

Privacy notice

Last amended: 17 October 2020. Valid from app version 1.5 (earlier versions available at: <https://www.coronawarn.app/en/privacy>)

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:

1. Who is the Corona-Warn-App published by?
2. Is using the app voluntary?
3. On what legal basis is your data processed?
4. Who is the app aimed at?
5. What data is processed?
6. Why is your data processed?
7. How does the transnational warning system work?
8. What permissions does the app require?
9. When will your data be deleted?
10. Who will receive your data?
11. Is your data transferred to countries outside the EU?
12. How can you withdraw your consent?
13. What other rights do you have under data protection law?
14. Data protection officer and contact

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 data is processed in accordance with data protection regulations.

If you are infected and voluntarily use the transnational warning feature, it is also possible to warn users of the official coronavirus apps of other participating countries with whom you have been in contact. In this case, the RKI and the competent health authorities of the countries participating in the transnational warning system 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. All of the app's features that

require data transfer will obtain your express consent in advance. If you do not give your consent or if you subsequently withdraw it, this will not result in any disadvantages for you.

3. On what legal basis is your data processed?

Your data will only be processed on the basis of your explicit consent. The legal basis is Art. 6(1) Sentence 1(a) GDPR and, in the case of health data, Art. 9(2)(a) GDPR. After granting your consent, you can withdraw it at any time. Please refer to Section 12 for further information about your right of withdrawal.

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 has been programmed to process as little personal data as possible. This means that the app does not collect any data that would allow the RKI or other users to infer your identity, your name, your location or other personal details. The app does not therefore use any analysis tools to evaluate the way you use it.

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 are not 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 Notification" 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 Notification" and tapping on "How Exposure Notification works ...".

c. 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 register a test or a positive test result
- If you retrieve a positive test result in the app
- If you use the app to warn other users that they may be infected
- If you provide information about the onset of any coronavirus symptoms.

Section 6 explains this in more detail.

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 contacts with persons who have tested positive for coronavirus ("possible exposures") in a number of different countries, to assess the risk that you yourself have been infected as a

result of one of those contacts, and to provide you with appropriate health advice and recommendations for what to do next.

For this purpose, the app runs in the background and retrieves an up-to-date list every day of random IDs, and possible information about the onset of symptoms, from the server system. This list contains the random IDs and possible symptom information of users who have tested positive for coronavirus and voluntarily used the warning feature in their app, which is the official coronavirus app in any country participating in the transnational warning system (see Section 7) (hereinafter referred to as a **positive list**). The random IDs in the positive list also contain a transmission risk value and an indication of the type of diagnosis (see Section 6 c.).

The app passes the random IDs to the COVID-19 Exposure Notification System, which compares them with the random IDs it has recorded. 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. The app evaluates this data as well as the information in the positive list (transmission risk value; information about the onset of symptoms) in order to determine your risk of infection. The evaluation algorithm which determines how this information is evaluated (for example, how the duration of a contact influences the risk of infection) is based on the RKI's latest scientific findings. In the event of new findings, the RKI can update the evaluation algorithm by adjusting the evaluation settings in the app. In this case, the new evaluation settings are sent to the app together with the positive list.

The risk of infection is calculated exclusively within 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).

b. Registering a test

If you have been tested for coronavirus, you can register your test in the app. The app will then notify you as soon as the test result is available. For this to work, the testing laboratory needs to be connected to the server system and, as part of the testing procedure, you must have agreed separately to the laboratory transmitting your test result to the server system (test result database). It is not possible to display test results from laboratories that are not connected to the server system. If you have not received a QR code, then you cannot use this feature.

Registering a test

To be able to retrieve your test result in the app, you must first register your test. Your doctor or the testing facility will provide you with a QR code for this purpose. This QR code contains a code number which the app can read. To register your test, you will need to scan the QR code in the app using your smartphone's camera. 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. As soon as your smartphone is connected to the internet, the app will transmit the hashed code number to the 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 in the server system. The app then deletes the hashed code number on your smartphone. This completes the registration of your test. 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.

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 located on a special server within the 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 server system. The server system then assigns the token to the hashed code number and transfers it to the test result database. This checks whether a test result has now been stored for the hashed code number and returns the result. The server system then forwards the status and the test result requested from the test database (i.e. whether your result is positive or negative) to the app. If you have enabled the test status notification in the app (under "Settings" > "Notifications"), you will be notified accordingly. The test result will be displayed when 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 if you subsequently activate the app's warning feature. To this end, 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 that 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.

c. Warning others

If you have tested positive for coronavirus, you can use the transnational warning feature to warn other people who use this app or any other official coronavirus app in participating countries. In this case, the app transmits the following data to the server system:

- Your own random IDs from the last 14 days
- Any information about the onset of symptoms
- Your TAN (see Section 6 b.).

Your smartphone may first ask you for permission to pass your own random IDs from the COVID-19 Exposure Notification System to the app.

Before transmitting the random IDs to the server system, the app adds a transmission risk value and a specification of the type of diagnosis to each of the random IDs (see also Section 6 a.). Since the app's warning feature can only be used for lab-confirmed diagnoses, the type of diagnosis is the same for all users. The transmission risk value is an estimate of how infectious you were on the day on which the respective random ID was used. 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.

The requested information about the onset of symptoms is optional. However, this information may help to calculate the transmission risk value 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.

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

Even if you have not retrieved your positive test result via the app, you can still warn your fellow human beings. 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 what’s called a TeleTAN 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 your TeleTAN via a special access to the server system and then call you back to tell you your TeleTAN. A TeleTAN 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 TeleTAN is entered in the app, it is transmitted to the server system for verification. Upon successful verification, 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.

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 features mentioned above, then processing only takes place locally on your smartphone and the RKI will not process any personal data. Websites linked in the app, such as www.bundesregierung.de, are opened and displayed in your smartphone’s standard browser (Android smartphones) or within the app (iPhones). The data processed here is determined by the respective providers of the websites accessed.

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 a central warning server for sharing warnings between countries (hereinafter referred to as the **exchange server**). The exchange server uses the digital infrastructure of the eHealth Network established between the Member States.

The national server systems of the coronavirus apps connected to the exchange server regularly transmit their own positive lists to the exchange server and receive the positive lists of the other countries.

The 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 point 6 c.) 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 joint exchange server. 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 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).

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 in the positive lists (random IDs and, if applicable, information about the onset of symptoms) on the exchange server in order to enable the transnational exposure notification and warning system.

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 a registered 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.
- To be notified of changes in your risk of infection and the status of test results, the notification feature must be enabled. The notification feature is enabled by default in the operating system.

The app also requires the following permissions:

- The feature for registering your test requires access to the camera in order to read the QR code.

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 Notification)
- Notifications must be enabled so that you can be notified of changes in your risk of infection and the status of test results.

The app also requires the following permissions:

- The feature for registering your test requires access to the camera in order to read the QR code.

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 (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 retrieved positive lists are deleted from the app memory after 14 days. The infection risk determined in the app (e.g. "low risk") is deleted from the app memory after each update, but after 14 days at the latest. If you have registered a positive coronavirus test, the token in the app memory is deleted as soon as you activate the warning feature.

b. Data on server systems

Positive lists are deleted from all server systems (including exchange servers) after 14 days. All other data will be deleted after 21 days at the latest.

10. Who will receive your data?

If you warn other users via the app, 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 server. 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 your data to their own users as part of the positive lists.

The competent national health authorities in the participating countries have commissioned the EU Commission, as data processor, to operate and maintain the joint warning system.

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.

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

If you activate the app's warning feature, the coronavirus apps connected to the shared exchange server can retrieve the current positive lists worldwide, which means that users who are currently abroad on holiday or business trips, for example, can also be warned. 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 that this will not affect the lawfulness of the processing before the withdrawal.

a. Consent to Exposure Logging

To withdraw your consent, you can disable the exposure notification feature or delete the app. If you would like to use the exposure notification feature again, you can re-enable the feature or reinstall the app.

b. Consent to test registration

To withdraw your consent, you can delete the test registration in the app. 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 will not be possible to register the same test again. If you wish to register a new test, you will be asked to grant your consent again.

c. Consent to warning feature

To withdraw your consent, you will need to delete 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. If you wish to activate the warning feature again, you will need to reinstall the app and grant your consent again. Once registered in the app, a test result cannot be used again to warn others.

Once your random 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 the 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.

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 Articles 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 competent 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.

In respect of the joint processing performed by the transnational exchange server, you also have these data protection rights vis-à-vis the health authorities responsible for data processing in the countries participating in the exchange server (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.
