Last amended: 16 August 2021, version 2.7 (earlier versions available at: https://www.coronawarn.app/en/privacy)

Privacy notice

This privacy notice explains how your data is processed and what data protection rights you have when using the German Federal Government's official coronavirus app, the Corona-Warn-App.

It covers the following topics:

To make sure that this text can be understood by all users, we have made every effort to make it simple and as non-technical as possible.

1. Who is the Corona-Warn-App published by?

This app is published by the Robert Koch Institute (**RKI**) for the German Federal Government. The RKI is also responsible for ensuring that your personal data is processed in accordance with data protection regulations.

If, after testing positive for coronavirus, you use the app's transnational warning feature, it is also possible to warn users of official coronavirus apps of other countries whom you have encountered. In this case, the RKI and the competent health authorities of the countries participating in the respective transnational warning systems are so-called joint controllers, meaning they are jointly responsible for data processing. Please refer to Section 7 for more details.

2. Is using the app voluntary?

Using the app is voluntary. It is entirely up to you whether you install the app, which of the app's features you use, and whether you share data with others. As a matter of principle, all

of the app's main features that require the transfer of your personal data to the RKI or to other users will obtain your express consent in advance.

In the context of the official digital COVID certificates (COVID test certificate, COVID vaccination certificate and COVID recovery certificate), new legal requirements apply to the creation of the certificates. For this reason, no additional consent is required in this context. However, the certificates will only be created if you wish for this to happen. Requesting and using digital COVID certificates is voluntary.

If you do not give your consent, if you subsequently withdraw it, or if you do not request any digital COVID certificates, this will not result in any disadvantages for you.

3. On what legal basis is your data processed?

As a matter of principle, the RKI will only process your data for the purposes of exposure logging and warning others if you have given your express consent beforehand. The legal basis is Art. 6(1) Sentence 1(a) GDPR and, in the case of health data, Art. 9(2)(a) GDPR. After giving your consent, you can withdraw it at any time (so-called right of withdrawal). Please refer to Section 12 for further information about your right of withdrawal.

In the context of the official digital COVID certificates (COVID test certificate, COVID vaccination certificate and COVID recovery certificate), data processing is regulated by law. The creation and confirmation of vaccination certificates is based on Art. 9(2)(g) GDPR in conjunction with Sect. 22(5) of the Infection Protection Act (IfSG). The creation and confirmation of test certificates is based on Art. 9(2)(g) GDPR in conjunction with Sect. 22(7) IfSG. The creation and confirmation of recovery certificates is based on Art. 9(2)(g) GDPR in conjunction with Sect. 22(6) IfSG. The processing of access data for the purpose of checking whether certificates are valid and authentic is based on Art. 6(1) Sentence 1(e) GDPR in conjunction with Sect. 3 of the German Federal Data Protection Act (BDSG).

On the basis of Art. 6(1) Sentence 1(e) GDPR in conjunction with Sect. 3 BDSG, the processing of access data for the provision of daily statistics (see Section 6 f.) is performed as part of the RKI's duty to inform the public pursuant to Sect. 4(4) of the Act on Successor Agencies to the Federal Health Agency (BGA-NachfG).

4. Who is the app aimed at?

The app is aimed at people who are resident in Germany and at least 16 years old.

5. What data is processed?

The app's entire system has been programmed to process as little personal data as possible. This means that, when you use exposure logging, warn other users, or retrieve a test result, the system does not need to collect any data that would allow the RKI or other users to infer your identity, your name, your location or other personal details.

Exceptions apply to the feature for proving a rapid test result, which allows you to display a confirmation issued in your name for negative rapid test results (see Section 6 c.), the feature for creating a rapid test profile, which allows you to provide a testing point with the data required to perform a rapid test (see Section 6 d.) and if you add digital COVID certificates in the app.

The app refrains by default from using analysis tools to evaluate the way you use it. Only if you expressly agree to voluntarily share data or to record an error report and share it with the RKI (see Sections 5 k. and 5 m.), will certain data about your use of the app be transmitted to the RKI.

The data processed by the app can be grouped into the following categories:

a. Access data

Every time the app exchanges data over the internet with the RKI's server system (hereinafter referred to as the **server system**), the server system processes so-called access data. This is necessary so that the app can retrieve current data (e.g. for warnings) or transmit certain data stored on your smartphone to the server system. This access data includes the following:

- IP address
- Date and time of retrieval
- Transmitted data volume (or packet length)
- Notification of whether the data exchange was a success.

This access data is processed to maintain and secure the technical operation of the app and the server system. You will not be identified personally as a user of the app and no user profile will be created. Your IP address will not be stored beyond the end of the usage procedure.

In order to prevent unauthorised parties from using your IP address to associate your data with you when you use the app, the app only ever accesses the server system via a special access server. This access server then forwards the data requested or transmitted by the app to the appropriate server, but without your IP address, meaning that your IP address is no longer processed within the server system.

b. Exposure data

As soon as you enable your iPhone's or your Android smartphone's COVID-19 exposure notification system (which is called "Exposure Notifications" or "COVID-19 Exposure Notifications" respectively), your smartphone transmits so-called exposure data via Bluetooth, which other smartphones in your vicinity can record. Your smartphone, in turn, also receives the exposure data of other smartphones. The exposure data transmitted by your smartphone comprises:

- Random identification numbers (hereinafter referred to as **random IDs**)
- Bluetooth protocol version
- Bluetooth transmit power in decibel-milliwatts (dBm).

If exposure to another smartphone is recorded, the exposure data also includes:

- Day, time and duration of the contact
- Bluetooth signal strength in dBm.

The random IDs are changed regularly. This helps prevent your smartphone from being identified using these random IDs. The exposure data transmitted by your smartphone and the exposure data recorded when you come into contact with other app users are stored on your smartphone and deleted after 14 days. The exposure data transmitted by your smartphone is processed in the same way when it is recorded by the smartphones of other app users.

Please note: the COVID-19 exposure notification system functionality is part of your operating system. The providers responsible for this system are therefore Apple (if you have an iPhone) and Google (if you have an Android smartphone). In this respect, the data processing is subject to these companies' own privacy policies, which means that the RKI is not responsible for this and has no influence on it. Depending on the version and configuration of your operating system, the actual names, operating steps and settings options may differ from those described in this privacy notice. More information is available from the respective providers:

- If you have an Android smartphone, you can find information from Google on your device by going to "Settings" > "Google" > "COVID-19 exposure notifications" and tapping on "Learn more".
- If you have an iPhone, you can find information from Apple on your device by going to "Settings" > "Exposure Notifications" and tapping on "How Exposure Notifications work ...".

c. Rapid test data

If you have taken rapid antigen tests at a testing point, you can retrieve the results of these through the app. If you choose to use this service, your testing point will generate an individual QR code for you to scan with the app. The QR code contains a unique code for your rapid test, and the time you were tested, in encoded form. If, in the event of a negative rapid test result, you wish to have the test result displayed along with your name in the app for verification purposes (see Section 6 c. for more information about this feature), the QR code will contain further data provided by you in encoded form.

d. Rapid test profile

You can store information about yourself in your rapid test profile in the app. The rapid test profile includes the following fields: first name, last name, date of birth, street and house number, postcode, town, phone number, email address. The app then converts your data into your personal QR code, which contains all the data you have entered. Creating a rapid test profile in the app, and using it at a testing point, are voluntary. You decide yourself which data you enter in your rapid test profile. The QR code only contains this data. If the testing point requires more information that is not contained in the QR code, you can also provide this to the testing point in another way.

e. Event data

If you visit an event (such as a party or concert) or a place (such as a shop or restaurant), you can record your stay there in the app. Event organisers and business owners can provide guests with a QR code for this purpose.

As a guest, you can "check in" when you arrive by simply scanning this QR code with the app. When leaving the event or place, you can "check out" again in the app. The app then remembers that you were at that event or place, and when you were there. If a guest later tests positive for coronavirus and activates the warning feature via their app, then all other guests who were checked in at the same time will receive a warning.

If you scan a QR code as a guest, the event details provided by the host (name of the event/place, address/location, typical length of stay and, if applicable, the time when the event started) as well as the check-in time will be stored on your smartphone. In addition, your app

will derive an encrypted identifier (hereinafter referred to as the **event ID**) that can be uniquely assigned to the event based on the information contained in the QR code. No conclusions about the event or the place can be drawn from the event ID. When you check out in the app or are automatically checked out after the time preset by the host, the check-out time will be stored on your smartphone.

An entry will also be created in your contact journal by default. Sections 5 g. and **Error! Reference source not found.**. explain this in more detail. If you do not want to create an entry in your contact journal for an event or place, you can simply switch off this feature using the corresponding toggle switch.

Under “My check-ins”, you can check and delete your previous check-ins and also adjust the check-out time.

If you as a host create a QR code for your guests, the event details you provide and a random code will be stored in the QR code. The random code ensures that different places and events for which the same event details have been entered will later have different event IDs. The QR codes you create are stored on your smartphone. Under “My QR codes”, you can delete the QR codes you have created at any time.

Using the event check-in feature is voluntary. You decide yourself whether you want to create a QR code for your event or place, and whether to check in at an event or place.

f. Health data

Health data is any data containing information about a person’s health. This includes not only information about past and current illnesses, but also about a person’s risk of illness (such as the risk that a person has been infected with coronavirus). The app processes health data in the following cases:

- When a possible exposure is identified
- If you use the app to retrieve a test result
- If you use the app to warn other users and guests from events or places you visited at the same time that they may be infected
- If you provide information about the onset of any coronavirus symptoms or
- If you add digital COVID certificates (vaccination certificates, test certificates or recovery certificates) in the app.

Section 6 explains this in more detail.

g. Entries in the contact journal

If you use the contact journal to note when and where you met certain people and record certain details of the encounter or contact details for people and places, this information is stored in encrypted form on your smartphone. The contact journal entries are only there to help you remember. The RKI and other agencies cannot gain access to entries in the contact journal. The contact journal can help you to keep track of your personal contacts over the last 14 days. If you test positive for coronavirus and the public health office (*Gesundheitsamt*) requests your assistance with contact tracing, then you can quickly provide the information it needs.

Using the contact journal is voluntary. You personally decide whether to store entries in the contact journal. In this respect, you are also responsible for what you record. For this reason,

we kindly ask you to respect the privacy of the people you include in your contact journal. You should not share your entries with third parties or via insecure communication channels. The competent public health office will tell you what information it needs from you for contact tracing purposes, and how you can provide it.

h. Data about your COVID vaccination (data in the COVID vaccination certificate)

In the app, it is possible to add your official vaccination certificates (digital COVID certificates) that you received when you were vaccinated. Requesting a digital vaccination certificate is voluntary. If you choose to use this service, you will receive a printout with a QR code at the time of your vaccination. This will contain the following data about your COVID vaccination in encoded form:

- Personal data (last name, first name, date of birth)
- Information about the vaccine (disease, vaccine, product, manufacturer)
- Vaccination information (dose number, total doses, date of vaccination, country, issuer)
- The RKI's electronic signature
- Unique vaccination certificate identifier.

The data will be stored in the app as soon as you scan the QR code for the digital vaccination certificate. This data will have been collected previously at the time of your vaccination.

i. Data about your recovery (data in the COVID recovery certificate)

In the app, it is possible to add your official recovery certificates (digital COVID recovery certificates) that you received from a doctor. Requesting a digital recovery certificate is voluntary. After requesting the recovery certificate, you will receive a printout with a QR code from the doctor. This will contain the following data about your recovery in encoded form:

- Personal data (last name, first name, date of birth)
- Date of testing
- Information about the test, including the type of test, and the issuer
- The RKI's electronic signature
- Unique recovery certificate identifier.

The data will be stored in the app as soon as you scan the QR code of the digital recovery certificate. This data will have been collected from you by the doctor when you requested the certificate.

j. Data in the COVID test certificate

You request official test certificates (digital COVID test certificates) through the app. Requesting a digital test certificate is voluntary and only possible if a negative test result is available. You will then receive your test certificate with a QR code in the app. This contains the following data about your test result:

- Personal data (last name, first name, date of birth)
- Information about the test (disease, type of test, product, manufacturer)
- Information about the testing procedure (date and time of the test, location of the testing centre)
- Test result
- The RKI's digital signature

- Unique test certificate identifier.

The data is stored in the app as soon as your test result is available.

k. Usage data (data sharing)

If you enable data sharing, the app will transmit certain data about your use of the app (hereinafter referred to as **usage data**) once a day to the RKI. This usage data concerns the possible exposures displayed by the app, warnings that have been received and triggered, test results that have been retrieved, and technical information about your smartphone's operating system.

Specifically, the usage data includes:

- The date when you shared the data (i.e. the date of transmission)
- Changes to the warning history compared to the previous day
- What risk status was shown to you at the time when you used the data sharing feature
- Information about which encounters served as a basis on which to calculate the risk status
- Information about the model and version of your smartphone and the version of your app as well as the operating system you are using.

If you retrieved a test result via the app:

- Whether the test result was positive or negative
- What risk was shown to you at the time when you registered the test
- How much time has passed since the last possible exposure and its display in the app until the relevant test registration
- Whether you have used the feature for warning others and, if so, which step you reached in the process (e.g. the part that asks about your symptoms).

If you have used the warning feature:

- Whether you provided information about the onset of symptoms
- When you gave your consent to warn others (before or after registering the test)
- Whether you completed the entire warning process or whether you aborted the process before the end (for example, because you did not wait for confirmation that your data had been successfully transmitted)
- How many hours it took before you received your test result after registering your test
- How many days passed since the last notification of an elevated risk before the warning feature was used
- How many hours have passed since the test was registered.

In addition, you can provide further optional information about your region and age group, which will be transmitted to the RKI together with the usage data.

The RKI will compile the usage data and any optional information into anonymised statistics and analyse it to assess the effectiveness and functioning of the app, and draw conclusions regarding the pandemic.

Participation in data sharing is voluntary. To enable the data sharing feature, the authenticity of your app first needs to be confirmed (please note the further information about this under Sections 5 n. and 11).

l. Participation in a survey

Some app users are offered to participate in a survey by the RKI. This offer to participate in the survey will usually be contingent on certain events registered in the app (e.g. an elevated risk being displayed). By taking part in the survey, you will help the RKI to assess the effectiveness of the app, to improve the app and, for example, to understand whether and how warnings sent via the app help to prevent further infections.

Participation in the surveys is voluntary. You decide yourself whether you want to participate in a survey and whether data should be transmitted to the RKI for this purpose. The surveys take place on a website outside of the app, which you will be redirected to. To enable participation in a survey, the authenticity of your app first needs to be confirmed (please note the further information about this in Sections 5 n. and 11).

m. Contents of the error reports

To assist the app's technical support team with error analysis, you can record an error report in the app. When you start recording the error report, a comprehensive record is made of

- the steps you take in the app,
- the technical steps and processes as well as status messages involving
    - exposure logging (e.g. involving the functioning of the processing of exposure data, the calculation of the risk of infection, the updating of the positive lists, the display of the calculated risk status),
    - the retrieval and display of test results, and
    - possible processes for warning others (e.g. the calculation of transmission risk values and the technical provision of your random IDs by your smartphone)

and stored on your smartphone. The error report may also contain health data, because the technical steps and processes related to the detection of a possible exposure are also recorded.

However, the error report does not contain information about QR codes for test registration, the token stored in your app (see "Retrieving a test result" in Section 6 b. below), rapid test results, digital COVID certificates and entries in your contact journal. Furthermore, the error report does not contain your name or other information with which the RKI can identify you.

You can stop recording the error report and delete the error report at any time. If you choose to share the error report with the RKI, you will receive an identifier for your error report (error report ID) via the app. The error report ID allows the RKI to assign your error report to further information that you provide separately to the technical support team, e.g. if you also wish to provide a description of the error by email. If you provide your error report ID to the technical support team, it may be possible to establish a link to you based on this further information.

Creating and sending an error report to the RKI is voluntary. You decide yourself whether you want to record an error report and send it to the app's technical support team. To send the error report, the authenticity of your app first needs to be confirmed (please note the further information about this in Sections 5 n. and 11).

n. Confirmation of the authenticity of your app

Before you can use some of the app's features, the authenticity of your app first needs to be checked and confirmed to the RKI. Specifically, this authentication serves to determine whether you are using a manipulated or counterfeit ("fake") version of the app. The authentication uses a feature of your operating system. Your smartphone generates a unique identifier and sends it to your operating system provider (if you use an Android smartphone, data is transmitted to Google; if you use an iPhone, data is transmitted to Apple). The identifier contains information about the version of your smartphone and the version of the app. It is possible for your operating system provider to infer your identity from the identifier and learn that your smartphone has been authenticated. Your operating system provider does not receive any other information, such as exposure data, from the app. Your operating system provider will use the identifier to confirm the authenticity of your app to the RKI. Using the feature for confirming the authenticity of your app is voluntary. However, if you do not agree to having the authenticity of your app confirmed, other features of the app may not be available to you.

6. Why is your data processed?

a. Exposure logging

Exposure logging is part of the app's main functionality. It serves to warn you of possible exposure to people who have tested positive for coronavirus ("possible exposures") in a number of different countries, to assess the risk that you have been infected as a result of the exposure, and to provide you with health advice and recommendations for what to do next.

For this purpose, the app retrieves an up-to-date positive list from the server system several times a day. This list contains information from users who have used the warning feature in an official coronavirus app (see Section 7). This positive list contains the random IDs of users who have activated the warning feature and, if applicable, information about the onset of symptoms. If the users who have activated the warning feature were checked in at events, the positive list also contains the relevant event IDs and the duration of the check-ins (check-in and check-out times).

The random IDs and event IDs on the positive lists also contain a transmission risk value and an indication of the type of diagnosis (see Section 6 e.).

The app passes the random IDs from the positive list to the COVID-19 exposure notification system, which compares them with the random IDs it has recorded from your encounters with other users. If the COVID-19 exposure notification system detects a match, it transfers to the app the exposure data recorded for the possible exposure in question.

Similarly, the app matches event IDs from the positive list with the event IDs from your check-ins to determine whether you were at an event or place at the same time as users who have tested positive for coronavirus.

The app evaluates this exposure data, event IDs (including the associated check-in and check-out times) as well as the information on the positive lists (transmission risk value; information about the onset of symptoms) in order to determine your risk of infection. The rules for evaluating this information (for example, how the duration of a contact influences the risk of infection) are based on the RKI's latest scientific findings. In the event of new findings, the RKI can update the evaluation rules by adjusting the evaluation settings in the app. In this case, the new evaluation settings are sent to the app together with the positive lists.

The risk of infection is calculated exclusively offline in the app and is not passed on to the COVID-19 exposure notification system or any other recipient (including the RKI, other health authorities in Germany or other countries, Apple, Google and other third parties).

If a risk of infection is identified for you, this will be displayed in the app. If an elevated risk is displayed, this means that you encountered one or more other users who later tested positive for coronavirus and used the warning feature in their app, or that such users were checked in at an event or place at the same time as you.

The risk calculated for each of the last 14 days is displayed in the calendar view of the contact journal. Please refrain from drawing false conclusions about the source of any risk: a risk calculated and displayed for a certain day may well be due to your having encountered users unknown to you without realising it, and will not necessarily have anything to do with the people, places or events you recorded in the contact journal.

b. Retrieving a test result

If you have taken a coronavirus test (PCR test or rapid antigen test), you can retrieve your test result via the app. The app will notify you as soon as your test result is available. For this to work, the testing facility (e.g. testing laboratory or testing point) needs to be connected to the server system and, as part of the testing procedure, you must have given separate consent to your test result being sent. It is not possible to display test results from testing facilities that are not connected to the app's server system. If you have not received a QR code, then you cannot use this feature either.

<u>Scanning the QR code</u>

In order to retrieve your test result via the app, you will need to scan the QR code using your smartphone's camera. The QR code contains a code number that is read during scanning and is assigned to your test. If the test is a rapid antigen test, then the QR code will also contain the rapid test data described in Section 5 c. After reading the code number, the app 'hashes' it. This means that the app performs a certain mathematical procedure in order to convert the code number in such a way that it can no longer be identified. However, it is still possible to clearly assign the hashed code number to your test result. As soon as your smartphone is connected to the internet, the app will transmit the hashed code number to the server system. The server system then provides a digital access key (a so-called token), which is stored in the app. The token is linked to the hashed code number in the server system. The app now deletes the code number that has been hashed on your smartphone and keeps only the token. Once the QR code has been used in this way, it becomes invalid and can no longer be used by anyone. This ensures that no other users can use your QR code to retrieve your test result.

Filing of the test result

As soon as your test result is available, the testing facility stores it in the RKI's test result database using only the hashed code number. The test result database is located on a special server within the server system. The testing facility generates the hashed code number based on the same QR code that you received.

Retrieval of the test result

Using the token stored in the app, the app regularly requests the status of your test from the server system. The server system then informs the app of the current status (result not yet available / result available). As soon as your test result is available, the outcome (i.e. whether you have tested positive or negative for coronavirus) is also transmitted to the app. If you have enabled the test status notification (under "Settings" > "Notifications"), you will be notified. The test result will not be displayed until you open the app.

If you have tested positive for coronavirus, the app uses the token again to request a TAN (transaction number) from the server system. The TAN is required to ensure that no false warnings are transmitted to other users. For this purpose, the server system reassigns the token to the hashed code number and requests confirmation from the test result database that a positive test result really does exist for the hashed code number. If this is confirmed, the server system generates the TAN and transmits it to the app. A copy of the TAN remains on the server system.

The test results are also stored in your contact journal. You can delete them there at any time.

c. Proof of a rapid test result

If you retrieve the result of a rapid antigen test and, when you were at the testing facility, you selected the option to have your name displayed in the event of a negative test result, then a negative result will be displayed along with your name, date of birth and the time you were tested. To do this, the app uses the corresponding rapid test data which it reads when scanning the QR code. The rapid test data will be deleted as soon as the negative rapid test result is no longer displayed in the app.

If necessary, you can show the test result displayed in the app to prove to third parties that you took a rapid test and the result of that test was negative. Please find out about applicable requirements for the recognition of digital test certificates where you are located.

Please note:

- The RKI cannot guarantee that a rapid test result displayed in the app will be recognised by the competent authorities and other authorised bodies that may or must require you to provide proof of testing (e.g. shops, employers).

- You are not obliged to use the app's certification feature. If you have to prove your test result to third parties, you can also present the proof in another form subject to the legal requirements (which may vary depending on the federal state).

Your name will not be displayed if you retrieve a positive rapid test result. In this case, your name and date of birth will be immediately deleted from the app memory. Your other rapid test data (code, time you were tested) will be deleted as soon as the positive rapid test result is no longer displayed in the app.

The rapid test results are also stored in your contact journal. You can delete them there at any time.

d. Rapid test profile

The rapid test profile feature offers you the possibility to speed up data collection at participating testing points. To do this, you can store information about yourself in your rapid test profile in the app and convert it into your personal QR code, which contains all the data you have entered. At the testing point, you can present your rapid test profile's QR code in your app so that it can be scanned by testing point staff, allowing the data you have provided to be read. This is a quick and secure way for you to provide the data required to perform a rapid test. You decide yourself which data you include in your rapid test profile and whether to present it at testing points. If the testing point requires information that is not contained in the QR code, you can provide the information to the testing point in another way.

e. Warning others

If you have tested positive for coronavirus and share your random IDs with the app, then it is possible to warn other users whom you have encountered. In addition, users who were checked in at the same events or places at the same time as you will be warned. In this case, the app transmits the following data to the server system:

- Your own random IDs from the last 14 days
- The event IDs of events or places where you have checked in during the last 14 days, including the recorded check-in and check-out times
- Any information about the onset of symptoms
- Your TAN (see Section 6 b.).

Before passing on your test result (more precisely: before transmitting your random IDs and event IDs, including the recorded check-in and check-out times) to the server system, the app adds a transmission risk value to the data and also specifies the type of test performed. The transmission risk value is an estimate of how infectious you were on each day of the 14-day period. Since how infectious a person is or was depends on the duration and course of the infection, it can be taken into account, for example, that the more time has passed since the onset of symptoms, the lower the risk of a person spreading the virus on the day of a possible exposure. These additional transmission risk values allow a more precise determination of the likelihood that you have infected other users.

The information requested by the app about the onset of symptoms is optional. However, this information may help to calculate the transmission risk value even more accurately. If you do not provide information about your symptoms, then the transmission risk values will be calculated assuming a typical case of infection with coronavirus, i.e. the more time has passed since a random ID was used, the lower the associated transmission risk value.

<u>If you have not retrieved your test result in the app:</u>

In the event of a positive rapid antigen test result, you can only warn other people if you retrieved the test result in the app.

In the event of a positive PCR test result, on the other hand, you can warn others even if you received the test result outside the app. To do this, select the "Request TAN" procedure. The app will then prompt you to call the app hotline. A hotline worker will then ask you a few questions to make sure that you really have tested positive for coronavirus. This is to prevent

false warnings being transmitted, either by accident or intentionally. Once you have answered these questions sufficiently, you will be asked for your mobile/telephone number and your name. This is so that you can be called back later and given a unique TAN to enter in the app. Your mobile/telephone number and your name will be temporarily stored for this purpose only and deleted after an hour at the latest. Immediately after your call, the hotline worker will generate a unique TAN via a special access to the server system and then call you back to tell you this TAN. A TAN is only valid for one hour and will therefore be deleted no later than one hour after it has been passed on to you. After a valid TAN is entered in the app, it is transmitted to the server system. The TAN thus makes it possible to check that a positive test result really does exist and thus prevent false alarms. The app then receives a token from the server system, as it does after a valid QR code is scanned (see "Retrieving a test result" in Section 6 b. above).

Please note that in rare cases, if you use the warning feature, people you know personally who also use the app and then receive a warning, may infer that the warning came from you. This may be the case if a person whom you know had no contact with anyone except with you on the day for which the possible exposure is displayed.

f. Using the app for information purposes only

The app automatically receives the daily statistics that appear in the app via the server system. This generates access data. Websites linked in the app, such as www.bundesregierung.de, are opened and displayed in your standard browser (Android smartphones) or within the app (iPhones). Which data is processed in this context depends on the respective providers of the websites accessed.

g. Contact journal

The contact journal is an additional feature of the app. What you enter in the contact journal serves as a reminder for you, and can only be accessed by you. If you later test positive for coronavirus and the public health office (*Gesundheitsamt*) requires your assistance with contact tracing, then you can provide the information that it needs more quickly. If the app calculates an elevated risk for you for a particular day, then seeing this information may help you to warn the people you have had contact with early on. This will give your contacts the chance to decide whether to change their plans if necessary, i.e. to meet up with fewer people and thus reduce the risk of causing undetected infections.

h. Digital COVID certificates

The app allows you to save your digital COVID certificates and keep them with you in electronic form.

A digital COVID certificate is proof that a person has

- Been vaccinated against COVID-19 (COVID vaccination certificate)
- Tested negative for COVID-19 (COVID test certificate) or
- Recovered from a COVID-19 infection (COVID recovery certificate).

Digital COVID certificates will be valid within the European Union (EU) from 1 July 2021 as certification of COVID-19 vaccination and testing, and of recovery from COVID-19 infection. The official name is "EU Digital COVID Certificate" (COVID Certificate).

A COVID Certificate can be obtained on request after a vaccination, a test or after recovering from a confirmed case of COVID-19, from a competent entity (vaccination centres, testing points, doctors or pharmacies). You can also request a COVID test certificate directly in the app when you register a test. To do this, scan the QR code you received during the test. The app will read the information about your test from the QR code and receive the test result from the server. If you have taken a PCR test, retrieving the result and the COVID test certificate is additionally secured by means of your date of birth. A security code is generated from your date of birth (in the form of what's known as a hash value) and compared with the RKI server. This ensures that no one else can retrieve your test result. The test certificate is stored in a secure area on your smartphone after the test result is retrieved. If you retrieved a positive test result, no COVID test certificate will be generated. Your current COVID test certificate will be displayed on the app's home screen and in the "Certificates" section.

You can use a COVID Certificate in paper form or carry it with you in electronic form on your smartphone. Each certificate contains a QR code with an electronic signature from the RKI to protect against forged certificates. If you would like to save a COVID Certificate on your smartphone, you can simply scan the QR code with the app. The app then securely stores an electronic version of the COVID Certificate on your smartphone. To prevent unwanted access to the certificates stored on your smartphone, you should set up a code lock on the device.

Please note that the QR codes on the COVID Certificates contain health data (data about coronavirus vaccinations, coronavirus test results or past coronavirus infections). You should only show the certificates and QR codes if you want to provide appropriate proof. Do not provide QR codes to anyone if you do not want the data to be read.

You can use the app to scan your own printed COVID Certificates and those of family members (family certificates) and store them in encrypted form on your smartphone. You should show family certificates only when necessary for your family members to exercise their rights, such as when dining out or travelling together.

In order to prove to third parties – in the situations where this is required by law – that you have been vaccinated, have tested negative, or have recovered from COVID-19, you can show the relevant COVID Certificate to the person performing the check. If the person performing the check uses a special verification app (such as the RKI's CovPassCheck app), it is sufficient to show the QR code of the certificate and have it scanned.

The QR code is the COVID Certificate in digital form and contains only the information necessary for the specific type of certificate (see also Section 5 h.–j.).

The verification app allows for example authorities, travel companies and other service providers in the EU to scan the QR code of a COVID Certificate presented to them, in order to check its validity. During the verification, the data contained in the certificate is read. The verification app will only show whether the certificate provided is valid. If the certificate is valid, the name and date of birth of the certificate holder will also be disclosed, as will whether or not it is a test certificate. In the case of test certificates, the time of sampling will also be displayed.

The name and date of birth of the certificate holder are displayed so that the person performing the check can compare this information with proof of identity (e.g. passport or ID card). A notification of whether the certificate is a test certificate and the time of sampling are necessary to enable the person performing the check to assess whether the test result on which the certificate is based is still valid.

To protect against forged certificates, it is necessary to verify the authenticity of the stored COVID Certificates. The electronic signature contained in a certificate's QR code is used for this purpose. The electronic signature is generated by the RKI when creating the COVID Certificate on the basis of the data contained in the certificate (see also Section 5 h.–j.). The signature is a special type of encryption that allows the RKI to confirm that the certificate is an official digital document created by the RKI.

The RKI also provides the corresponding public keys from the authorities that issue certificates (in Germany, this is the RKI). These public keys can be used to check whether a certificate's electronic signature actually originates from the issuing authority and whether the certificate has been manipulated since being signed electronically.

The app regularly downloads the public keys in the background and stores them locally on your smartphone. This allows the app to check the validity of the electronic signature and thus the authenticity of the stored certificates. The public keys do not contain any personal data.

You can use the app to check whether the COVID Certificates stored in the app are valid. EU countries may adopt their own rules for the validity of COVID Certificates. For example, test certificates may be valid for a longer period in some EU countries than in others. The EU countries exchange these rules via a common exchange server. Before starting a trip, you can therefore use the app to check whether your certificates are valid in the destination country.

If you want to check whether a COVID Certificate is valid, your app downloads the current rules of all Member States from the app's server system. The app then uses the data contained in a certificate to check whether that certificate complies with the rules before showing you the corresponding result. The subsequent verification takes place exclusively offline in the app and no data is passed on here to the RKI or other recipients (other health authorities in Germany or other countries, Apple, Google and other third parties).

Please note that entry rules are subject to change and additional rules may apply both in the destination country and when you return. Guidance on entry requirements can also be found on this EU website: https://reopen.europa.eu/en.

i. Data sharing

Data sharing is an additional feature of the app. The usage data and other voluntary information transmitted to the RKI by the data sharing feature are used to assess the effectiveness of the app and enable the following improvements:

- Improving exposure logging – The aim is to improve the accuracy and reliability of the technical calculation of risks of infection. For this purpose, information about possible exposures and warnings displayed to you is analysed. The calculation method can then be fine-tuned.
- Improving app navigation for users – The aim is to make it easier to use the app. For this purpose, information about the individual steps that users take in the app is analysed. This makes it possible to make labels and texts clearer, and buttons can be placed in such a way that they can be found more easily. In addition, displays can be customised for different smartphone models.
- Providing information and assistance with the app – The aim is to identify whether there are problems when the app is used, for example with certain testing facilities and laboratories or in certain regions. This can be determined if, for example, the data sharing feature reveals that test results are available later in certain regions than in

others. In this way, the competent health authorities can also be specifically informed of potential technical disruptions.

- Improving statistics about the pandemic – The data can provide information about the temporal and spatial distribution of certain events in the pandemic and allow the authorities to respond more quickly to certain developments.

The usage data and other voluntary information will be stored and analysed without any connection to your name or identity. This means the RKI will not find out who you are or who you have met.

j. Error reports

The RKI strives to offer a bug-free app. However, due to the large number of different systems involved, this cannot always be guaranteed. To assist the app's technical support team with error analysis, you can send the error report that has been recorded in your app to the RKI. The RKI will analyse the error report in order to be able to identify and eliminate the cause of the errors that occur in your app.

For the error analysis, the error reports will be temporarily stored and analysed without any connection to your name or identity. This means the RKI will not find out who you are or who you have met. Please note that if you provide your error report ID to the technical support team (e.g. by email), this may reveal information about your identity.

k. Surveys

The surveys take place on a website outside of the app, which you will be redirected to. The app will not transmit any data to the RKI in connection with the surveys. The purposes of an RKI survey are described in the information about the survey on the survey website.

l. Confirmation of the authenticity of your app

A feature of your smartphone's operating system is used to confirm the authenticity of your app. This ensures that only app users whose app is functioning properly can share their data or participate in surveys. This prevents the statistics and survey results from being distorted.

Please note that your operating system provider may be able to tell that your smartphone has been authenticated and may therefore be able to infer your identity. However, your operating system provider will not receive any further information about your use of the Corona-Warn-App.

7. How does the transnational warning system work?

To ensure that users are also warned by the official coronavirus apps of other countries, the RKI, together with several official healthcare bodies and authorities in other countries (hereinafter referred to as **health authorities**) has set up central warning servers for sharing warnings between countries (hereinafter referred to as the **exchange server**).

- The exchange server of the participating countries among European Member States uses the digital infrastructure of the eHealth Network established between the Member States and the EU.
- In order to also enable warnings between users of the Swiss coronavirus app and the Corona-Warn-App, the RKI also operates another exchange server together with Switzerland (Federal Office of Public Health of the Swiss Confederation).

The national server systems of the coronavirus apps connected to the exchange servers regularly transmit their own positive lists to the exchange servers and receive the positive lists of the other countries. Transnational warnings can only be transmitted based on a positive PCR test and only based on encounters recorded in the COVID-19 exposure notification system. Event IDs and random IDs based on positive rapid antigen tests are therefore not transmitted to the exchange servers.

Each server system merges the positive lists received in this way with its own positive list, which allows the exposure logging feature to also take into account possible exposures involving users of another coronavirus app (see Section 6 e.) The other participating countries proceed in the same way with the positive lists provided by the RKI.

Only countries whose coronavirus apps are compatible with each other and which guarantee a comparably high level of data protection can participate in the exchange servers. In particular, this requires that the coronavirus apps of the participating countries also use the COVID-19 exposure notification system, are approved by the respective national health authorities, and respect the privacy of their users.

- The technical and organisational details of this cooperation concerning the exchange server operated within the EU are laid down in an EU Commission Decision (Commission Implementing Decision (EU) 2020/1023 of 15 July 2020, which is available at https://eur-lex.europa.eu/eli/dec_impl/2020/1023/oj). Under it, together with the respective competent health authorities of the participating countries, the RKI is a joint controller under data protection law, meaning it is responsible for processing the information contained on the positive lists (random IDs and, if applicable, information about the onset of symptoms) on the exchange servers in order to enable the transnational exposure logging and warning system.
- The operation and data exchange of the joint exchange server with Switzerland is regulated in an individual agreement between the RKI and Switzerland, available at https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html. Under the agreement, the technical operation of the exchange server is carried out by the Federal Office of Public Health of the Swiss Confederation. Together with the Federal Office of Public Health of the Swiss Confederation, the RKI is a joint controller under data protection law, meaning it is responsible for the storage, provision and subsequent erasure of the positive lists.

Please note that the list of participating countries is subject to change. The current list, with details of the competent health authorities in each case, can be found in the FAQs available at https://www.coronawarn.app/en/faq/#interoperability_countries.

8. What permissions does the app require?

The app requires access to a number of your smartphone's features and interfaces. For this purpose, you need to grant the app certain permissions. The permission system depends on your operating system's specifications. For example, your smartphone may combine individual permissions into permission categories, where you can only agree to the permission category as a whole. Please note that without the permissions requested by the app, you will not be able to use some or all of the app features.

a. Technical requirements (all smartphones)

- The app requires an internet connection in order to exchange data with the server system.
- The Bluetooth feature must be enabled so that your smartphone can transmit its own random IDs and record the random IDs of other smartphones.
- The app needs to be able to run in the background on your smartphone in order to automatically identify your risk of infection and check the status of your test. If you deny the app permission to run in the background, then you must start all actions in the app itself.

b. Android smartphones

If you are using an Android smartphone, the following system features must also be enabled:

- The Android COVID-19 exposure notification system (COVID-19 Exposure Notifications)
- If you have a smartphone running on Android version 10 or lower, location services need to be enabled for your smartphone to search for Bluetooth signals from other smartphones. Please note that no location data is collected in this process.
- The notification feature must be enabled so that you can be notified of changes to your risk of infection and the status of test results. The notification feature is enabled by default in the operating system.

The app also requires the following permissions:

- The features for retrieving a test result, checking in at an event, and adding certificates require access to the camera in order to scan QR codes.

c. iPhones (Apple iOS)

If you are using an iPhone, the following system features must be enabled:

- The iOS COVID-19 exposure notification system (Exposure Notifications)
- Notifications must be enabled so that you can be notified of changes to your risk of infection and the status of your test.

The app also requires the following permissions:

- The features for retrieving a test result, checking in at an event, and adding certificates require access to the camera in order to scan QR codes.

9. When will your data be deleted?

The storage period depends on the purposes or app features for which your data has been stored. When determining the storage period, the RKI takes into account the latest scientific findings on the incubation period (i.e. the period between exposure to infection and the appearance of the first symptoms, which is up to 14 days) as well as on how long there is a risk of an infected person infecting someone else after the end of the incubation period. Unless otherwise specified under Section 6, the following storage periods apply:

a. Data on your smartphone

The positive lists are deleted from the app memory after 14 days. Event data under “My check-ins” is automatically deleted after 14 days. Alternatively, you can delete entries under “My check-ins” manually at any time. The infection risk determined for you (e.g. “low risk”) is deleted from the app memory after each update, but after 14 days at the latest. If you have retrieved a positive test result, the token in the app memory is deleted as soon as you activate the warning feature or remove the test from the app. Your entries in the contact journal will be stored on your smartphone for 16 days before being automatically deleted. You can also delete these entries yourself at any time. Please note that if entries are added to the contact journal when you check in at an event or place, these will still be stored there even after you delete the associated check-in. Once you have created your rapid test profile, it will be stored in the app until you delete it yourself. Once you have scanned your COVID vaccination, test or recovery certificates, including family certificates, these will also be stored in the app until you delete them yourself. Please delete family certificates when you no longer need them for their intended purposes.

b. Data on server systems

Positive lists are deleted from all server systems (including the exchange server) after 14 days. All other data, with the exception of data transmitted by the data sharing feature and to confirm the authenticity of your app, will be deleted after 21 days at the latest.

c. Data sharing

Usage data and other voluntary information transmitted to the RKI by the data sharing feature will be deleted after 180 days.

d. Error reports

You can delete a recorded error report on your smartphone at any time. Error reports that you have sent to the technical support team will be deleted after 14 days at the latest.

e. Confirmation of the authenticity of your app

The identifier generated by your smartphone to confirm the authenticity of your app will be deleted from the server system after 30 days after transmission to the RKI.

10. Who will receive your data?

If you warn other users of a positive PCR test via the app, your test result (in the form of your random IDs from the last 14 days) as well as optional information you provide about the onset of your symptoms will be forwarded to the competent health authorities of each of the countries participating in the exchange servers. From there, they will be passed on to the server systems of the coronavirus apps of those countries participating in the transnational warning system. The server systems of the national coronavirus apps then distribute this information to their own users as part of the positive lists. Event IDs are only distributed to users of the Corona-Warn-App via the RKI's server system. In the event of a warning based on a positive rapid antigen test, your data will not be passed on to the exchange servers.

The competent national health authorities have commissioned the EU Commission, as data processor, to operate and maintain the joint exchange server of the participating EU countries. The exchange server for transnational warnings between the Corona-Warn-App and the Swiss coronavirus app is operated and maintained by the Federal Office of Public Health of the Swiss Confederation in consultation with the RKI.

The RKI has commissioned T-Systems International GmbH and SAP Deutschland SE & Co. KG to operate and maintain part of the technical infrastructure of the app (e.g. server system, hotline), meaning that these two companies are processors under data protection law and acting on the RKI's behalf. The EU Commission has also commissioned these companies, as sub-processors, with the technical provision and management of the participating countries' joint warning system.

Otherwise, the RKI will only pass on your data collected in connection with your use of the app to third parties if the RKI is legally obliged to do so or if this is necessary for legal action or criminal prosecution in the case of attacks on the app's technical infrastructure. In other cases, personal data will not generally be passed on by the RKI.

If, in the situations where it is required by law, you present a COVID Certificate to other persons or entities (for example, European border authorities or service providers), they will become aware of all the data contained in the certificate.

You can prevent this by only presenting the QR code of the COVID Certificate in the app, so that it can be scanned using a verification app (e.g. as proof of your vaccination status and entitlement to certain exemptions under coronavirus restrictions). Then, only the data contained in the QR code will be read. Here the verification app will only show whether the certificate shown is valid, together with an explanation of the result. In the case of a valid certificate, the name and date of birth of the certificate holder are displayed additionally in the verification app, so that the person performing the check can compare this information with proof of identity (e.g. passport or ID card). In addition, it is displayed whether the certificate is a test certificate or not. In the case of test certificates, the time of sampling is then also displayed so that the person performing the check can assess whether the underlying test result is still valid.

11. Is your data transferred to countries outside the EU?

If you activate the warning feature based on a positive PCR test, your random IDs will also be transmitted to Switzerland to the exchange server that is operated by the RKI together with the Federal Office of Public Health of the Swiss Confederation. In the event of a warning based on a positive rapid antigen test, no such transmission of your data will take place.

The EU has issued an adequacy decision for Switzerland, which determines the adequacy of the level of data protection in the country (Art. 45 GDPR). In addition, please note that users can retrieve the latest positive lists regardless of where they are (even if they are abroad on holiday or on a business trip, for example).

In addition, the confirmation of the authenticity of your app may involve the transfer of data to a country outside the EU. The identifier generated by your smartphone, which contains information about the version of your smartphone and the app, will be transmitted to the provider of your smartphone's operating system (Apple or Google). This may result in data being transferred to third countries, in particular the US. There, the level of data protection may not be considered equivalent under European law and it may not be possible to enforce your European data protection rights. In particular, there is a possibility that once the transmitted data reaches the operating system provider, it may be accessed and analysed by security authorities in the third country, for example by linking the data with other information. However, this only concerns the submitted identifier. It does not concern other information from the app, such as exposure data.

Otherwise, the data transmitted by the app is processed exclusively on servers in Germany or in another country in the EU (or the European Economic Area), which are therefore subject to the strict requirements of the General Data Protection Regulation (GDPR).

12. How can you withdraw your consent?

You have the right to withdraw any consent you granted the RKI in the app at any time with effect for the future. Please note, however, that any processing of your data that has already been carried out cannot be reversed. In particular, once your random IDs have been transmitted, the RKI has no way of deleting these from other users' smartphones.

a. Consent to "exposure logging"

You can withdraw your consent to the app's exposure logging feature at any time by disabling the feature in the app's settings or by deleting the app. If you would like to use the exposure logging feature again, you can re-enable the feature or reinstall the app.

b. Consent to "retrieving a test result"

You can withdraw your consent to the test result retrieval feature by displaying the test in the app and then deleting it. The token for retrieving the test result will consequently be deleted from the app memory, so that the token can no longer be assigned on the server system. It is not possible to assign the same test to your app again or to scan the same QR code again. If you have been tested again and wish to retrieve the test result, you will be asked for your consent again. If the test result is already available in the app, then you can no longer withdraw your consent.

c. Consent to "warning others"

If you would like to withdraw your consent to the transmission of your test result (or, more precisely, your consent to the transmission of your random IDs and event IDs, including the recorded check-in and check-out times, from the last 14 days) for warning other people, you can display the test and then disable "Warn others". You can also delete entries for events or places under "My check-ins" and thus prevent data for these events from being used for

warnings. This option is available as long as you have not yet transmitted your random IDs and event IDs to warn other users.

After you have transmitted your random IDs, you can only withdraw your consent by deleting the app. Your random IDs already transmitted to the server system will consequently be deleted from the app memory and can no longer be assigned to you personally or your smartphone. If you wish to activate the warning feature again, you will need to reinstall the app and give your consent again. Once a test result has been assigned to your app and transmitted in order to warn others, it cannot be used again to warn others.

If event IDs have already been transmitted to the server system, you can also delete them from the app memory, by deleting the entries for the events or places under “My check-ins”. Event IDs can then no longer be assigned to you personally or your smartphone.

Once your random IDs, event IDs and transmission risk values have been transmitted, the RKI has no way of deleting them from the positive lists distributed by the server system or from users’ smartphones. If you also wish to delete your exposure data stored in your smartphone’s COVID-19 exposure notification system, you may be able to manually delete it in your smartphone’s system settings. Please also note the information in Section 5 b.

d. Consent to “event check-in”

You can delete entries for events or places at any time under “My check-ins”. This will prevent data about these events from being used by the feature for warning others, and event IDs from being assigned to you personally or your smartphone.

e. Consent to “data sharing”

You can withdraw your consent to the data sharing feature at any time by disabling the data sharing feature in the app’s settings. The app will then no longer transmit your usage data and other voluntary information to the RKI on a daily basis. If you would like to allow data sharing again, you can re-enable the feature in the settings.

f. Consent to “error reports”

You can withdraw your consent to the analysis of error reports already submitted to the RKI by informing the technical support team that you no longer wish to have the error report analysed, stating your error report ID. Your error report will then be deleted. Please note that the RKI may learn your identity in the process. If you do not provide your error report ID to the technical support team, the submitted error report will be automatically deleted after 14 days.

g. Consent to “survey participation”

You do not give your consent to participate in an RKI survey in the app, but via the website on which the survey is conducted. There you will also find information about how you can withdraw your consent.

h. Consent to “confirmation of the authenticity of your app”

If you withdraw your consent to the confirmation of your app’s authenticity, this will not directly affect the related data processing. The transmission of the identifier generated by your

smartphone to the operating system provider, and the verification and confirmation of the authenticity of your app, take place immediately after you have given your consent.

13. What other rights do you have under data protection law?

If the RKI processes your personal data, you also have the following data protection rights:

- The rights under Art. 15, 16, 17, 18, 20 and 21 GDPR,
- the right to contact the official RKI data protection officer and raise your concerns (Art. 38(4) GDPR) and
- the right to lodge a complaint with a data protection supervisory authority. To do so, you can either contact your local supervisory authority or the authority responsible for the RKI. The supervisory authority responsible for the RKI is the Federal Commissioner for Data Protection and Freedom of Information, Graurheindorfer Straße 153, 53117 Bonn.

You also have these data protection rights vis-à-vis the health authorities responsible for data processing in the countries participating in the exchange servers, insofar as you have transmitted your random IDs from recent days to warn other people (see Section 7).

Please note that the rights mentioned above can only be fulfilled if the data on which your claim is based can be clearly assigned to you. This would only be possible if the app were used to collect further personal data that would allow the data transmitted to the server system to be clearly assigned to you or your smartphone. Since this is not necessary for the purposes of the app, the RKI is not obliged to collect such additional data (Art. 11(2) GDPR). Moreover, this would run counter to the stated objective of collecting as little data as possible. For this reason, it will generally not be possible to fulfil the above data protection rights even if you provide additional information about your identity.

14. Data protection officer and contact

If you have any questions or concerns regarding data protection, you are welcome to send them to the RKI's official data protection officer by post to Robert Koch-Institut, FAO the data protection officer, Nordufer 20, 13353 Berlin, or by emailing datenschutz@rki.de.