdaten**). Diese Nutzungsdaten betreffen die von der App angezeigten Risiko-Begegnungen, erhaltene und ausgelöste Warnungen, abgerufene Testergebnisse sowie technische Angaben über das Betriebssystem Ihres Smartphones.

Im Einzelnen umfassen die Nutzungsdaten:

- Das Datum der Datenspende (d. h. der Tag der Übermittlung).
- Änderungen der Warnungshistorie im Vergleich zum Vortag.
- Welcher Risikostatus zum Zeitpunkt der Datenspende angezeigt wurde.
- Angaben dazu, auf welcher Grundlage welcher Begegnungen der Risikostatus berechnet wurde.
- Angaben zum Modell und der Version Ihres Smartphones und zur Version Ihrer App sowie dem verwendeten Betriebssystem.

Wenn Sie ein Testergebnis über die App abgerufen haben:

- Ob es sich um ein positives oder negatives Testergebnis handelt.
- Welches Risiko zum Zeitpunkt der Testregistrierung angezeigt wurde.
- Wieviel Zeit seit der letzten Risiko-Begegnung und deren Anzeige in der App bis zur Testregistrierung jeweils vergangen ist.
- Ob Sie die Funktion zum Auslösen einer Warnung gestartet haben und, falls ja, bis zu welchem Schritt Sie dabei gekommen sind (z. B. bis zur Symptomabfrage).

Wenn Sie eine Warnung ausgelöst haben:

- Ob Sie Angaben zum Symptombeginn gemacht haben.
- Wann Sie Ihr Einverständnis zur Warnung anderer erteilt haben (vor oder nach der Testregistrierung).

- Ob Sie den Warnprozess bis zum Ende vollständig durchlaufen haben oder ob Sie den Prozess vorher abgebrochen haben (etwa, weil Sie nicht die Bestätigung der erfolgreichen Übermittlung Ihrer Daten abgewartet haben).
- Die Test-Art, die Grundlage für die Warnung war
- Wie viele Stunden es gedauert hat, bis Sie Ihr Testergebnis nach der Testregistrierung erhalten haben.
- Wie viele Tage seit der letzten Mitteilung eines hohen Risikos vor Auslösen der Warnung vergangen sind.
- Wie viele Stunden seit der Testregistrierung vergangen sind.

Zusätzlich können Sie weitere optionale Angaben zu Ihrer Region sowie zu Ihrer Altersgruppe machen, die zusammen mit den Nutzungsdaten an das RKI übermittelt werden.

m. Teilnahme an einer Befragung

Einigen Nutzern wird in der App die Teilnahme an einer Befragung des RKI angeboten. In der Regel wird das Angebot zur Teilnahme an der Befragung abhängig von bestimmten in der App registrierten Ereignissen sein (z.B. der Anzeige eines erhöhten Risikos). Mit der Teilnahme an der Befragung helfen Sie dem RKI, die Wirksamkeit der App zu bewerten, die App zu verbessern und beispielsweise zu verstehen, ob und wie Warnungen über die App dabei helfen, weitere Infektionen zu verhindern.

n. Inhalte der Fehlerberichte

Um den technischen Support der App bei der Fehleranalyse zu unterstützen, können Sie in der App einen Fehlerbericht aufzeichnen. Wenn Sie die Aufzeichnung des Fehlerberichts starten, werden

- Ihre Bedienschritte in der App,
- die technischen Schritte und Abläufe sowie Statusmeldungen
 - zur Risiko-Ermittlung (z.B. zur Funktionsweise der Verarbeitung der Begegnungsdaten, der Berechnung des Infektionsrisikos, der Aktualisierung der Positiv-Listen, der Anzeige des errechneten Risikostatus),
 - zum Abruf und der Anzeige von Testergebnissen und
 - zu möglichen Vorgängen zur Warnung Anderer (z.B. die Berechnung von Übertragungsrisiko-Werten und die technische Bereitstellung Ihrer Zufalls-IDs durch Ihr Smartphone)

umfassend aufgezeichnet und auf Ihrem Smartphone gespeichert. Im Fehlerbericht können auch Gesundheitsdaten enthalten sein, weil auch die technischen Schritte und Abläufe im Zusammenhang mit der Erkennung einer Risiko-Begegnung aufgezeichnet werden.

Der Fehlerbericht enthält jedoch keine Informationen über QR-Codes für die Testregistrierung, das in Ihrer App gespeicherte Token (siehe dazu unten Punkt 6 b. unter „Testergebnis abrufen“), Schnelltest-Ergebnisse, digitale COVID-Zertifikate und Einträge in Ihrem Kontakt-Tagebuch. Der Fehlerbericht enthält auch nicht Ihren Namen oder andere Angaben, mit denen Sie vom RKI identifiziert werden können.

Sie können die Aufzeichnung des Fehlerberichts jederzeit stoppen und den Fehlerbericht löschen. Wenn Sie sich entscheiden, den Fehlerbericht mit dem RKI zu teilen, erhalten Sie über die App eine Kennung zu Ihrem Fehlerbericht (Fehlerbericht-ID). Mit der Fehlerbericht-

ID ermöglichen Sie dem RKI die Zuordnung Ihres Fehlerberichts zu weiteren Informationen, die Sie dem technischen Support gesondert mitteilen, z.B. wenn Sie noch eine Fehlerbeschreibung per E-Mail bereitstellen möchten. Wenn Sie dem technischen Support Ihre Fehlerbericht-ID mitteilen, kann anhand dieser weiteren Informationen möglicherweise eine Verbindung zu Ihrer Person hergestellt werden.

o. Echtheitsbestätigung des Betriebssystems

Einige Funktionen der App setzen voraus, dass vorab die Echtheit Ihrer App geprüft und gegenüber dem RKI bestätigt wird. Die Echtheitsprüfung des Betriebssystems dient insbesondere dazu, festzustellen, ob Sie eine manipulierte oder gefälschte („unechte“) Version der App verwenden. Ihr Smartphone erzeugt dabei eine eindeutige Kennung und sendet diese an den Hersteller Ihres Betriebssystems (wenn Sie ein Android-Smartphone verwenden, werden Daten an Google übermittelt; wenn Sie ein iPhone verwenden, werden Daten an Apple übermittelt). Die Kennung enthält Informationen über die Version Ihres Smartphones und die Version der App. Wenn diese Funktion des Betriebssystems verfügbar ist, kann der Hersteller Ihres Betriebssystems anhand der Kennung auf Ihre Identität schließen und nachvollziehen, dass die App die Echtheitsprüfung beantragt hat. Das RKI stellt dem Hersteller Ihres Betriebssystems keine Angaben aus der App, z.B. Begegnungsdaten, zur Verfügung.

6. Wofür werden Ihre Daten verarbeitet?

a. Risiko-Ermittlung

Die Risiko-Ermittlung ist eine Hauptfunktion der App. Sie dient dazu, Sie bei möglichen Begegnungen mit Corona-positiv getesteten Personen (Risiko-Begegnungen) länderübergreifend zu warnen, Ihr persönliches Infektionsrisiko zu bewerten und Ihnen Verhaltens- und Gesundheitshinweise zu geben.

Hierzu ruft die App vom Serversystem mehrmals täglich eine aktuelle Positiv-Liste mit den Angaben von Nutzern ab, die über eine offizielle Corona-App eine Warnung ausgelöst haben (siehe hierzu Punkt 7). Diese Positiv-Liste enthält die Zufalls-IDs der warnenden Nutzer sowie eventuelle Angaben zum Symptombeginn. Falls die warnenden Nutzer bei einem Event eingchecked waren oder der Gastgeber eines Events oder Ortes andere warnt, enthält die Positiv-Liste auch die betreffenden Event-IDs und die Dauer des Check-ins (Eincheck- und Auscheck-Zeit).

Die Zufalls-IDs und Event-IDs in den Positiv-Listen enthalten zusätzlich einen Übertragungsrisiko-Wert und eine Angabe zur Art der Diagnose (siehe hierzu Punkt 6 e.).

Die App gibt die Zufalls-IDs aus der Positiv-Liste an das COVID-19-Benachrichtigungssystem weiter, welches diese mit den aufgezeichneten Zufalls-IDs Ihrer Begegnungen abgleicht. Wenn das COVID-19-Benachrichtigungssystem dabei eine Übereinstimmung feststellt, übergibt es der App die zu der jeweiligen Risiko-Begegnung aufgezeichneten Begegnungsdaten.

Ebenso gleicht die App Event-IDs aus der Positiv-Liste mit den Event-IDs Ihrer Check-ins ab, um festzustellen, ob Sie sich zeitgleich mit Corona-positiv getesteten Nutzern bei einem Event oder Ort aufgehalten haben.

Diese Begegnungsdaten, Event-IDs (einschließlich der zugehörigen Eincheck- und Auscheck-Zeiten) und die Angaben in den Positiv-Listen (Übertragungsrisiko-Wert, Angaben zum Symptombeginn) werden von der App bewertet, um Ihr Infektionsrisiko zu ermitteln. Die Regeln für die Bewertung dieser Informationen (beispielsweise welchen Einfluss die Dauer eines Kontakts auf das Infektionsrisiko hat) basieren auf den aktuellen wissenschaftlichen Erkenntnissen des RKI. Bei neuen Erkenntnissen kann das RKI die Bewertungsregeln aktualisieren, indem die Bewertungs-Einstellungen der App angepasst werden. Die neuen Bewertungs-Einstellungen werden in diesem Fall zusammen mit den Positiv-Listen an die App übermittelt.

Das Infektionsrisiko wird ausschließlich offline in der App berechnet und weder an das COVID-19-Benachrichtigungssystem noch an sonstige Empfänger (auch nicht an das RKI, andere Gesundheitsbehörden in Deutschland oder anderen Ländern, Apple, Google und sonstige Dritte) weitergegeben.

Sollte für Sie ein Infektionsrisiko ermittelt werden, wird dies in der App angezeigt. Sollte ein erhöhtes Risiko angezeigt werden, bedeutet dies, dass Sie mit anderen Nutzern, die später Corona-positiv getestet wurden und eine Warnung ausgelöst haben, eine oder mehrere Begegnungen hatten oder dass Sie zeitgleich mit solchen Nutzern bei einem Event oder Ort eingchecked waren.

Das für die letzten 14 Tage jeweils berechnete Risiko wird Ihnen in der Kalenderansicht des Kontakt-Tagebuchs angezeigt. Bitte vermeiden Sie falsche Rückschlüsse auf die Quelle des Risikos: Ein für einen Tag berechnetes und angezeigtes Risiko kann auf eine unbemerkte Begegnung mit Ihnen unbekanntem Nutzern zurückgehen und muss nicht im Zusammenhang mit den von Ihnen im Kontakt-Tagebuch eingetragenen Personen, Orten oder Events stehen.

b. Testergebnis abrufen

Wenn Sie einen Corona-Test (PCR-Test oder Antigen-Schnelltest) gemacht und diesen Test mit dem QR-Code in der App registriert haben, können Sie Ihr Testergebnis über die App abrufen. Die App benachrichtigt Sie, sobald Ihr Testergebnis vorliegt. Dies setzt voraus, dass die Testeinrichtung (z.B. Testlabor oder Testzentrum) an das Serversystem angeschlossen ist und Sie im Rahmen der Testdurchführung gesondert Ihr Einverständnis zur Übermittlung Ihres Testergebnisses erteilt haben. Testergebnisse von Testeinrichtungen, die nicht an das Serversystem der App angeschlossen sind, können nicht angezeigt werden. Wenn Sie keinen QR-Code erhalten haben, können Sie diese Funktion ebenfalls nicht nutzen.

Scan des QR-Codes

Damit Sie das Testergebnis per App abrufen können, müssen Sie den QR-Code mit der App scannen. Der QR-Code enthält eine Kennzahl, die beim Scannen ausgelesen wird und Ihrem Test zugeordnet ist. Handelt es sich um einen Antigen-Schnelltest, sind zudem die unter Punkt 5 c. beschriebenen Schnelltestdaten im QR-Code enthalten. Die ausgelesene Kennzahl wird von der App gehasht. Das bedeutet, dass die Kennzahl nach einem bestimmten mathematischen Verfahren so verfremdet wird, dass sie nicht mehr erkennbar ist. Die eindeutige Zuordnung der gehashten Kennzahl zu Ihrem Testergebnis ist aber weiterhin möglich. Sobald Ihr Smartphone eine Verbindung zum Internet hat, wird die gehashte Kennzahl von der App an das Serversystem übermittelt. Das Serversystem stellt sodann einen digitalen Zugangsschlüssel (ein sogenanntes Token) zur Verfügung, der in der App gespeichert wird. Das Token ist auf dem Serversystem mit der gehashten Kennzahl verknüpft. Die App löscht nun die auf Ihrem Smartphone gehashte Kennzahl und behält nur das Token.

Der QR-Code ist damit verbraucht (ungültig), das heißt er kann von niemanden mehr verwendet werden. So ist sichergestellt, dass Ihr QR-Code von keinem anderen Nutzer für die Abfrage des Testergebnisses verwendet werden kann.

Hinterlegung des Testergebnisses

Sobald Ihr Testergebnis vorliegt, wird es von der Testeinrichtung nur unter Angabe der gehashten Kennzahl in der vom RKI betriebenen Testergebnis-Datenbank hinterlegt. Die Testergebnis-Datenbank befindet sich auf einem speziellen Server innerhalb des Serversystems. Die Testeinrichtung erzeugt die gehashte Kennzahl auf Basis des gleichen QR-Codes, den auch Sie erhalten haben.

Abruf des Testergebnisses

Die App fragt bei dem Serversystem unter Verwendung des in der App gespeicherten Tokens regelmäßig den Status Ihres Tests ab. Das Serversystem teilt der App dann den aktuellen Status (Ergebnis liegt noch nicht vor / Ergebnis liegt vor) mit. Sobald Ihr Testergebnis vorliegt, wird auch der Befund (Corona-positiv oder Corona-negativ) an die App übermittelt. Falls Sie die Mitteilungen zum Teststatus aktiviert haben (unter „Einstellungen“ > „Mitteilungen“), erhalten Sie eine Benachrichtigung. Das Testergebnis wird erst angezeigt, wenn Sie die App öffnen.

Wenn Sie Corona-positiv getestet wurden, fordert die App bei dem Serversystem unter erneuter Verwendung des Tokens eine TAN (Transaktionsnummer) an. Die TAN wird benötigt, um sicherzustellen, dass keine Falschwarnungen an andere Nutzer ausgegeben werden. Das Serversystem ordnet hierfür das Token wieder der gehashten Kennzahl zu und fordert von der Testergebnis-Datenbank eine Bestätigung an, dass zu der gehashten Kennzahl tatsächlich ein positives Testergebnis vorliegt. Sofern dies bestätigt wird, erzeugt das Serversystem die TAN und übermittelt sie an die App. Eine Kopie der TAN verbleibt auf dem Serversystem.

Die Testergebnisse werden auch in Ihrem Kontakt-Tagebuch hinterlegt.

c. Nachweis des Schnelltest-Ergebnisses

Wenn Sie das Ergebnis eines Antigen-Schnelltests abrufen und in der Testeinrichtung die Option zur namentlichen Anzeige für den Fall eines negativen Testergebnisses gewählt haben, wird ein negativer Befund unter Angabe Ihres Namens, Ihres Geburtsdatums und des Testzeitpunkts angezeigt. Die App verwendet hierzu die entsprechenden beim Scan des QR-Codes ausgelesenen Schnelltestdaten. Die Schnelltestdaten werden gelöscht, sobald das negative Schnelltest-Ergebnis nicht mehr in der App angezeigt wird.

Sie können das in der App angezeigte Testergebnis bei Bedarf vorzeigen, um die Durchführung eines negativen Schnelltests gegenüber Dritten nachzuweisen. Informieren Sie sich hierzu bitte, welche Anforderungen an Ihrem Aufenthaltsort im Einzelfall für die Anerkennung von digitalen Testnachweisen erfüllt werden müssen.

Bitte beachten Sie:

- Das RKI übernimmt keine Gewähr für die Anerkennung des angezeigten Schnelltest-Ergebnisses durch zuständige Behörden und andere berechnigte Stellen, die von Ihnen die Vorlage eines Testnachweises verlangen dürfen oder müssen (z. B. Geschäfte, Arbeitgeber).

- Sie sind nicht verpflichtet, die Nachweisfunktion der App zu verwenden. Falls Sie gegenüber Dritten Ihr Testergebnis nachweisen müssen, können Sie den Nachweis im Rahmen der gesetzlichen (auch Bundesland-spezifischen) Vorgaben auch in einer anderen Form vorlegen.

Bei Abruf eines positiven Schnelltest-Ergebnisses erfolgt keine namentliche Anzeige. In diesem Fall werden Ihr Name und Ihr Geburtsdatum sofort aus dem App-Speicher gelöscht. Ihre weiteren Schnelltestdaten (Kennzahl, Testzeitpunkt) werden gelöscht, sobald das positive Schnelltest-Ergebnis nicht mehr in der App angezeigt wird.

Die Schnelltest-Ergebnisse werden auch in Ihrem Kontakt-Tagebuch hinterlegt.

d. Schnelltest-Profil

Das Schnelltest-Profil bietet Ihnen die Möglichkeit, die Datenerfassung in teilnehmenden Teststellen zu beschleunigen. Sie können hierfür Angaben zu Ihrer Person in Ihrem Schnelltest-Profil in der App speichern und diese in Ihren persönlichen QR-Code umwandeln, der alle eingegebenen Daten enthält. In der Teststelle können Sie den QR-Code Ihres Schnelltest-Profiles in Ihrer App vorzeigen, damit dieser von der Teststelle gescannt und die von Ihnen angegebenen Daten auslesen werden können. Die für die Durchführung des Schnelltests erforderlichen Daten werden so schnell und sicher bereitgestellt. Sie entscheiden selbst, welche Daten Sie im Schnelltest-Profil angeben und ob Sie dieses in Teststellen vorzeigen. Angaben, die die Teststelle benötigt und die nicht im QR-Code enthalten sind, können Sie der Teststelle auch auf andere Weise mitteilen.

e. Andere warnen

Wenn Sie Corona-positiv getestet sind und Ihre Zufalls-IDs mit der App teilen, können andere Nutzer, denen Sie begegnet sind, gewarnt werden. Daneben werden Nutzer gewarnt, die zeitgleich mit Ihnen an denselben Events oder Orten eing_checked waren. In diesem Fall übermittelt die App folgende Daten an das Serversystem:

- Ihre eigenen Zufalls-IDs der letzten 14 Tage
- Event-IDs von Events oder Orten, bei denen Sie in den letzten 14 Tagen eing_checked waren, einschließlich der erfassten Eincheck- und Auscheck-Zeiten
- eventuelle Angaben zum Symptombeginn
- Ihre TAN (siehe Punkt 6 b.)

Vor der Weitergabe Ihres Testergebnisses (genauer gesagt: der Übermittlung Ihrer Zufalls-IDs und Event-IDs sowie der erfassten Eincheck- und Auscheck-Zeiten) an das Serversystem fügt die App den Daten einen Übertragungsrisiko-Wert und eine Angabe zur Art der durchgeführten Tests hinzu. Der Übertragungsrisiko-Wert ist ein Schätzwert zur Infektionswahrscheinlichkeit an den einzelnen Tagen des 14-Tage-Zeitraums. Da die Infektionswahrscheinlichkeit von der Dauer und dem Verlauf der Infektion abhängt, kann so beispielsweise berücksichtigt werden, dass am Tag einer Risiko-Begegnung die Gefahr einer Infektion in der Regel je geringer ist, desto mehr Zeit seit Symptombeginn verstrichen ist. Diese zusätzlichen Übertragungsrisiko-Werte ermöglichen eine genauere Bestimmung der Infektionswahrscheinlichkeit für andere Nutzer.

Die in der App abgefragten Angaben zum Symptombeginn sind optional. Diese Angaben können jedoch helfen, den Übertragungsrisiko-Wert noch genauer zu berechnen. Wenn Sie

keine Angaben machen, werden die Übertragungsrisiko-Werte unter Annahme eines typischen Infektionsverlaufs berechnet, das heißt je mehr Zeit seit Verwendung einer Zufalls-ID vergangen ist, desto kleiner ist der zugehörige Übertragungsrisiko-Wert.

Wenn Sie Ihr Testergebnis nicht in der App abgerufen haben:

Sie können Ihre Mitmenschen auch warnen, wenn Sie das positive Testergebnis nicht in der App abgerufen haben, z.B. weil Sie einen Selbsttest zuhause gemacht haben oder weil Sie von der Testeinrichtung keinen QR-Code erhalten haben.

Wählen Sie hierzu das Verfahren „Selbsttest positiv?“ bzw. „Test positiv und kein Ergebnis in der App?“.

Bitte beachten Sie, dass Ihre Warnung in seltenen Fällen dazu führen kann, dass Personen in Ihrem persönlichen Umfeld, die die App nutzen und gewarnt werden, unter Umständen darauf schließen können, dass Sie die Warnung abgegeben haben. Dies kann der Fall sein, wenn eine Person in Ihrem persönlichen Umfeld an dem Tag, an dem die Risiko-Begegnung angezeigt wird, außer mit Ihnen keine anderen Kontakte hatte.

f. Informatrische Nutzung der App

Die täglichen Statistiken, die in der App erscheinen, erhält die App automatisch über das Serversystem. Dabei fallen Zugriffsdaten an. In der App verlinkte Webseiten, z. B.: www.bundesregierung.de werden im Standard-Browser (Android-Smartphones) oder in der App (iPhones) geöffnet und angezeigt. Welche Daten dabei verarbeitet werden, wird von den jeweiligen Anbietern der aufgerufenen Webseite festgelegt.

g. Kontakt-Tagebuch

Das Kontakt-Tagebuch ist eine Zusatzfunktion der App. Ihre Einträge im Kontakt-Tagebuch dienen Ihnen als Gedächtnisstütze und sind nur Ihnen zugänglich. Falls Sie zu einem späteren Zeitpunkt Corona-positiv getestet werden sollten und das Gesundheitsamt Ihre Mithilfe bei der Kontaktnachverfolgung erbittet, können Sie dem Gesundheitsamt so schneller die für die Kontaktnachverfolgung benötigten Informationen mitteilen. Die Anzeige des für Sie berechneten Risikos an den einzelnen Tagen kann Ihnen helfen, Ihre Kontaktpersonen oder Personen, die Sie begleitet haben, frühzeitig zu warnen, wenn für Sie ein erhöhtes Risiko an einem bestimmten Tag festgestellt wurde. Dadurch können auch Ihre Kontaktpersonen ihr eigenes Kontaktverhalten ggf. anpassen und so weitere Infektionen in ihrem Umfeld durch eventuell noch unerkannte Infektionen verhindern.

h. Digitale COVID-Zertifikate

Die App erlaubt es Ihnen digitale COVID-Zertifikate zu speichern, in elektronischer Form bei sich zu führen und diese für Zertifikatsprüfungen bei Ticketbuchungen zu verwenden.

Ein digitales COVID-Zertifikat ist ein Nachweis dafür, dass eine Person

- eine Schutzimpfung gegen COVID-19 erhalten hat (COVID-Impfzertifikat),
- negativ auf COVID-19 getestet wurde (COVID-Testzertifikat) oder
- von einer COVID-19-Erkrankung genesen ist (COVID-Genesenzertifikat).

Die digitalen COVID-Zertifikate gelten seit dem 01.07.2021 innerhalb der Europäischen Union (EU) als Bescheinigung von COVID-19-Impfungen und -Tests sowie der Genesung von einer COVID-19-Infektion. Die offizielle Bezeichnung lautet „EU Digitales COVID-Zertifikat“ (COVID-Zertifikat).

Ein COVID-Zertifikat erhalten Sie auf Wunsch nach einer Impfung, einem Test oder nach einer durchgemachten COVID-19-Erkrankung von einer zuständigen Einrichtung (Impfzentren, Teststellen, Ärzte oder Apotheken). Ein COVID-Testzertifikat können Sie auch direkt in der App anfordern, wenn Sie einen Test registrieren. Scannen Sie hierfür den QR-Code, den Sie beim Test erhalten haben. Die App liest die Daten zu Ihrem Test aus dem QR-Code aus und erhält das Testergebnis vom Server. Wenn Sie einen PCR-Test gemacht haben, wird der Abruf des Ergebnisses und des COVID-Testzertifikats zusätzlich mit Ihrem Geburtsdatum gesichert. Aus dem Geburtsdatum wird ein Sicherheitscode erstellt (in Form eines sog. Hashwertes) und mit dem Server des RKI abgeglichen. Auf diese Weise wird sichergestellt, dass andere Personen nicht Ihr Testergebnis abrufen können. Das Testzertifikat wird nach dem Abruf des Testergebnisses in einem gesicherten Bereich Ihres Smartphones gespeichert. Wenn Sie ein positives Testergebnis abgerufen haben, wird kein COVID-Testzertifikat erstellt. Ihr aktuelles COVID-Testzertifikat wird auf dem Homescreen in der App und im Bereich „Zertifikate“ angezeigt und ist auch über das Testergebnis aufrufbar.

Sie können ein COVID-Zertifikat in Papierform verwenden oder in elektronischer Form auf Ihrem Smartphone bei sich führen. Jedes Zertifikat enthält einen QR-Code mit einer elektronischen Signatur des RKI zum Schutz vor Fälschungen. Wenn Sie ein COVID-Zertifikat auf Ihrem Smartphone speichern möchten, können Sie den QR-Code einfach mit der App einscannen. Die App speichert dann eine elektronische Version des COVID-Zertifikats sicher auf Ihrem Smartphone. Um einen ungewollten Zugriff auf die auf Ihrem Smartphone gespeicherten Zertifikate zu verhindern, sollten Sie auf dem Gerät eine Codesperre einrichten.

Bitte beachten Sie, dass die QR-Codes der COVID-Zertifikate Gesundheitsdaten (Daten über Corona-Impfungen, Corona-Testergebnisse oder durchgemachte Corona-Infektionen) enthalten. Zeigen Sie die Zertifikate und QR-Codes nur vor, wenn Sie einen entsprechenden Nachweis erbringen möchten. Stellen Sie die QR-Codes niemandem zur Verfügung, wenn Sie nicht wollen, dass die Daten ausgelesen werden.

Mit der App können Sie ausgedruckte eigene COVID-Zertifikate und COVID-Zertifikate von Familienmitgliedern (Familienzertifikate) scannen und verschlüsselt auf Ihrem Smartphone speichern. Zeigen Sie Familienzertifikate nur vor, wenn dies für die Wahrnehmung der Rechte Ihrer Familienmitglieder erforderlich ist, beispielsweise bei einem gemeinsamen Restaurantbesuch oder bei gemeinsamen Reisen.

Um in den gesetzlich vorgesehenen Fällen gegenüber Dritten eine Impfung, ein negatives Testergebnis oder eine durchgemachte COVID-19-Erkrankung nachzuweisen, können Sie das entsprechende COVID-Zertifikat der prüfenden Person vorzeigen. Wenn die prüfende Person eine spezielle Prüf-App (etwa die CovPassCheck-App des RKI) nutzt, genügt es den QR-Code des Zertifikats vorzuzeigen und scannen zu lassen.

Der QR-Code stellt das COVID-Zertifikat in digitaler Form dar und enthält ausschließlich die für die jeweilige Art des Zertifikats notwendigen Informationen (siehe unter Punkt 5 h.-j.).

Mit der Prüf-App kann der QR-Code beispielsweise von Behörden, Reiseunternehmen und anderen Dienstleistern in der EU gescannt werden, um die Gültigkeit eines vorgezeigten COVID-Zertifikats zu überprüfen. Bei der Prüfung werden die im Zertifikat enthaltenen Daten ausgelesen. In der Prüf-App wird nur angezeigt, ob das vorgelegte Zertifikat gültig ist. Im Falle

eines gültigen Zertifikats wird zusätzlich der Name und das Geburtsdatum des Zertifikatsinhabers mitgeteilt und ob es sich um ein Testzertifikat handelt oder nicht. Bei Testzertifikaten wird zudem der Zeitpunkt der Probenahme angezeigt.

Der Name und das Geburtsdatum des Zertifikatsinhabers werden angezeigt, damit die prüfende Person diese Angaben mit einem Identitätsnachweis (z. B. Reisepass oder Personalausweis) abgleichen kann. Die Mitteilung, ob es sich um ein Testzertifikat handelt und der Zeitpunkt der Probenahme sind erforderlich, damit die prüfende Person beurteilen kann, ob das dem Zertifikat zugrunde liegende Testergebnis noch gültig ist.

Zum Schutz vor Fälschungen muss die Echtheit der gespeicherten COVID-Zertifikate überprüft werden. Hierzu wird die im QR-Code eines Zertifikats enthaltene elektronische Signatur verwendet. Die elektronische Signatur wird bei der Erstellung des COVID-Zertifikats vom RKI auf Basis der im Zertifikat enthaltenen Daten (siehe unter Punkt 5 h.-j.) erzeugt. Bei der Signatur handelt es sich um eine besondere Form der Verschlüsselung, die wie eine elektronische Unterschrift des RKI funktioniert und sicherstellt, dass es sich um ein offiziell vom RKI erstelltes digitales Dokument handelt.

Das RKI stellt zudem die zugehörigen öffentlichen Schlüssel (sogenannte Public Keys) der zertifikats-ausstellenden Behörden (in Deutschland das RKI) bereit. Mit diesen öffentlichen Schlüsseln kann geprüft werden, ob die elektronische Signatur des Zertifikats tatsächlich von der ausstellenden Behörde stammt und ob das Zertifikat nach der elektronischen Signierung manipuliert worden ist.

Die App lädt regelmäßig im Hintergrund die öffentlichen Schlüssel herunter und speichert diese lokal auf Ihrem Smartphone. So kann die App die Gültigkeit der elektronischen Signatur und damit die Echtheit der gespeicherten Zertifikate überprüfen. Die öffentlichen Schlüssel enthalten keine personenbezogenen Daten.

Sie können mit der App die Gültigkeit der in der App hinterlegten COVID-Zertifikate prüfen. Die EU-Länder können eigene Regeln für die Gültigkeit der COVID-Zertifikate erlassen. Beispielsweise können Testzertifikate in einigen EU-Ländern längere Gültigkeit aufweisen als in anderen. Die EU-Länder tauschen diese Regeln über einen gemeinsamen Austausch-Server aus. Vor dem Antritt einer Reise können Sie daher mit der App die Gültigkeit der Zertifikate im Reiseland überprüfen.

Wenn Sie die Gültigkeit eines COVID-Zertifikats überprüfen möchten, lädt Ihre App die jeweils aktuellen Regeln aller Mitgliedstaaten vom Serversystem der App herunter. Die App überprüft dann anhand der in einem Zertifikat enthaltenen Daten, ob das Zertifikat den Regeln entspricht und zeigt Ihnen das entsprechende Ergebnis an. Die anschließende Überprüfung findet ausschließlich offline in der App statt und es werden dabei keine Daten an das RKI oder sonstige Empfänger (andere Gesundheitsbehörden in Deutschland oder anderen Ländern, Apple, Google und sonstige Dritte) weitergegeben.

Bitte beachten Sie, dass sich die Einreiseregeln ändern können und sowohl im Reiseland als auch bei der Rückkehr weitere Regeln gelten können. Hinweise auf die Einreisebestimmungen können Sie auch dieser Website der EU: <https://reopen.europa.eu/de>.

Zusätzlich kann die App Sie daran erinnern, gespeicherte Impfzertifikate zu überprüfen, sobald die letzte Impfung länger zurückliegt. Falls Sie die Mitteilungen in der App aktiviert haben (unter „Einstellungen“ > „Mitteilungen“), erhalten Sie in diesen Fällen eine Benachrichtigung. Die App lädt in regelmäßigen Abständen die aktuellen Regeln für die Empfehlungen der Auffrischungsimpfungen vom Serversystem herunter. Die App überprüft dann anhand der in

den Zertifikaten enthaltenen Daten, ob eine baldige Auffrischungsimpfung empfohlen ist. Auch diese Überprüfung findet ausschließlich offline in der App statt und es werden keine Daten über die Impfung an das RKI weitergegeben.

Sie haben die Möglichkeit ein in der App gespeichertes Zertifikat zu exportieren, um es auszudrucken und in der Papierversion zu verwenden (z.B. auf längeren Reisen) oder das Zertifikat anschließend mit einem neuen Smartphone zu scannen und erneut in der elektronischen Version in der App zu speichern (z.B. nach einem Gerätewechsel). Die Funktion „EU-Ausdruck“ verwendet die in der App gespeicherten Daten des jeweiligen Zertifikats, um eine PDF-Datei zu erstellen. Diese Verarbeitung erfolgt ausschließlich offline auf dem Smartphone. Sie haben anschließend die Möglichkeit, diese PDF-Datei zu speichern. Die Erstellung des EU-Ausdrucks ist freiwillig. Das PDF-Dokument enthält sensible Gesundheitsdaten (Daten über Corona-Impfungen, Tests oder durchgemachte Corona-Erkrankungen). Bitte bewahren Sie das gespeicherte oder ausgedruckte Zertifikat daher sicher auf und veröffentlichen oder teilen Sie das Dokument nicht.

i. Widerruf von digitalen COVID-Zertifikaten

Zum Gesundheitsschutz von Zertifikatsinhabern und der Bevölkerung kann es notwendig werden, dass bestimmte digitale COVID-Zertifikate widerrufen werden. Das ist beispielsweise der Fall, wenn Zertifikate von einer Einrichtung (z. B. Apotheke) irrtümlich oder in betrügerischer Absicht ausgestellt worden sind. Der Widerruf führt dazu, dass das Zertifikat ungültig wird und bei Überprüfungen nicht mehr anerkannt wird. Dabei spielt es keine Rolle, ob das Zertifikat bei der Überprüfung in elektronischer Form auf dem Smartphone oder im Papierformat verwendet wird.

Wenn Sie ein widerrufenes COVID-Zertifikat in der App gespeichert haben, wird es als „ungültig“ angezeigt. Falls Sie die Mitteilungen in der App aktiviert haben (unter „Einstellungen“ > „Mitteilungen“), erhalten Sie im Fall eines Widerrufs eine Benachrichtigung.

Um festzustellen, ob ein in der App gespeichertes COVID-Zertifikat widerrufen worden ist, lädt die App in regelmäßigen Abständen eine Widerrufsliste vom Serversystem. Die Widerrufsliste enthält keine personenbezogenen Daten, sondern lediglich einen kleinen Teilabschnitt aus der eindeutigen Kennung der widerrufenen Zertifikate. Dieser Teilabschnitt ist bei allen COVID-Zertifikaten, die von der gleichen Einrichtung ausgegeben worden sind, identisch. Die App gleicht dann diesen Teilabschnitt mit der eindeutigen Kennung der auf dem Smartphone gespeicherten Zertifikate ab. Sofern es eine Übereinstimmung gibt, wird das betreffende Zertifikat in der App als ungültig angezeigt. Das widerrufene digitale COVID-Zertifikat selbst wird dabei jedoch nicht verändert. Der Abgleich findet ausschließlich offline in der App statt und es werden keine Daten über diesen Vorgang an das RKI weitergegeben.

j. Datenspende

Die Datenspende ist eine freiwillige Zusatzfunktion der App. Die im Rahmen der Datenspende an das RKI übermittelten Nutzungsdaten und weiteren freiwilligen Angaben dienen der Bewertung der Wirksamkeit der App und sie werden ausgewertet, um folgende Verbesserungen zu ermöglichen:

- Verbesserung der Risiko-Ermittlung – Die Genauigkeit und Zuverlässigkeit der technischen Berechnung der Infektionsrisiken sollen verbessert werden. Hierfür werden Angaben über Risiko-Begegnungen und Ihnen angezeigte Warnungen ausgewertet. In der Folge kann die Berechnungsmethode verfeinert werden.

- Verbesserung der Nutzerführung in der App – Die Bedienung der App soll erleichtert werden. Hierfür werden Angaben über die einzelnen Schritte ausgewertet, die Nutzer in der App vornehmen. So können Beschriftungen und Hinweistexte klarer gestaltet und Bedienelemente so platziert werden, dass sie besser gefunden werden können. Außerdem können Darstellungen für verschiedene Smartphone-Modelle angepasst werden.
- Informationen und Hilfestellungen zur App ermöglichen – Es soll möglich werden, zu erkennen, ob es z.B. bei der Nutzung der App im Zusammenhang mit bestimmten Testeinrichtungen und Laboren oder in bestimmten Regionen zu Problemen kommt. Dies kann festgestellt werden, wenn aufgrund der Datenspende auffällt, dass in bestimmten Regionen Testergebnisse verspätet zur Verfügung stehen. So können die zuständigen Gesundheitsbehörden auch gezielt auf mögliche technische Störungen hingewiesen werden.
- Verbesserung der Statistiken über den Pandemieverlauf – Die Daten können Aufschluss über die zeitliche und räumliche Verteilung bestimmter Ereignisse des Pandemieverlaufs geben und es ermöglichen, auf bestimmte Entwicklungen schneller zu reagieren.

Die Nutzungsdaten und die weiteren freiwilligen Angaben werden ohne jeden Zusammenhang mit Ihrem Namen oder Ihrer Identität gespeichert und ausgewertet. Das RKI erfährt also nicht, wer Sie sind oder wen Sie getroffen haben. Die Aktivierung der Datenspende setzt die Bestätigung der Echtheit Ihrer App voraus (Beachten Sie bitte die weiteren Informationen hierzu unter Punkt 5 n. und Punkt 11).

k. Zertifikatsprüfung bei Ticketbuchungen

Wenn Sie bei einem Reise- oder Veranstaltungsunternehmen oder einem sonstigen Anbieter eine Ticketbuchung vornehmen, können Sie über die App ein digitales COVID-Zertifikat an den Prüfpartner des Anbieters übermitteln, damit dieser die Gültigkeit des Zertifikats für Ihre Buchung gegenüber dem Reise- oder Veranstaltungsunternehmen bestätigt.

Voraussetzung hierfür ist, dass Sie in der App ein digitales COVID-Zertifikat hinzugefügt haben. Die App erfragt beim jeweiligen Anbieter die zur Prüfung zu verwendenden Buchungsdaten und schlägt auf Basis dieser Angaben ein geeignetes Zertifikat vor. Dieses können Sie sodann auswählen und zusammen mit den vom Anbieter bereitgestellten Buchungsdaten (siehe Punkt 5.k.) dem Prüfpartner übermitteln.

Der Prüfpartner überprüft, ob die elektronische Signatur des Zertifikats echt und das technische Ablaufdatum des Zertifikats noch nicht erreicht ist. Der Prüfpartner teilt dem Anbieter sofort das Prüfungsergebnis mit. Es wird nur mitgeteilt, ob die Prüfung erfolgreich war oder nicht. Das Prüfungsergebnis wird Ihnen auch in der App angezeigt.

Die vom Anbieter bereitgestellten Buchungsdaten werden nur lokal in der App verarbeitet. Das RKI kann daher nicht nachvollziehen, welche Zertifikate Sie ausgewählt und prüfen lassen haben oder welche Reisen oder Veranstaltungen Sie gebucht haben.

Für die Datenverarbeitung durch den Anbieter und den Prüfpartner ist das RKI nicht verantwortlich. Lesen Sie bitte deren Datenschutzhinweise, damit Sie wissen, wozu und wie Ihre Daten verwendet werden.

I. Fehlerberichte

Das RKI ist bemüht, eine fehlerfreie App anzubieten. Aufgrund der großen Anzahl verschiedener Systeme kann dies jedoch nicht immer gewährleistet werden. Um den technischen Support der App bei der Fehleranalyse zu unterstützen, können Sie einen in Ihrer App erstellten Fehlerbericht an das RKI übermitteln. Das RKI wird den Fehlerbericht auswerten, um die Ursache der in Ihrer App auftretenden Fehler erkennen und beseitigen zu können.

Die Fehlerberichte werden ohne jeden Zusammenhang mit Ihrem Namen oder Ihrer Identität vorübergehend gespeichert und im Rahmen der Fehleranalyse ausgewertet. Das RKI erfährt also nicht, wer Sie sind oder wen Sie getroffen haben. Beachten Sie bitte, dass sich Hinweise auf Ihre Identität ergeben können, wenn Sie dem technischen Support Ihre Fehlerbericht-ID unter Offenlegung Ihrer Identität (z. B. per E-Mail) mitteilen.

Die Erstellung und Übersendung eines Fehlerberichts an das RKI ist freiwillig. Sie entscheiden selbst darüber, ob Sie einen Fehlerbericht aufzeichnen möchten und diesen an den technischen Support der App übersenden. Die Übersendung des Fehlerberichts setzt die Bestätigung der Echtheit Ihrer App voraus (Beachten Sie bitte die weiteren Informationen hierzu unter Punkt 5 n. und Punkt 11).

m. Befragungen

Die Teilnahme an Befragungen ist freiwillig. Sie entscheiden selbst darüber, ob Sie an einer Befragung teilnehmen möchten und Daten hierfür an das RKI übermittelt werden sollen. Befragungen finden auf einer Webseite außerhalb der App statt, auf die Sie weitergeleitet werden. Welche Zwecke mit einer Befragung durch das RKI verfolgt werden, ist in den Informationen zur Befragung auf der Befragungs-Webseite beschrieben. Die Teilnahme an einer Befragung setzt die Bestätigung der Echtheit Ihrer App voraus (Beachten Sie bitte die weiteren Informationen hierzu unter Punkt 5 n. und Punkt 11).

n. Bestätigung der Echtheit Ihrer App

Zur Bestätigung der Echtheit Ihrer App wird eine Funktion des Betriebssystems Ihres Smartphones genutzt. Damit kann sichergestellt werden, dass nur Nutzer der App an der Datenspende oder an Befragungen teilnehmen, deren App ordnungsgemäß funktioniert. Auf diese Weise wird sichergestellt, dass die Statistiken und Befragungsergebnisse nicht verfälscht werden. Die Echtheitsprüfung wird außerdem im Rahmen der Übersendung von Fehlerberichten verwendet, um sicherzustellen, dass nur Aufzeichnungen einer echten App übersandt werden können und ein Missbrauch der Funktion verhindert wird. Außerdem wird die Echtheitsprüfung auch bei einer Warnung mit einem positiven Testergebnis genutzt, das nicht in der App abgerufen wurde. Hierbei wird unter Verwendung der Bestätigung sichergestellt, dass eine solche Warnung nur einmalig in einem Zeitraum von drei Monaten erfolgen kann. Dies dient dem Schutz der technischen Infrastruktur und anderen Nutzern der App vor einer Überflutung mit gefälschten Warnungen.

Bitte beachten Sie, dass der Hersteller Ihres Betriebssystems nachvollziehen kann, dass die Echtheitsprüfung Ihres Smartphones stattgefunden hat und dadurch auf Ihre Identität oder den Zusammenhang der Prüfung schließen kann (z.B. Warnung anderer Nutzer).

Die Nutzung der Funktion zur Bestätigung der Echtheit ist in jedem Zusammenhang freiwillig. Wenn Sie mit der Bestätigung der Echtheit Ihrer App und der hierbei möglicherweise

erfolgenden Datenübermittlung Ihres Betriebssystems in Länder außerhalb der EU nicht einverstanden sind, sind die Teilnahme an der Datenspende oder Befragungen sowie die Übersendung von Fehlerberichten nicht möglich. Sie können andere Nutzer aber auch ohne die Bestätigung der Echtheit warnen, wenn Sie einen offiziellen Test in einer Testeinrichtung durchführen lassen und diesen anhand des QR-Codes in der App registrieren.

o. Aktualisierungsfunktion für COVID-Zertifikate

Es kann vorkommen, dass die App Ihnen die Aktualisierung eines gültigen digitalen COVID-Zertifikats anbietet. Beschließen die EU-Mitgliedstaaten beispielsweise eine Änderung des Inhalts oder der Datenstruktur der Daten im COVID-Zertifikat, kann es für die reibungslose weitere Zertifikatsnutzung erforderlich sein, die jeweilige inhaltliche oder technische Änderung auf ein vorhandenes digitales COVID-Zertifikat anzuwenden.

Dazu lädt die App im Hintergrund die aktuellen inhaltlichen und technischen Spezifikationen für die digitalen COVID-Zertifikate vom Serversystem der App herunter. Die App überprüft dann anhand der in den von Ihnen gespeicherten digitalen COVID-Zertifikaten enthaltenen Daten, ob eine Aktualisierung eines gespeicherten digitalen COVID-Zertifikats über die App möglich ist. Sie werden dann auf eine mögliche Aktualisierung hingewiesen. Für die Aktualisierung wird mit Ihrem Einverständnis das zu aktualisierende digitale COVID-Zertifikat von der App verschlüsselt an das Serversystem der App übermittelt. Wenn es sich bei dem zu aktualisierenden digitalen COVID-Zertifikat um ein COVID-Impfzertifikat zum Nachweis einer Auffrischungsimpfung (Booster-Impfung) handelt, werden dabei auch die digitalen COVID-Zertifikate zum Nachweis der der Auffrischungsimpfung vorausgegangenen Grundimmunisierung bzw. Genesung an das Serversystem der App übermittelt. Dort wird dann die Gültigkeit der übermittelten digitalen COVID-Zertifikate geprüft (siehe Abschnitt 6.h.). Anhand der Daten aus den übermittelten digitalen COVID-Zertifikaten wird eine neue Version des COVID-Impfzertifikats für die Auffrischungsimpfung generiert. Bei der Aktualisierung werden die Daten in den übermittelten COVID-Zertifikaten (siehe Abschnitte 5.h und 5.i) kurzzeitig verarbeitet. Das aktualisierte COVID-Zertifikat wird sodann an Ihre App zurückübermittelt.

Um eine missbräuchliche mehrfache Verwendung der Aktualisierungsfunktion verhindern zu können, werden die elektronischen Signaturen des aktualisierten und des neuen digitalen COVID-Zertifikats in Form spezieller Einwegverschlüsselungen (sog. Hash-Werte) vorübergehend gespeichert. Das bedeutet, dass die elektronische Signatur nach einem bestimmten mathematischen Verfahren so verfremdet wird, dass sie nicht mehr erkennbar ist. Aus dem Hash-Wert kann nicht auf die Daten im betreffenden digitalen COVID-Zertifikat oder andere Angaben zu Ihrer Person geschlossen werden. Die eindeutige Zuordnung des Hash-Werts zu dem aktualisierten digitalen COVID-Zertifikat ist aber weiterhin möglich. 365 Tage nach der Aktualisierung werden die Hash-Werte wieder gelöscht.

7. Wie funktioniert das länderübergreifende Warnsystem?

Damit auch Nutzer von den offiziellen Corona-Apps anderer Länder gewarnt werden, hat das RKI zusammen mit mehreren in anderen Ländern für Gesundheitsaufgaben zuständigen amtlichen Stellen und Behörden (im Folgenden: **Gesundheitsbehörden**) zentrale Warnserver

zum länderübergreifenden Austausch von Warnungen (im Folgenden: **Austausch-Server**) eingerichtet.

- Der Austausch-Server der teilnehmenden Länder unter den europäischen Mitgliedstaaten nutzt die digitale Infrastruktur des zwischen den Mitgliedsstaaten und der EU eingerichteten Netzwerks für elektronische Gesundheitsdienste.
- Damit auch Warnungen zwischen Nutzern der Schweizer Corona-App und der Corona-Warn-App möglich sind, betreibt das RKI zudem gemeinsam mit der Schweiz (Bundesamt für Gesundheit der Schweizerischen Eidgenossenschaft) einen weiteren Austausch-Server.

Die nationalen Serversysteme der an den Austausch-Servern angebotenen Corona-Apps übermitteln ihre eigenen Positiv-Listen regelmäßig an die Austausch-Server und erhalten die Positiv-Listen der anderen Länder. Länderübergreifende Warnungen können nur aufgrund eines positiven PCR-Tests und nur aufgrund von im COVID-19-Benachrichtigungssystem erfassten Begegnungen ausgelöst werden. Event-IDs und Zufalls-IDs aufgrund von positiven Antigen-Schnelltests oder Testergebnissen, die nicht über die App abgerufen wurden, werden daher nicht an die Austausch-Server übermittelt.

Das jeweilige Serversystem führt die erhaltenen Positiv-Listen mit der eigenen Positiv-Liste zusammen, so dass die Risiko-Ermittlung auch Risiko-Begegnungen mit Nutzern einer anderen Corona-App berücksichtigen kann (siehe Punkt 6 e.). Die anderen teilnehmenden Länder verfahren entsprechend mit den vom RKI bereitgestellten Positiv-Listen.

An den Austausch-Servern können nur Länder teilnehmen, deren Corona-Apps zueinander kompatibel sind und die ein vergleichbar hohes Datenschutzniveau gewährleisten. Dies setzt insbesondere voraus, dass die Corona-Apps der teilnehmenden Länder ebenfalls das COVID-19-Benachrichtigungssystem nutzen, von der jeweiligen nationalen Gesundheitsbehörde zugelassen sind und die Privatsphäre ihrer Nutzer wahren.

- Die technischen und organisatorischen Einzelheiten der Zusammenarbeit betreffend den innerhalb der EU betriebenen Austausch-Server werden in einem Beschluss der EU-Kommission festgelegt (Durchführungsbeschluss (EU) 2020/1023 vom 15. Juli 2020, abrufbar unter https://eur-lex.europa.eu/eli/dec_impl/2020/1023/oj). Für die Verarbeitung der in den Positiv-Listen enthaltenen Angaben (Zufalls-IDs und eventuelle Angaben zum Symptombeginn) auf den Austausch-Servern zur Ermöglichung der länderübergreifenden Risiko-Ermittlung und Warnung ist das RKI danach mit den jeweils zuständigen Gesundheitsbehörden der teilnehmenden Länder gemeinsam verantwortlich.
- Der Betrieb und der Datenaustausch des gemeinsam mit der Schweiz betriebenen Austausch-Servers ist in einer individuellen Vereinbarung des RKI mit der Schweiz geregelt, abrufbar unter https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html. Danach erfolgt der technische Betrieb des Austausch-Servers durch das Bundesamt für Gesundheit der Schweizerischen Eidgenossenschaft. Für die Speicherung, Bereitstellung und spätere Löschung der Positiv-Listen ist das RKI gemeinsam mit dem Bundesamt für Gesundheit der Schweizerischen Eidgenossenschaft verantwortlich.

Bitte beachten Sie, dass sich die Liste der teilnehmenden Länder ändern kann. Die aktuelle Liste mit Angaben zu den jeweils verantwortlichen Gesundheitsbehörden finden Sie in den FAQ: abrufbar unter https://www.coronawarn.app/de/faq/#interoperability_countries.

8. Welche Berechtigungen benötigt die App?

Die App benötigt Zugriff auf verschiedene Funktionen und Schnittstellen Ihres Smartphones. Dazu ist es erforderlich, dass Sie der App bestimmte Berechtigungen erteilen. Das Berechtigungssystem richtet sich nach den Vorgaben Ihres Betriebssystems. So können auf Ihrem Smartphone beispielsweise Einzelberechtigungen zu Berechtigungskategorien zusammengefasst sein, wobei Sie der Berechtigungskategorie nur insgesamt zustimmen können. Bitte beachten Sie, dass ohne die von der App angeforderten Berechtigungen keine oder nur wenige App-Funktionen genutzt werden können.

a. Technische Voraussetzungen (alle Smartphones)

- Die App benötigt eine Internetverbindung, um mit dem Serversystem Daten austauschen zu können. Insbesondere können so durch die App von dem Serversystem des RKI aktuelle Informationen heruntergeladen werden (z.B. das aktuelle Schlüsselmaterial, Widerrufslisten).
- Die Bluetooth-Funktion muss aktiviert sein, damit Ihr Smartphone eigene Zufalls-IDs aussenden und die Zufalls-IDs von anderen Smartphones aufzeichnen kann.
- Die App muss auf Ihrem Smartphone im Hintergrundbetrieb laufen können, um Ihr Infektionsrisiko automatisch zu ermitteln und den Status Ihres Tests abfragen zu können. Wenn Sie den Hintergrundbetrieb deaktivieren, müssen Sie alle Aktionen in der App selbst starten.

b. Android-Smartphones

Wenn Sie ein Android-Smartphone verwenden, müssen außerdem folgende Systemfunktionen aktiviert sein:

- Das COVID-19-Benachrichtigungssystem von Android (COVID-19-Benachrichtigungen)
- Die Standortermittlung muss unter Android bis Version 10 aktiviert sein, damit Ihr Smartphone nach Bluetooth-Signalen anderer Smartphones sucht. Standortdaten werden dabei jedoch nicht erhoben.
- Um über Änderungen Ihres Infektionsrisikos und den Status von Testergebnissen benachrichtigt werden zu können, muss die Benachrichtigungsfunktion aktiviert sein. Die Benachrichtigungsfunktion ist im Betriebssystem standardmäßig aktiviert.

Daneben benötigt die App folgende Berechtigungen:

- Die Funktionen „Testergebnis abrufen“, „Event-Check-in“ und „Zertifikate hinzufügen“ benötigen Zugriff auf die Kamera, um QR-Codes scannen zu können. Um ein Foto eines QR-Codes in der App öffnen zu können, ist ein Zugriff auf die auf dem Smartphone gespeicherten Fotos, Medien und Dateien erforderlich.

c. iPhones (Apple iOS)

Wenn Sie ein iPhone verwenden, müssen folgende Systemfunktionen aktiviert sein:

- Das COVID-19-Benachrichtigungssystem von iOS (Begegnungsmitteilungen)
- Um über Änderungen Ihres Infektionsrisikos und den Test-Status benachrichtigt werden zu können, müssen Mitteilungen aktiviert sein.

Die App benötigt zudem folgende Berechtigungen:

- Die Funktionen „Testergebnis abrufen“, „Event-Check-in“ und „Zertifikate hinzufügen“ benötigen Zugriff auf die Kamera, um QR-Codes scannen zu können. Um ein Foto eines QR-Codes in der App öffnen zu können, ist ein Zugriff auf die auf dem Smartphone gespeicherten Fotos erforderlich.

9. Wann werden Ihre Daten gelöscht?

Die Speicherdauer richtet sich danach, für welche Zwecke bzw. App-Funktionen Ihre Daten jeweils gespeichert worden sind. Bei der Festlegung der Speicherdauer berücksichtigt das RKI die aktuellen wissenschaftlichen Erkenntnisse zur Inkubationszeit (Dauer von der Infektion bis zum Ausbruch der Krankheit), die bis zu 14 Tage beträgt und zur Dauer des Infektionsrisikos für Mitmenschen einer infizierten Person nach dem Ende der Inkubationszeit. Soweit unter Punkt 6 keine kürzere Speicherdauer genannt wird, gelten folgende Fristen:

a. Daten auf Ihrem Smartphone

Die Positiv-Listen werden nach 14 Tagen aus dem App-Speicher gelöscht. Event-Daten im Bereich „Meine Check-ins“ werden nach 14 Tagen automatisch gelöscht. Alternativ können Sie Einträge im Bereich „Meine Check-ins“ jederzeit händisch löschen. Das für Sie ermittelte Infektionsrisiko (z. B. „niedriges Risiko“) wird nach jeder Aktualisierung, spätestens aber nach 14 Tagen aus dem App-Speicher gelöscht. Sofern Sie ein positives Testergebnis abgerufen haben, wird das Token im App-Speicher gelöscht, sobald Sie eine Warnung auslösen oder den Test aus der App entfernen. Die Einträge im Kontakt-Tagebuch bleiben für 16 Tage auf Ihrem Smartphone gespeichert und werden dann automatisch gelöscht. Sie können diese Einträge jederzeit auch vorzeitig selbst löschen. Bitte beachten Sie, dass beim Einchecken zu einem Event oder an einem Ort übernommene Einträge im Kontakt-Tagebuch auch nach der Löschung des zugehörigen Check-ins dort noch gespeichert sind. Wenn Sie Ihr Schnelltest-Profil einmal angelegt haben, bleibt dieses so lange in der App gespeichert, bis Sie es selbst wieder löschen. Wenn Sie COVID-Impf-, Test- oder Genesenzertifikate einschließlich Familienzertifikate gescannt haben, bleiben auch diese so lange in der App gespeichert, bis Sie sie selbst wieder löschen. Bitte löschen Sie Familienzertifikate, wenn Sie diese nicht mehr für die vorgesehenen Zwecke benötigen. Die Buchungsdaten werden nach Beendigung der Zertifikatsprüfung gelöscht.

b. Daten auf Serversystemen

Im Falle der Aktualisierung eines digitalen COVID-Zertifikats (siehe Abschnitt 6.0. werden die für die Aktualisierung an das Serversystem der App übermittelten digitalen COVID-Zertifikate nach Abschluss des Aktualisierungsvorgangs wieder gelöscht. Die Hash-Werte der elektronischen Signaturen des aktualisierten und des neuen digitalen COVID-Zertifikats werden nach 365 Tagen gelöscht.

Positiv-Listen werden nach 14 Tagen von allen Serversystemen (einschließlich dem Austausch-Server) gelöscht. Alle anderen Daten, mit Ausnahme der im Rahmen der Datenspende sowie zur Bestätigung der Echtheit Ihrer App übermittelten Daten, werden spätestens nach 21 Tagen gelöscht.

c. Datenspende

Nutzungsdaten und weitere freiwillige Angaben, die im Rahmen der Datenspende an das RKI übermittelt werden, werden nach 180 Tagen gelöscht.

d. Fehlerberichte

Sie können einen aufgezeichneten Fehlerbericht auf Ihrem Smartphone jederzeit löschen. Fehlerberichte, die Sie an den technischen Support übersandt haben, werden spätestens nach 14 Tagen gelöscht.

e. Echtheitsbestätigung des Betriebssystems

Die Kennungen, die Ihr Smartphone zur Bestätigung der Echtheit Ihrer App erzeugt, werden nach 30 Tagen nach Übermittlung an das RKI vom Serversystemen gelöscht.

10. An wen werden Ihre Daten weitergegeben?

Wenn Sie andere Nutzer aufgrund eines positiven PCR-Tests über die App warnen, werden Ihr Testergebnis (in Form Ihrer Zufalls-IDs der letzten 14 Tage) sowie optionale Angaben zum Symptombeginn an die jeweils verantwortlichen Gesundheitsbehörden der an den Austausch-Servern teilnehmenden Länder und von dort an die Serversysteme der an den länderübergreifenden Warnungen teilnehmenden Corona-Apps weitergegeben. Die Serversysteme der nationalen Corona-Apps verteilen diese Informationen dann als Bestandteil der Positiv-Listen an ihre jeweiligen eigenen Nutzer. Event-IDs werden nur über das Serversystem des RKI an Nutzer der Corona-Warn-App verteilt. Im Fall einer Warnung aufgrund eines positiven Antigen-Schnelltests erfolgt keine Weitergabe Ihrer Daten an die Austausch-Server.

Mit dem Betrieb und der Wartung des gemeinsam betriebenen Austausch-Servers der teilnehmenden EU-Länder haben die jeweils zuständigen nationalen Gesundheitsbehörden die EU-Kommission als Auftragsverarbeiter beauftragt. Der Austausch-Server für länderübergreifende Warnungen zwischen der Corona-Warn-App und der schweizerischen Corona-App wird vom Bundesamt für Gesundheit der Schweizerischen Eidgenossenschaft in Abstimmung mit dem RKI betrieben und gewartet. Mit dem Betrieb und der Wartung eines Teils der technischen Infrastruktur der App (z. B. Serversysteme, Hotline) hat das RKI die T-Systems International GmbH und die SAP Deutschland SE & Co. KG beauftragt, die als Auftragsverarbeiter des RKI tätig werden. Diese Unternehmen sind von der EU-Kommission zudem als Unterauftragsverarbeiter mit der technischen Bereitstellung und Verwaltung des gemeinsam betriebenen Warnsystems der teilnehmenden Länder beauftragt. Im Übrigen gibt das RKI Ihre Daten, die im Zusammenhang mit der Nutzung der App erhoben werden, nur an Dritte weiter, soweit das RKI rechtlich dazu verpflichtet ist oder die Weitergabe im Falle von Angriffen auf die technische Infrastruktur der App zur Rechts- oder Strafverfolgung erforderlich ist. Eine Weitergabe durch das RKI in anderen Fällen erfolgt grundsätzlich nicht.

Wenn Sie anderen Personen oder Einrichtungen in den gesetzlich vorgesehenen Situationen (beispielsweise europäische Grenzbehörden oder Dienstleister) ein COVID-Zertifikat vorzeigen, erlangen diese Kenntnis über alle im Zertifikat enthaltenen Daten.

Dies können Sie verhindern, indem Sie nur den QR-Code des COVID-Zertifikats in der App vorzeigen, sodass dieser mit einer Prüf-App gescannt werden kann (z. B. als Nachweis der Schutzimpfung im Rahmen einer Ausnahme von Schutzmaßnahmen gegen das Coronavirus).

Dann werden nur die im QR-Code enthaltenen Daten ausgelesen. In der Prüf-App wird dabei nur angezeigt, ob das vorgezeigte Zertifikat gültig ist sowie eine Erläuterung des Ergebnisses. Im Falle eines gültigen Zertifikats werden zusätzlich der Name und das Geburtsdatum des Zertifikatsinhabers in der Prüf-App angezeigt, damit die prüfende Person diese Angaben mit einem Identitätsnachweis (z. B. Reisepass oder Personalausweis) abgleichen kann. Zusätzlich wird angezeigt, ob es sich um ein Testzertifikat handelt oder nicht. Bei Testzertifikaten wird dann auch der Zeitpunkt der Probenahme angezeigt, damit die prüfende Person beurteilen kann, ob das zugrunde liegende Testergebnis noch gültig ist.

Bei der Zertifikatsprüfung für Ticketbuchungen werden Ihre COVID-Zertifikate und die Buchungsdaten an einen Prüfpartner des Anbieters übermittelt. Der konkrete Prüfpartner wird Ihnen vor der Übermittlung in der App angezeigt. Zum Abruf der individuellen Buchungsdaten übermittelt die App dem Anbieter die im Buchungs-QR-Code des Anbieters enthaltene Buchungskennung.

11. Werden Ihre Daten in Länder außerhalb der EU übermittelt?

Wenn Sie eine Warnung aufgrund eines positiven PCR-Tests auslösen, werden Ihre Zufalls-IDs auch in die Schweiz zu dem vom RKI gemeinsam mit dem Bundesamt für Gesundheit der Schweizerischen Eidgenossenschaft betriebenen Austausch-Server übermittelt. Im Fall einer Warnung aufgrund eines positiven Antigen-Schnelltests oder Testergebnissen, die nicht über die App abgerufen wurden, erfolgt eine solche Übermittlung Ihrer Daten nicht. Für die Schweiz hat die EU einen Angemessenheitsbeschluss erlassen, in dem die Angemessenheit des Datenschutzniveaus festgestellt wird (Art. 45 DSGVO).

Daneben können die aktuellen Positiv-Listen unabhängig vom Aufenthaltsort des Nutzers (etwa im Urlaub oder auf Geschäftsreise) abgerufen werden.

Zudem kann es im Rahmen der Bestätigung der Echtheit Ihrer App zu einer Übermittlung von Daten in ein Land außerhalb der EU kommen. Die von Ihrem Smartphone erzeugte Kennung, die Informationen über die Version Ihres Smartphones und der App enthält, wird an den Hersteller des Betriebssystems Ihres Smartphones (Apple oder Google) übermittelt. Dabei kann es auch zu einer Datenübermittlung in Drittländer, insbesondere in die USA, kommen. Dort besteht möglicherweise kein dem europäischen Recht entsprechendes Datenschutzniveau und Ihre europäischen Datenschutzrechte können eventuell nicht durchgesetzt werden. Insbesondere besteht die Möglichkeit, dass Sicherheitsbehörden im Drittland auf die übermittelten Daten beim Hersteller des Betriebssystems zugreifen und diese auswerten, beispielsweise indem sie Daten mit anderen Informationen aus anderen Quellen verknüpfen.

Im Übrigen werden die von der App übermittelten Daten ausschließlich auf Servern in Deutschland oder in einem anderen Land in der EU (oder dem Europäischen Wirtschaftsraum) verarbeitet, die somit den strengen Anforderungen der Datenschutz-Grundverordnung (DSGVO) unterliegen.

12. Wie können Sie Ihr Einverständnis zurücknehmen?

Ihnen steht das Recht zu, ein in der App erteiltes Einverständnis gegenüber dem RKI jederzeit mit Wirkung für die Zukunft zurückzunehmen. Sofern die jeweilige Verarbeitung Ihrer Daten bereits durchgeführt worden ist, kann die Verarbeitung jedoch nicht mehr rückgängig gemacht werden. Insbesondere hat das RKI keine Möglichkeit, Ihre bereits an andere Nutzer übermittelten Zufalls-IDs von deren Smartphones zu löschen.

a. Einverständnis „Risiko-Ermittlung“

Ihr Einverständnis in die Risiko-Ermittlung können Sie jederzeit zurücknehmen, indem Sie diese Funktion in den Einstellungen der App deaktivieren oder die App löschen. Wenn Sie die Risiko-Ermittlung wieder nutzen möchten, können Sie die Funktion erneut aktivieren oder die App erneut installieren.

b. Einverständnis „Testergebnis abrufen“

Ihr Einverständnis zum Abruf des Testergebnisses durch die App können Sie zurücknehmen, indem Sie den Test in der App anzeigen und anschließend entfernen. Das Token zum Abruf des Testergebnisses wird dadurch aus dem App-Speicher gelöscht, sodass das Token auf dem Serversystem nicht mehr zugeordnet werden kann. Eine erneute Zuordnung des gleichen Tests zu Ihrer App bzw. der erneute Scan desselben QR-Codes ist nicht möglich. Wenn Sie erneut getestet wurden und das Testergebnis abrufen möchten, werden Sie erneut um Ihr Einverständnis gebeten. Liegt das Testergebnis bereits in der App vor, kann das Einverständnis nicht mehr zurückgenommen werden.

c. Einverständnis „Andere warnen“

Ihr Einverständnis zur Übermittlung Ihres Testergebnisses (genauer gesagt: Ihrer Zufalls-IDs und Event-IDs sowie der erfassten Eincheck- und Auscheck-Zeiten der letzten 14 Tage) zur Warnung Ihrer Mitmenschen können Sie zurücknehmen, indem Sie den Test anzeigen und anschließend „Andere warnen“ deaktivieren. Sie können unter „Meine Check-ins“ auch Einträge zu Events oder Orten löschen, und so verhindern, dass Daten zu diesen Events im Rahmen der Warnung verwendet werden. Diese Möglichkeit besteht, solange Sie Ihre Zufalls-IDs und Event-IDs noch nicht zur Warnung anderer Nutzer übermittelt haben.

Nachdem Sie Ihre Zufalls-IDs übermittelt haben, können Sie Ihr Einverständnis insoweit nur zurücknehmen, indem Sie die App löschen. Ihre bereits an das Serversystem übermittelten Zufalls-IDs werden dadurch aus dem App-Speicher gelöscht und können dann nicht mehr Ihrer Person oder Ihrem Smartphone zugeordnet werden. Wenn Sie erneut eine Warnung auslösen möchten, müssen Sie die App erneut installieren und Ihr Einverständnis erneut abgeben. Ein Testergebnis, das Ihrer App bereits zugeordnet und zur Warnung anderer übermittelt wurde, kann nicht erneut verwendet werden, um andere zu warnen.

Um bereits an das Serversystem übermittelte Event-IDs aus dem App-Speicher zu löschen, können Sie unter „Meine Check-ins“ auch Einträge zu Events oder Orten löschen. Event-IDs können dann nicht mehr Ihrer Person oder Ihrem Smartphone zugeordnet werden.

Das RKI hat keine Möglichkeit, um Ihre bereits übermittelten Zufalls-IDs, Event-IDs und Übertragungsrisiko-Werte aus den vom Serversystem verteilten Positiv-Listen und von Smartphones der Nutzer zu löschen. Um auch Ihre im COVID-19-Benachrichtigungssystem Ihres Smartphones gespeicherten Begegnungsdaten zu löschen, können Sie in den Systemeinstellungen Ihres Smartphones möglicherweise eine manuelle Löschung vornehmen. Beachten Sie hierzu auch die Hinweise unter Punkt 5 b.

d. Einverständnis „Event-Check-in“

Sie können unter „Meine Check-ins“ Einträge zu Events oder Orten jederzeit löschen. So verhindern Sie, dass Daten zu diesen Events verwendet werden und Event-IDs Ihrer Person oder Ihrem Smartphone zugeordnet werden können, wenn Sie andere warnen.

e. Einverständnis „Datenspende“

Sie können Ihr Einverständnis in die Datenspende jederzeit zurücknehmen, indem Sie „Daten spenden“ in den Einstellungen der App deaktivieren. Die App wird dann Ihre Nutzungsdaten und weiteren freiwilligen Angaben nicht weiter täglich an das RKI übermitteln. Wenn Sie die Datenspende wieder erlauben möchten, können Sie die Funktion in den Einstellungen erneut aktivieren.

f. Einverständnis „Fehlerberichte“

Ihr Einverständnis zur Analyse von bereits an das RKI übermittelten Fehlerberichten können Sie zurücknehmen, indem Sie dem technischen Support unter Nennung Ihrer Fehlerbericht-ID mitteilen, dass Sie die Analyse des Fehlerberichts nicht mehr wünschen. Ihr Fehlerbericht wird dann gelöscht. Bitte beachten Sie, dass das RKI dabei Ihre Identität erfahren kann. Wenn Sie dem technischen Support Ihre Fehlerbericht-ID nicht mitteilen, wird der übermittelte Fehlerbericht automatisch nach 14 Tagen gelöscht.

g. Einverständnis „Befragung“

Ihr Einverständnis zur Teilnahme an einer Befragung des RKI erteilen Sie nicht in der App, sondern über die Website, auf der auch die Befragung durchgeführt wird. Dort ist auch beschrieben, wie Sie Ihr Einverständnis zurücknehmen können.

h. Einverständnis „Bestätigung der Echtheit Ihrer App“

Wenn Sie Ihr Einverständnis zur Bestätigung der Echtheit Ihrer App zurücknehmen, hat dies keine direkte Auswirkung auf die damit zusammenhängende Datenverarbeitung. Die Übermittlung der von Ihrem Smartphone erzeugten Kennung an den Hersteller des Betriebssystems Ihres Smartphones und die Überprüfung und Bestätigung der Echtheit Ihrer App findet unmittelbar statt, nachdem Sie Ihr Einverständnis erteilt haben.

i. Einverständnis „Aktualisierungsfunktion für COVID-Zertifikate“

Da die Aktualisierung eines digitalen COVID-Zertifikats nach der Erteilung Ihres Einverständnisses sofort durchgeführt wird, kann das Einverständnis nicht mehr zurückgenommen werden. Wenn die Aktualisierung nicht erfolgreich war oder Sie ein weiteres digitales COVID-Zertifikat aktualisieren möchten, müssen Sie für jeden einzelnen Aktualisierungsvorgang ein gesondertes Einverständnis erteilen.

13. Welche weiteren Datenschutzrechte haben Sie?

Soweit das RKI personenbezogene Daten von Ihnen verarbeitet, stehen Ihnen außerdem folgende Datenschutzrechte zu:

- die Rechte aus den Artikeln 15, 16, 17, 18, 20 und 21 DSGVO,
- das Recht, die behördliche Datenschutzbeauftragte des RKI zu kontaktieren und Ihr Anliegen vorzubringen (Art. 38 Abs. 4 DSGVO) und
- das Recht, sich bei einer Aufsichtsbehörde für den Datenschutz zu beschweren. Dazu können Sie sich entweder an die zuständige Aufsichtsbehörde an Ihrem Wohnort oder an die für des RKI zuständige Behörde wenden. Die zuständige Aufsichtsbehörde für

das RKI ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Graurheindorfer Str. 153, 53117 Bonn.

Diese Datenschutzrechte stehen Ihnen entsprechend auch gegenüber den für die Datenverarbeitung verantwortlichen Gesundheitsbehörden der an den Austausch-Servern teilnehmenden Länder zu, sofern Sie Ihre Zufalls-IDs der letzten Tage zur Warnung Ihrer Mitmenschen übermittelt haben (siehe Punkt 7).

Bitte beachten Sie, dass die vorgenannten Datenschutzrechte nur erfüllt werden können, wenn die Daten, auf die sich die geltend gemachten Ansprüche beziehen, eindeutig Ihrer Person zugeordnet werden können. Dies wäre nur möglich, wenn über die App weitere personenbezogene Daten erhoben würden, die eine eindeutige Zuordnung der an das Serversystem übermittelten Daten zu Ihrer Person oder Ihrem Smartphone ermöglichen. Da dies für die Zwecke der App grundsätzlich nicht erforderlich ist, ist das RKI zu einer solchen zusätzlichen Datenerhebung nicht verpflichtet (Art. 11 Abs. 2 DSGVO). Zudem würde dies dem erklärten Ziel zuwiderlaufen, so wenige Daten wie möglich zu erheben. Deshalb werden die vorgenannten Datenschutzrechte auch mit zusätzlich von Ihnen bereitgestellten Informationen zu Ihrer Identität in der Regel nicht erfüllt werden können.

Wenn anlässlich der Aktualisierung eines digitalen COVID-Zertifikats die Hash-Werte der elektronischen Signaturen vorübergehend gespeichert werden, ermöglichen es diese dem RKI nicht, die Identität von Zertifikatsinhabern zu ermitteln (siehe Abschnitt 6.o.).

14. Datenschutzbeauftragte und Kontakt

Fragen und Anliegen zum Datenschutz können Sie an die behördliche Datenschutzbeauftragte des RKI senden: Robert Koch-Institut, z. H. der Datenschutzbeauftragten, Nordufer 20, 13353 Berlin oder per E-Mail an: datenschutz@rki.de.