Privacy notice
Corona-Warn-App

This privacy notice explains what data is collected when you use the Corona-Warn-App, how that data is used, and your rights under data protection law.

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

1. Who has provided you with this app?

The Corona-Warn-App (the "**App**") is provided by the Robert Koch Institute, Nordufer 20, 13353 Berlin (the "**RKI**").

The RKI is also what is called the controller under data protection law, meaning it is responsible for the processing of App users' data.

You can contact the RKI's data protection officer at the above address ("FAO the data protection officer") and by emailing: datenschutz@rki.de.

2. Is using the App voluntary?

Using the App is entirely voluntary. It is your decision alone whether and how you use the App.

Although installing and using the App is voluntary, if you wish to use the risk identification feature you still have to grant the RKI your consent to let the App process your personal data (including health data, if the App detects that you may be infected). You do this by tapping on the "Enable/Turn On" button the first time you open the App. This is necessary because otherwise the App will not be able to access your smartphone's exposure logging feature. You can, however, use the toggle switch in the App to disable the risk identification feature at any time. Doing this will mean that you are unable to use the full functionality of the App. Separate consent is also required for the data processing performed for the following features:

- Registering a test (see 6 b.)
- Sharing your test result (see 6 c.).

The data processing performed in connection with these features is described in more detail in the following sections.

3. On what legal basis is your data processed?

In principle, the RKI will process your personal data only on the basis of your consent granted pursuant to Article 6(1) Sentence 1(a) and Article 9(2)(a) of the General Data Protection Regulation (GDPR). If you have granted your consent, you can withdraw it at any time. Further information on your right of withdrawal and instructions on how to exercise this right can be found under 11.

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 personal data is processed?

The App is designed to process as little personal data as possible. This means, for example, that the App does not collect any data that would allow the RKI or other users to infer your identity, health status or location. In addition, the App deliberately refrains from using tracking tools to record or analyse how you use the App.

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

a. Access data

Each time a file stored on a server is retrieved, this generates access data. Specifically, the following data is processed with each retrieval:

- IP address
- Date and time of retrieval (time stamp)
- Transmitted data volume (or packet length)
- Notification of successful retrieval
- Requesting domain
- Operating system used
- Device type (smartphone), the manufacturer and the model of your smartphone (e.g. iPhone 7 or Galaxy S9).

This access data is only processed to secure and maintain the technical infrastructure. You are not identified personally as a user of the App and it is not possible to create a user profile.

Access data is generated when you use or enable the following features:

- Risk identification
- Registering a test
- Sharing your test result.

b. Contact data

If you enable exposure logging in your smartphone's operating system, which serves to record encounters (contacts) with other users, then your smartphone will continuously send out randomly generated identification numbers ("**random IDs**") via Bluetooth, which other smartphones in your vicinity can receive if exposure logging is also enabled on them. Your smartphone, in turn, also receives the random IDs of the other smartphones. In addition to the random IDs received from other smartphones, your smartphone's exposure logging functionality records and stores the following contact data:

- Date of the contact
- Duration of the contact
- Bluetooth signal strength of the contact.

Your own random IDs and those received from other smartphones as well as the other contact data (date, duration, signal strength) are recorded by your smartphone in an exposure log and stored there for 14 days.

The functionality used to record encounters with other users is called "COVID-19 Exposure Notifications" on Android smartphones and "COVID-19 Exposure Logging" on iPhones. Please note that this exposure logging functionality is not part of the App, but an integral part of your smartphone's operating system. This means that the exposure logging functionality is provided to you by Apple (iPhones) or Google (Android smartphones) and is subject to these companies' respective privacy policies. The RKI has no influence on data processing performed by the operating system in connection with exposure logging.

More information about the exposure logging functionality on Android smartphones is available at: https://support.google.com/android/answer/9888358?hl=en.

More information about Apple's exposure logging functionality can be found in your iPhone's settings under "Privacy" > "Health" > "COVID-19 Exposure Logging". Please note that the exposure logging functionality is only available if iOS version 13.5 or higher is installed on your iPhone.

The App will only process the contact data generated and stored by your smartphone if the App's risk identification feature is enabled.

c. Health data

Health data is any data containing information about the health of a particular individual. This includes not only information about past and current illnesses, but also about a person's risk of illness (such as the risk that the person has been infected with the coronavirus).

Your health data will be processed in the following cases:

- If the risk identification feature detects that you may have been in contact with a person who has been infected with the coronavirus.
- If you register your test.
- If you share a positive test result.

6. App features

a. Risk identification

The App's core functionality is risk identification. This serves to track possible contacts with other users of the App who are infected with the coronavirus, to evaluate the risk that you yourself have been infected, and – based on the risk identified – to provide you with health advice and recommendations for what to do next.

If you enable the risk identification feature, then several times a day while the App runs in the background (or when you tap on "Update"), the App will retrieve a list from the App's server system of random IDs from users who have shared a positive test result. The App shares these random IDs with your smartphone's exposure logging functionality, which then compares them with the random IDs stored in your smartphone's exposure log. If your smartphone's exposure logging functionality detects a match, it transfers the contact data (date, duration, signal strength) to the App, but not the random ID of the contact in question.

In the event of a contact, the App analyses the contact data provided by the exposure logging functionality in order to determine your individual risk of infection. The evaluation algorithm which determines how the contact data is interpreted (for example, how the duration of a contact influences the risk of infection) is based on current scientific findings. To account for new findings as and when they arise, the RKI can update the evaluation algorithm by adjusting its settings. The settings for the evaluation algorithm are sent to the App together with the list of random IDs.

The identification of your risk of infection is only carried out locally on your smartphone, meaning that the data is processed offline. Once identified, the risk of infection is also only stored in the App and is not passed on to any other recipients (including the RKI, Apple, Google and other third parties).

The legal basis for the processing of your access data, contact data and, if applicable, health data (if the App determines that you may have been infected) described above is your consent which you gave when enabling the risk identification feature.

b. Registering a test

If you have been tested for the coronavirus, you can register the test in the App by scanning the QR code which you received from your doctor or the testing facility. The app will then inform you as soon as the test result is available from the laboratory.

For this to work, the testing laboratory needs to be connected to the App's server system and, as part of the testing procedure, you must have agreed separately to the laboratory transmitting your test result to the App's server system (test result database). Test results from laboratories that are not connected to the App's server system cannot be displayed in the App. If you have not received a QR code, the testing laboratory is not connected. In this case you will not be able to use this feature.

Registering a test

To receive the test result in the App, you must first register the test you have taken in the App. For this purpose, your doctor or the testing facility will provide you with a QR code when taking the sample. This QR code contains a code number which can be read with a QR code scanner. To register your test, you will need to scan the QR code in the App using your smartphone's camera.

The code number read from the QR code is then hashed by the App, which means that the App performs a certain mathematical procedure in order to convert the code number in such a way that nobody can identify it. As soon as your smartphone is connected to the internet, the App will transmit the hashed code number to the App's server system. In return, the App receives a token from the server system, i.e. a digital access key that is stored in the App. The token is linked to the hashed code number on the server system. The App then deletes the hashed code number on your smartphone. The server system will only issue a token once for each hashed code number. This ensures that your QR code cannot be used by other users of the App to retrieve test results.

This completes the registration of your test.

Filing of the test result

As soon as the testing laboratory receives the test result, it stores the result in the RKI's test result database, indicating the hashed code number. The test result database is

operated by the RKI on a special server within the App's server system. Based on the code number contained in the QR code issued to you, the testing laboratory also generates the hashed code number using the same mathematical procedure as the App.

Retrieval of the test result

Using the token, the App regularly requests the status of the registered test from the App's server system. The server system then assigns the token to the hashed code number and transfers it to the test result database. If the test result has now been stored there, the test result database sends the test result back to the server system, which forwards it to the App without gaining any knowledge of the content.

If the test result is positive, the App uses the token again to request a TAN (transaction number) from the server system. The server system reassigns the token to the hashed code number and requests confirmation from the test result database that a positive test result exists for the hashed code number. If the test result database confirms this, the server system generates the TAN and transmits it to the App. A copy of the TAN remains on the server system.

The TAN is required to ensure that no false information is distributed to other users in the event of a positive test result being transmitted.

The legal basis for the processing described above of the data mentioned above is your consent to using the test registration feature.

c. Sharing your test result

If you share your positive test result in order to warn other users, the App will transfer the random IDs generated and stored by your smartphone from the last 14 days and the TAN to the App's server system. The server system first checks whether the TAN is valid and then adds your random IDs to the list of random IDs of users who have shared a positive test result. Your random IDs can now be downloaded by other users as part of the risk identification process.

If you have not retrieved your test result in the App:

Even if you have not retrieved a positive test result in the app, you can share the test result via the App to warn other users. In this case, the App prompts you to enter a so-called TeleTAN, which acts as a TAN.

To obtain a TeleTAN, please call the Corona-Warn-App hotline on +49 (0)800 7540002. The operator will first ask you some questions over the phone to check the plausibility of your call. These questions serve to prevent fraudulent reports of infections and any resulting incorrect warnings and risk levels. Once you have answered these questions sufficiently, you will be asked for your mobile/telephone number. This is so that you can be called back later and given a TeleTAN to enter in

the App. Your mobile/telephone number will only be temporarily stored for this purpose and deleted within one hour at the latest.

After your call, the hotline employee will generate a TeleTAN via a special access to the App's server system and then call you to tell you the TeleTAN. If you enter the TeleTAN in the App, the TeleTAN will be sent back from the App to the App's server system for comparison and verification. In return, the App receives a token from the server system, i.e. a digital access key that is stored in the App. Using this token, the App then requests a TAN from the server system.

The legal basis for this processing of your access data and health data (random IDs, test result, TAN and, if applicable, TeleTAN) is your consent to using the feature for sharing your test result.

d. Using the App for information purposes only

As long as you use the App for information purposes only, i.e. do not use any of the App features mentioned above and do not enter any data, then processing only takes place locally on your smartphone and no personal data is generated.

7. What permissions and functionality 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. Permissions are programmed differently by different manufacturers. For example, individual permissions may be combined into permission categories, where you can only agree to the permission category as a whole. Please note that if the App is denied access, you will not be able to use any or all of the App's features.

a. Technical requirements (all smartphones)

- Internet

  The App requires an internet connection for the risk identification feature, and so that it can receive and transmit test results, so that it can communicate with the App's server system.

- Bluetooth

  Your smartphone's Bluetooth interface must be enabled for your smartphone to record random IDs from other smartphones and store them in the device's exposure log.

- Camera

  Your smartphone requires a camera to be able to scan a QR code when registering a test.

- Background operation

The App runs in the background (i.e. when you are not actively using the App) in order to be able to automatically identify your risk and query the status of a registered test. If you deny the App permission to run in the background in your smartphone's operating system, then you must start all actions in the App itself.

b. Android smartphones

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

- COVID-19 Exposure Notifications

  The App's risk identification feature requires this functionality. Otherwise, no exposure log with the random IDs of your contacts will be available. The functionality must be enabled within the App to allow the App to access the exposure log.

- Location

  Your smartphone's location service must be enabled for your device to search for Bluetooth signals from other smartphones. Please note that no location data is collected in this process.

- Notification

  The user is notified locally of the identified risk and available test results. The necessary notification function is already enabled in the operating system.

The App also requires the following permissions:

- Camera

  The App requires access to the camera to read the QR code when registering a test.

c. iPhones (Apple iOS)

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

- COVID-19 Exposure Logging

  The App's risk identification feature requires this functionality, otherwise no exposure log with the random IDs of your contacts will be available. The functionality must be enabled within the App to allow the App to access the exposure log.

- Notifications

  The user is notified locally of the identified risk and available test results. Notifications must be enabled for this.

The App also requires the following permissions:

- Camera

  The App requires access to the camera to read the QR code when registering a test.

8. When will data be deleted?

All data stored in the App is deleted as soon as it is no longer needed for the App features:

a. Risk identification

- The list of random IDs of users who have shared a positive test result will be deleted from the App immediately after comparison with the random IDs in your smartphone's exposure log.
- The RKI has no way of influencing the deletion of contact data in your smartphone's exposure log (including your own random IDs) and contact data on other smartphones, as this functionality is provided by Apple or Google. In this case, the deletion depends on what Apple or Google has determined. Currently, the data is automatically deleted after 14 days. It may also be possible, using the functionality provided by Apple and Google, to manually delete data in your device's system settings.
- The risk level displayed in the App will be deleted as soon as a new risk level has been determined. A new risk level is usually determined after the App has received a new list of random IDs.

b. Registering a test

- The hashed code number will be deleted from the App's server system after 21 days.
- In the event of a negative test result, the hashed code number and the test result will be deleted from the test result database immediately after the test result is retrieved; and in the event of a positive test result, they will be deleted immediately after the copy of the TAN stored on the server system is deleted (see below).
- The token stored on the server system will be deleted after 21 days.
- The token stored in the app will be deleted from the smartphone after the App is deleted or after the test result is shared.

c. Sharing your test result

- Your smartphone's own random IDs which are shared in the App will be deleted from the server system after 14 days.
- The copy of the TAN stored on the server system will be deleted after 21 days.
- The TAN stored in the App will be deleted after the test result has been shared.
- The TeleTAN stored in the App will be deleted after the test result has been shared.
- The TeleTAN stored on the server system will be deleted after 21 days.
- The TeleTAN sent to the hotline employee will be deleted there immediately after it has been passed on to you by telephone.
- The token stored on the server system will be deleted after 21 days.
- The token stored in the App will be deleted after the test result has been shared.

9. Who will receive your data?

If you share a test result to warn other users, your random IDs from the last 14 days will be passed on to the App on other users' smartphones.

The RKI has commissioned Deutsche Telekom AG 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 (Article 28 GDPR).

Otherwise, the RKI will only pass on personal 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.

10. Is data transferred to a third country?

The data generated when the App is used is processed exclusively on servers in Germany or in another EU or EEA member state.

11. Withdrawal of 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 that this will not affect the lawfulness of the processing before the withdrawal.

To withdraw your consent to the risk identification feature, you can disable the feature using the toggle switch in the App or delete the App. If you decide to use the risk identification feature again, you can toggle the feature back on or reinstall the App.

To withdraw your consent to the test registration feature, you can delete the test registration in the App. The token for retrieving the test result will then be deleted from your device. Neither the RKI nor the testing laboratory can then assign the transmitted data to your App or smartphone. If you wish to register another test, you will be asked to grant your consent again.

To withdraw your consent to the sharing of your test result, you must delete the App. All of your random IDs stored in the App will then be removed and can no longer be assigned to your smartphone. If you wish to report another test result, you can reinstall the App and grant your consent again. Alternatively, you may be able to delete your own random IDs in the exposure log in your smartphone's system settings. Please note that, once transmitted, the RKI has no way of deleting your random IDs from the lists and from other users' smartphones.

12. Your other rights under data protection law

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

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

Please note that the RKI can only fulfil the rights mentioned above if the data on which your claim is based can be clearly assigned to you. This would only be possible if the RKI were to collect further personal data that would allow the data mentioned above to be clearly assigned to you or your smartphone. Since this is not necessary – and not intended – for the purposes of the App, the RKI is not obliged to collect such additional data (Article 11(2) GDPR). Moreover, this would run counter to the stated objective of keeping the amount of data processed for the App as low as possible. Against this backdrop, it will not normally be possible to directly fulfil the above data protection

rights under Articles 15, 16, 17, 18, 20 and 21 GDPR, as doing so would require additional information about you which is not available to the RKI.

Last amended: 5 June 2020