EUROPEAN COMMISSION

QUESTIONS AND ANSWERS

Brussels, 19 October 2020

Coronavirus: EU interoperability gateway for contact tracing and warning apps – Questions and Answers

Index

1. Using coronavirus tracing and warning apps

What is a coronavirus tracing and warning app?

Most public health authorities in the EU have developed apps that support contact tracing and warning in the fight against coronavirus. The apps notify you if you have been at risk of exposure to the virus over the last 14 days, whether or not you feel symptoms. You will then get appropriate health advice. This helps to minimise the spread of the virus and speed up a return to normal life within the EU. Furthermore, you can get tested and receive any necessary treatment promptly and lower the risk of serious consequences, if you get alerted at an early stage.

Tracing and warning apps are part of a package of measures to prevent the spread of the virus, along with hygiene measures such as hand washing, social distancing and using everyday facemasks.

Why using a coronavirus tracing and warning app?

A tracing and warning app can help break the chain of coronavirus infections, nationally and across borders, and help save lives by complementing manual tracing. The faster people who have been diagnosed with COVID-19 and their contacts can be informed, the less quickly and widely the virus can spread. The app therefore help to protect yourself, your family, your friends and everyone around you.

If you use an official app available in your country, developed with the health authorities, you can trust them and use them without concerns. More information also on re-open EU.

How does a coronavirus tracing and warning app work?

A coronavirus tracing and waring app informs you if you have been, for a certain period, close, to another app user who was confirmed infected with COVID-19. Such an encounter would be considered a high-risk exposure. Typically, this means a contact for more than 15 minutes and less than 2 meters. The exact parameters are set by national health authorities.

When you have installed the app, your smartphone generates random 'keys' multiple times a day. These keys are exchanged through Bluetooth between nearby smartphones running a tracing app, and stored on the device for 14 days.

In case you are tested positive for COVID-19, you can share this information to warn the people you have previously been close to. Your phone will then share the keys generated during the last 14 days with the backend server of your national app.

On the basis of the keys received, each app calculates the risk score of a user, who may receive an exposure alert if the criteria are met.

What data will I share when using these apps?

The apps generate arbitrary identifiers, which are random sets of numbers and letters. These arbitrary identifiers do not allow the identification of an individual person. The keys are exchanged via Bluetooth between phones at short distance. No geolocation or movement data are used.

Do tracing apps use a lot of data or battery?

Once you have downloaded the app, its data usage is minimal. You should also not notice a significant difference in terms of battery life, nor should your smartphone overheat. The contact and warning app runs in the background. It uses Bluetooth Low Energy, a technology designed to be particularly energy efficient.

Can I use the app without internet connection?

For the tracing functionality as such, a permanent Internet connection is not necessary. Bluetooth, which is used to detect proximity with other app users, does not require Internet. It would even work in flight mode if you switch on Bluetooth during the flight. However, the app does need to connect to the internet at least once a day to download the information necessary to check if you have been exposed to other, infected users. Hence, to check infection chains, to receive alerts, and for additional functionalities, the apps will need to connect through mobile Internet or Wi-Fi.

Is the exposure notification automatic?

The apps work in the background of the device without requiring any daily action. Notifications come in automatically. You do not have to activate updates manually, however you need to have the exposure notification function switched on.

May I use several national coronavirus tracing and warning apps at the same time?

No. Using two or more apps at the same time is not possible as the Google/Apple exposure notification interface always supports only one tracing app at a time. Thanks to the EU interoperability gateway service, citizens can use one single app even when they travel cross-borders, while continuing to benefit from contact tracing and being able to report a positive test or to receive an alert.

2. In case of a notification

What should I do if I receive an alert?

Receiving a contact alert does not necessarily mean you have been infected with COVID-19. An alert is a simple way of making you aware that there is a risk of exposure to coronavirus. The app will guide you on what you should do, according to the instructions of national health authorities, such as advice to get tested or to self-isolate, and who you have to contact.

Which criteria are used to assess exposure risk levels?

Potential exposures happen when you encounter, for a certain amount of time and at a certain distance, a person who has reported being infected with the virus. Bluetooth technology is used to determine whether or not an encounter is close and long enough to result in a potential exposure. There are typically three levels of risk:

- **Low risk:** The app user had no encounter with anyone known to have been diagnosed with COVID-19, or if they have had such an encounter it was not close and/or long enough according to the criteria. The user is informed about generally applicable social distancing regulations and hygiene recommendations.

- **Increased risk:** The user is informed that the check of their exposure logging has shown an increased risk of infection, as they have encountered at least one person in the last 14 days who has been diagnosed with COVID-19. The person is recommended to stay at home if possible, and to seek advice from their general practitioner or local health authorities.

- **Unknown risk:** If the risk identification has not been activated for long enough by the person, then no risk of infection can be calculated yet. Risk identification is possible within 24 hours of installation, at which point the status information displayed changes from "unknown risk" to "low risk" or "increased risk".

Can the app warn me how to avoid contact with people who tested positive?

No, the app cannot predict such contacts or detect risky contact in real time. To protect user privacy, no app user can be identified or located using the app, and no app can detect whether there is an infected person in, for example a supermarket. The app is no substitute for the usual necessary precautions, like wearing a mask.

3. EU interoperability gateway: contact tracing across borders

How do coronavirus tracing and warning apps work across borders?

Coronavirus does not stop at borders. This is why Member States, supported by the Commission, were working on an interoperability solution for national contact tracing and warning apps, to allow citizens to use one single app when they travel abroad in Europe, while continuing to benefit from contact tracing and being able to receive an alert.

At the request of Member States, the Commission has set up an interoperability gateway service, an interface to efficiently receive and pass on relevant information from national contact tracing apps. It will ensure the secure and efficient cross-border exchange between participating apps while keeping mobile data usage to a minimum.

How does the exchange of data between the apps work?

The individual coronavirus tracing and warning apps only connect to their own national backend server. The national backend servers do not connect directly with each other. They exchange the information via the EU interoperability gateway service, which reduces data consumption compared with direct exchanges between participating apps.

The exchange consists of two main parts: Uploading of national keys to the gateway server takes places if users upload their keys and have agreed with sharing them with other European app users; downloading of keys to the national backend server is required so that the keys can be distributed to the users of the individual national app.

What is the EU interoperability gateway service?

The interoperability gateway service (gateway) is a digital infrastructure that ensures the secure transmission of generated keys between the backend servers of participating national contact tracing and warning apps. While doing so, the gateway will share the minimum information necessary for a person to be alerted if they have been exposed to an infected person also using one of the participating apps.

The data exchanged will only be stored in the gateway for a maximum period of 14 days. No other information except the keys, generated by the national apps, will be handled by the gateway.

The design of the gateway builds on the guidelines for interoperability, the set of technical specifications agreed between Member States and the Commission, the principles set out in the EU toolbox and the Commission and European Data Protection Board guidelines on data protection for contact tracing and warning apps.

The gateway was developed and set up by companies T-Systems and SAP, and is operated from the Commission's data centre in Luxembourg.

Are all contact tracing apps interoperable?

The gateway ensures a safe exchange of information between contact tracing apps based on a 'decentralised' architecture. This concerns the vast majority of tracing apps that were, or are to be, launched in the EU. Apps that are interoperable can exchange information among themselves, so people in the EU only need install one app – typically

the app of their home country – and still be able to report a positive test or to receive an alert, even if they travel in the EU.

What is the difference between 'centralised' and 'decentralised' apps?

Confronted with the new potential of smartphones to combat the coronavirus pandemic, developers discussed mainly two different ways of how to set up contact tracing and waring apps, typically referred to as 'decentralised' and 'centralised' architectures. In both approaches, smartphones exchange temporary keys via Bluetooth and communicate with a central server. The main difference is in the calculation of the exposure risk of users and the storage of the data. Regardless of the approach, none of the tracing apps track location or movements

In a centralised system, a central server receives the keys of the contacts collected by users confirmed with COVID-19, and the server does the matchmaking to alert users at risk.

In a decentralised approach, the keys of the contacts remain on the phone. The app downloads the arbitrary keys of COVID-19 infected users and checks whether there is a match, directly on the device. The decentralised approach uses a joint interface provided by Apple and Google (see below). In the end, almost all national health authorities in the EU opted for a decentralised app, and these apps are all potentially interoperable.

Which national apps are, or will be, linked to the gateway?

About two third of EU Member States have developed compatible tracing and warning apps, and the gateway is open to all of them, once they are ready to connect. The connection will gradually take place during October and November, however apps can also connect at a later stage if national authorities wish so. An 'onboarding protocol' has been developed, setting out the necessary steps.

While your app is able to detect proximity with other participating apps everywhere in the world, including during flights in a plane, it does of course matter if people around you also have access to and use a participating app.

The overview of participating countries is updated regularly and available here [LINK].

What about if I did a test in another EU country?

You can only insert a positive coronavirus test result in the app of the country where the test was taken. However, when you enter the code in that app, thanks to the interoperability, citizens from the country that you have visited will get notified that they have been in close contact of an infected case.

I never travel anywhere. Do I need to take part in interoperability?

Downloading and using an app is voluntary, and participating in the interoperability framework is as well. To do so, you need to agree to your data being processed. However, even if you do not intend to travel, other people may do so, and you may be close to them without knowing. Therefore, interoperability also benefits those who stay in their home country.

Do I need to download a new app to benefit from interoperability?

No. You can continue to use your national app. Most EU Member States have decided to set up a national coronavirus tracing and warning app, and almost all of those have opted for a decentralised system – all these apps are potentially interoperable and can connect to the gateway, once they are ready. Once an app gets connected to the gateway, an update needs to be issued in the app stores so the additional functionality can be used. Users need to install that update so that their app works cross-border.

How do I update the app?

If your phone is set to update automatically, your tracing app will update automatically within a few days of the update being released. If you want to update manually:

- For iPhone users, open the App Store and tap 'Today' at the bottom of the screen. Then tap your profile icon to bring up your Account. Scroll down until you see your national app and then tap 'Update'.

- For Android users, open the 'Play Store' and tap on the three horizonal lines at the top-left of the screen to open the sidebar. Open 'My apps & games' and select the 'Updates' tab. Then scroll down to your national app and tap 'Update'.

4. Privacy and security

Can tracing apps be used by authorities to monitor quarantine?

No, this is technically impossible. Contact tracing and warning apps do not gather any location or movement data.

How is my privacy protected?

Throughout the entire process of design and development of contact and warning tracing apps, respect for privacy has been of paramount importance:

- The app does not collect any data that could lead to unveiling your identity. It does not ask for and cannot obtain your name, date of birth, address, telephone number, or email address.
- The app does not collect any geolocation data, including GPS data. It also does not track any movements.
- The Bluetooth Low Energy code is generated completely randomly and does not contain any information about you or your device. This code changes several times each hour, as a further protection.
- All data stored by the app on your smartphone, and all connections between the app and the server, and between the servers and the gateway, are encrypted.
- All data, whether stored on your device or on the server, is deleted when no longer relevant, i.e. 14 days after transfer between app and server.

- The data is stored on secure backend servers, managed by national authorities. The gateway uses a secure server, hosted by the Commission in its own data centre in Luxembourg.
- EU rules, notably the General Data Protection Regulation (GDPR) and the ePrivacy Directive, provide the strongest safeguards of trustworthiness (e.g. voluntary approach, data minimisation).
- The apps – as well as the gateway – are time-limited, that means they will only be in place as long as the pandemic persists.
- The European Data Protection Board was consulted on the draft guidance and issued a letter to welcome the Commission's initiative to develop a pan-European and coordinated approach.

Will personal data be shared between Member States through the gateway?

The Commission developed with Member States a privacy preserving interoperability protocol. If an app from one Member State is to work in another Member State, some encrypted data will be shared with the server of that other Member State. All backend servers are under the control of the competent national authority. Each app must be fully compliant with the EU data protection and privacy rules, following the Commission's guidance.

5. App usage information

How will we know that tracing apps are working?

Member States are monitoring and evaluating the apps and their contribution to the fight against the pandemic. The Commission, with the European Centre for Disease Prevention and Control, is assisting Member States to identify a series of assessment criteria to evaluate the effectiveness of the apps. Some of those criteria could include, for example, the uptake of the app as a percentage of population and number of users notified of potential exposure.

Currently, download rates range from below 10% to above 40%, depending on the Member State. But even at low uptake, apps can make a difference, according to researchers – and each notification is a life potentially saved.

What are the minimum device requirements?

All coronavirus tracing and warning apps should be accessible to everybody. They can be used on the vast majority of devices with commonly used operating systems. The required update to the relevant operating system (iOS, Android) is usually carried out automatically on smartphones. The apps run on iOS smartphones from the iPhone 6s upwards using iOS 13.5, and on Android-based smartphones from Android 6 upwards. If the result of your COVID-19 test is verified via QR code, the camera on your phone must be functional.

What role do Apple and Google play?

Almost all, that is 99% of smartphones in the EU, run on iOS or Android mobile operating systems. In the context of the development of contact tracing and warning

apps, Apple and Google provided a uniform standard for Bluetooth distance measurement. This was important so apps running on the two main operating systems would be able to register each other's Bluetooth signal. Furthermore, the companies needed to ensure that the Bluetooth signal continues to operate passively in the background in battery-saving mode, even if the apps is not actively used. National apps based on a 'decentralised' architecture rely on this basic functionality – these are interoperable and can be linked to the gateway.