SQUIRE PATTON BOGGS

Local Connections. Global Influence.

An Overview of the EU and National Guidance and Approaches to Contact Tracing Apps With a Focus on Data Protection Issues

Introduction

From the outset, it has been clear that data can play a major role in dealing with a pandemic like COVID-19. Partly that is because China, where the government has unparalleled ability to access information about the whereabouts and activities of citizens, was first to have to tackle a major outbreak of the virus. It is also partly because the ability to collect and analyse information about the propagation of the virus is vital to being able to bring the pandemic under control.

As European countries now consider that the virus is sufficiently subdued that governments can start to re-open social activities and unlock their economies, the ability to identify possible new outbreaks and deal with them rapidly is fundamental for preventing a "second spike". Therefore, attention has turned to how apps can help to enable such "test and trace" strategies. No app is ever going to be able to do this on its own, partly because no government would consider it politically proportionate to make the use of apps mandatory across the whole population (though some use of apps in specific circumstances – e.g. isolation – has been made mandatory in some countries), and partly because governments know that even if they tried to make an app mandatory, it never would be, and some of those who would not use it are likely to be among the most vulnerable in society.

However, there is acceptance that apps, if adopted by a large enough proportion of people, can play a positive role in complementing test and trace systems. But here governments face a dilemma – the more they use apps to collect data, the less people may be willing to use the apps. Conversely, the less usable data a government gets from the app, the smaller the contribution it will make to controlling the spread of the virus. It is no surprise that this dilemma has led governments to different conclusions, reflecting national attitudes towards healthcare systems, privacy, technology, etc.

This note on the EU guidance on how the apps should be implemented in the EU and what a number of European countries are doing helps to illustrate both the challenge and the potential. How much difference apps will actually make to managing the re-opening is up for debate. But there seems little doubt that the role of data in managing a pandemic is here to stay.

Contact Tracing Apps

In considering methods to relax the COVID-19 lockdown measures and revive the economy while at the same time containing the spread of the virus, the EU and national EU governments have been actively pursuing the development and use of contact tracing apps. Essentially, contact tracing apps alert everyone who has been in contact with someone who has tested positive for coronavirus, so that they can take the appropriate measures (e.g. quarantine, testing, etc.).

To be effective, any contact tracing app would require the majority of the population to use it. There are reservations about the overall benefit of such an app as a means of responding to the COVID-19 crisis (among others because it may lead to false positives or negatives, the technology may be unable to distinguish between people in crowded places, as well as because of the possible abuse of the data).

The EU Commission, the European Data Protection Supervisor ("EDPS") and the European Data Protection Board ("EDPB") have issued guidance on the use of contact tracing apps in the EU (hereinafter "EU guidance"). The objective of the EU guidance is to promote the interoperability of the apps across all EU member states, including allowing the detection of proximity encounters between users of different contact tracing apps and harmonize the application of the GDPR.

In parallel, EU Member States and the UK have started devising measures at national level to further the development and adoption of contact tracing apps.

This note aims to provide an overview of the EU guidance and of EU Member States and UK developments.

To this end, the section on the European approach to contact tracing apps is divided into four sub-sections:

- The first one describes the recommended features of a contact tracing app, the possible solutions vis-à-vis the storage of the data and the proposed Google/Apple application programming interfacing solutions. It then summarises the Guidelines on interoperability issued by the eHealth Network on 13 May.
- The second sub-section describes the legal grounds for processing personal data collected via the contact tracing app.
- The third sub-section outlines the suggested retention time for any personal data collected.
- The last sub-section explains how proximity data differs and interacts with location data collected by telecom providers.

The section on National Efforts provides a summary of the EU Member State initiatives undertaken to date to manage COVID-19, covering six EU Member States (Czech Republic, France, Germany, Poland, Slovakia and Spain) and the UK.

European approach to contact tracing apps

Developments in relation to a contact tracing app have been fast moving.

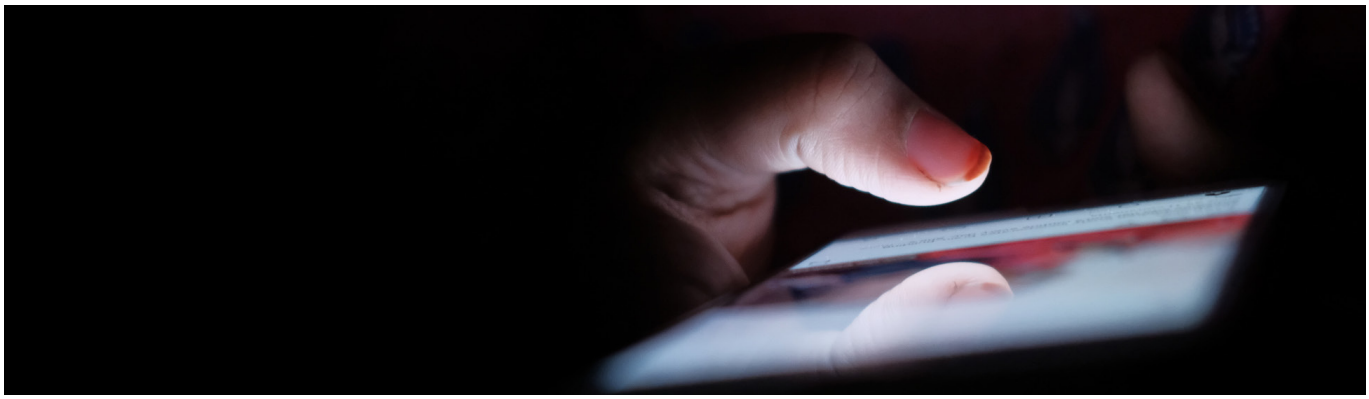
On 8 April 2020, the EU Commission issued a recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data (Recommendation).

On 15 April, the EU Member States represented in the eHealth Network (a voluntary network of Member States' competent authorities dealing with digital health) with the support of the EU Commission published detailed guidance for the development of a common approach across the EU, to use digital means to address COVID-19 (Toolbox).

On 21 April, the EDPB issued guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (hereinafter "the EDPB Guidelines").

On 11 May, the EDPS published guidelines entitled "TechDispatch #1/2020: Contact tracing with mobile applications" (TechDispatch), which covers data protection implications of contact tracing apps.

On 13 May, the e-health Network published guidelines on the interoperability for the approved contact tracing apps (Interoperability Guidelines) which aim to enable the use of the apps across the borders in the EU.



Recommended general features, storage, Google/Apple proposed application programming interfacing solutions and interoperability

According to the Toolbox, contact tracing should be carried out by measuring proximity data via Bluetooth Low Energy. Contact tracing by collecting location data is not recommended: "*Location data is not necessary nor recommended for the purpose of contact tracing apps, as their goal is not to follow the movements of individuals or to enforce prescriptions*."

In relation to proximity data, a user's device should emit and record random identifiers of other devices that it is in close proximity with, by exchanging a "digital handshake". When a user is diagnosed with COVID-19, which is confirmed by the public health authorities, they send a message via the app to confirm that they are infected. In response, the app should send a warning/alert to holders of identifiers who have been in close proximity to the infected person. The installation of the contact tracing app should be voluntary and consent for the activation of the app by users will need to be fully informed.

On 10 April, Apple and Google announced they would be launching "*a comprehensive solution that includes application programming interfaces (APIs) and operating system-level technology to assist in enabling contact tracing […] in May, both companies will release APIs that enable interoperability between Android and iOS devices using apps from public health authorities. These official apps will be available for users to download via their respective app stores.*" The contact tracing solution is not itself a contact tracing app, and Google and Apple are not yet proposing to build such an app, although they have indicated that they intend to develop more functionality into their solution. For now, the aim is to enable third parties, such as public health authorities ("PHAs"), to create contact tracing apps that exchange information via Bluetooth Low Energy between devices.

According to the Interoperability Guidelines, the Member States are to "guarantee" the interoperability of contact tracing apps. The key considerations set out to ensure interoperability include the following:

(a) Proximity detection should take place via Bluetooth;

(b) The distance, duration and time of exposure to an infected person (which will trigger the alert to people within a distance) should be determined by competent authorities responsible for the app; and

(c) Communication to the users should be in their own native language.

The information on contacts may be stored on a central server or using a decentralised protocol. The first option allows the proximity or location data recorded on a user's phone to be uploaded to the server of competent PHAs. Matches and alerts sent to users at risk take place and come from a central server held by PHAs. The second option is where the proximity data are recorded and stored on the users' devices in a so-called "decentralised" protocol. All users' phones periodically query the backend server if their identifiers have been in contact with devices of those who were positively diagnosed in the given region. If there is a match, the user receives a notification. The main difference from the centralised database is that the matches are carried out and stored on the users' devices and this information is not shared with the server.

There are concerns[1] that the use of central servers may tempt governments or bad actors to use the data collected for other purposes, including mass surveillance. The EDPS Guidelines recommend that collected information resides on the terminal equipment of the user and only relevant information is collected. This approach is also reflected in the Toolbox. EU guidance highlights that the purposes of the use of the app must exclude the use of the data collected for purposes other than the management of the COVID-19 crisis, such as commercial or law enforcement (para 10(1) of the Recommendation and p. 26 of the Guidelines).

The data controller and the lawful bases for processing

According to the Toolbox and EDPB Guidelines, the PHAs of each Member State should act as the controllers of the data collected by the app (p. 20 of the Toolbox and para 25 of the Guidelines). They may engage service providers to act on their behalf, for example, to design or to deploy the app. The EDPB Guidelines state that where there may be a number of organisations involved in the provision of a contact tracing app "their roles and responsibilities must be clearly established from the outset and explained to the users" (para 25 of the Guidelines).

The EU Commission, the EDPS and the EDPB recommend that contact tracing apps be used on a voluntary basis. There are specific processing activities, which are recommended to be voluntary, as follows:

(a) Voluntary installation of the app by a user;

(b) Voluntary upload of pseudo-random identifiers to the server by a user upon confirmed diagnosis with COVID-19; and

(c) Consent to receive direct communications and advice from public health authorities, where this is a feature of the app.

1 Around 300 scientists and researchers signed a "Joint Statement on Contact Tracing: Date 19 April 2020" urging not to store data on centralised databases for the purposes of contact tracing apps due to concerns of creating a tool that will enable large scale collection of invasive information on the population either now or at a later time.

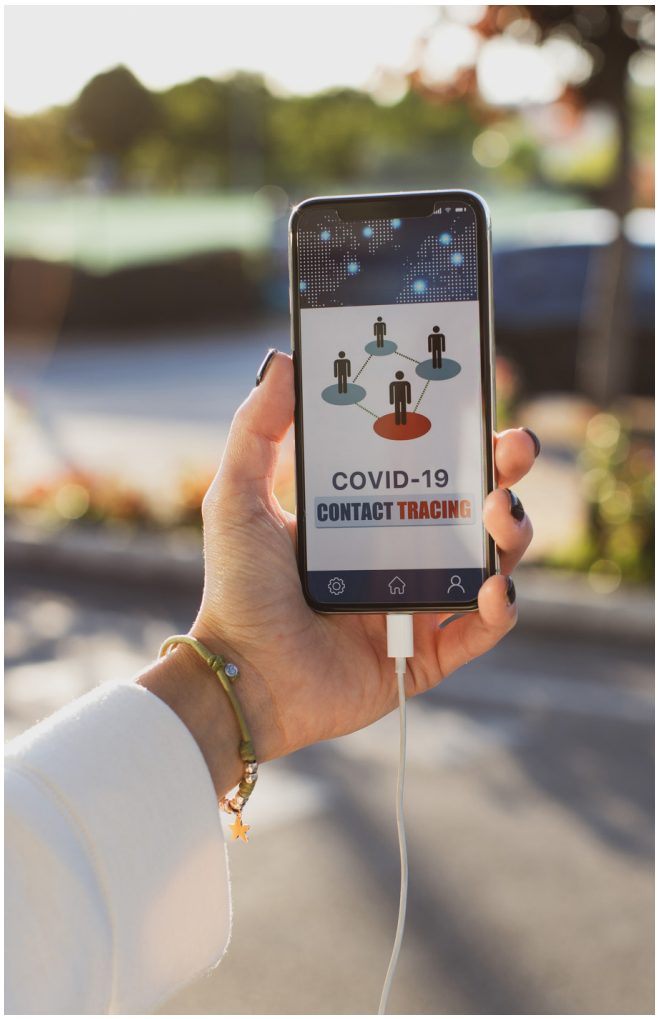
Controllers must ensure they comply with their obligation under the GDPR to determine the lawful basis for the processing of personal data collected via the app. In the EDPB's opinion, "the mere fact that the use of contact tracing applications takes place on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent" (para 29 of the Guidelines). PHAs that are assigned to collect the personal data may rely on the lawful basis that processing is necessary for the performance of a task in the public interest, based on EU Member State law under Article 6(1)(e). When it comes to processing health data via the app the EDPB has referred to the following as possible lawful bases (para 33 of the Guidelines):

(a) Article 9(2)(a) – explicit consent;

(b) Article 9(2)(i)- the processing necessary for reasons of public interests in the area of public health; and

(c) Article 9(2)(h)- on the processing necessary for health care purposes.

The EDPB also highlighted the requirements of Article 5(3) of the EU Directive on Privacy of Electronic Communications (2002/58/EC) (e-Privacy Directive), in relation to any information stored or accessed on the user's device. The user's consent will be required, unless the storage or access to information on the user's device is strictly necessary to provide a service explicitly requested by the user (para 28 of the Guidelines).



What is the shut off plan?

The EDPB recommends that the legal basis or the legislative measure relied on for the processing of personal data collected via the contact tracing app should include the criteria for determining when the use of the app should be stopped (para 31 of the Guidelines). The Toolbox calls for automated self-dismantling including deletion of all personal data and proximity information as soon as the crisis is over (p. 19).

Location data vs proximity data

According to the guidance in the Toolbox, "*Collecting an individual's movements in the context of contact tracing apps would violate the principle of data minimisation and would create major security and privacy issues*" (p. 19 of the Toolbox). The EDPB's position on the use of location data is the same[2]. Accordingly, contact tracing apps are recommended not to collect location data.

If contact tracing apps collect location data, in addition to personal data, the GDPR and ePrivacy requirements have to be met. The e-Privacy Directive permits processing of location data if it is anonymised or with informed prior consent of subscribers or users (these requirements have been implemented in the national EU Member State law). Member States and the UK have started to use anonymised and aggregated location data provided by telecom operators to study how the movements of people take place and map it with the spread of the virus, so that they can better understand how the movements impact the virus spread[3].

Article 15 of the e-Privacy Directive allows Member States to introduce restrictions to the rights and obligations in relation to location data to safeguard public security, provided such restrictions constitute "*a necessary and proportionate measure in a democratic society*". Several EU Member States have introduced new emergency laws permitting the collection of location data for public security purposes. For example, such data is used to visualise locations where individuals have spent significant time over a period of several days, in order to help trace the infection.

2 The EDPB letter concerning the European Commssion's draft Guidance on apps supporting the fight against the COVID-19 pandemic, 14 April 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

3 Vodafone, *Correct use of telco data can help in this crisis*, 27 March 2020,

National Efforts

The EDPS recently stated[4] that the GDPR was drafted with emergencies in mind and is fit for purpose (including Article 9 of the GDPR). Recital 46 of the GDPR specifically states, "*Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters*." The application of the GDPR is now being tested, but no matter what approach is adopted on the national level, there will be scrutiny of the initiatives in the EU Member States from the EU compliance perspective.

Please see below a summary of national initiatives on deploying contact tracing apps to manage the pandemic.

4 "Virtual Discussion: How Will COVID-19 Shape the Future of European Privacy Policy?", Information Technology Industry Council (ITI), 15 April 2020, https://m.youtube.com/watch?v=R4AELxbJQxY

Czech Republic

What are the current/planned measures involving a contact tracing app?

The Czech Republic has launched a consensual tracking system called "Smart Quarantine". The monitoring system uses data from mobile phones and payment cards of people who have tested positive to help them identify all the people they met that could be potentially infected.

The solution was developed by the non-governmental group of computer experts (Covid19cz group), who coordinate the system for the state. The location data is accessible to and used by the Regional Hygiene Stations. The Ministry of Health has issued an extraordinary decree ordering mobile operators to provide location data of mobile phone users and banks to provide the time and location data of the use of electronic means of payment.

Procedure

- A person who has tested positive for COVID-19 is contacted by the Regional Hygiene Station to identify all their contacts in the last 5 days.
- The person is also asked to participate in the smart quarantine system.
- Upon the individual giving their explicit consent, mobile operators and banks provide location data and the system creates a "commemorative map" of the places where the infected person was moving.
- The Regional Hygiene Station and the infected person identify all potentially endangered contacts.
- These people are contacted by a specially built call centre, informed about their potential infection and isolated in the quarantine.
- Subsequently (after 4-5 days), these quarantined people are visited by a sampling team to collect the sample and ensure the result is known in the fastest possible time (ideally within 48 hours).

In addition, a mobile app Mapy.cz (map portal) can be used as a part of the Smart Quarantine system. It can notify the user who has enabled geolocation data in case he is at increased risk of being infected with COVID-19 because of significant personal contact with a person who has tested positive.

Besides the Smart Quarantine system, the same developers have also introduced a mobile app "eRouška" (eMask, or in full, electronic facemask). Thanks to Bluetooth technology, the application remembers other app users that happened to be nearby (including unknown people such as co-commuters in a bus). When asked by the staff of the Regional Hygiene Station for an overview of people the infected person has met in recent days, they can- in one click- send an anonymous list of eMask users they were in risky contact with.

Data protection perspective

In early April, the Czech Office for Personal Data Protection ("ÚOOÚ") published two statements regarding the system of Smart Quarantine. It follows from the statement, that this project, which raises significant privacy concerns was not yet properly consulted with the Office.

In the statements, the ÚOOÚ has highlighted that the processing of personal data for the purpose of combating or preventing the pandemic must be adequate, effective, and limited in time. The emergency measure provides for the retention of personal data only for as long as it is necessary and, in the case of non-anonymised data, not more than six hours.

The ÚOOÚ noted that it is up to each controller (including mobile operators or banks) to define and perform the processing of behavioural data as required by the Ministry or the Regional Hygiene Station. According to the ÚOOÚ, the lawful basis for such processing carried out by private data controllers (banks or mobile operators) is fulfilment of the task performed in the public interest (Article 6(1)(e) of the GDPR).

The controller responsible for the entire processing of personal data of the Smart Quarantine system is the Ministry of Health.

The emergency measure provides for the retention of personal data only for as long as it is necessary and, in the case of non-anonymised data, not more than six hours.

France

What are the current/planned measures involving a contact tracing app?

On June 2, 2020, the French government rolled out its contact-tracing app "StopCovid" which alerts app users of exposure to COVID-19. A useful online guide, which introduces the features of the app and shares various opinions and reviews, including those of the CNIL's, is also available.

The app was developed by a group of companies and institutions, including the National Research Institute for Digital Science and Technology ("INRIA"), the French National Institute of Health and Medical Research (Inserm), the National Cybersecurity Agency of France ("ANSSI") and the National Health Agency (Santé Publique France), as well as a number of private companies listed on the INRIA website.

The app was conceptualised by researchers from the Pan-European Privacy Preserving Proximity Tracing (PEPP-PT) with German, Italian and Swiss teams. It is based on a protocol called "ROBERT", which stands for ROBust and privacy-presERving proximity Tracing. ANSSI has published a number of technical recommendations including that data should be encrypted.

App users must grant permanent access to the Bluetooth function to be able to use the StopCovid app as it relies on a Bluetooth Low Energy signal and does not search the location of the users. It uses a centralised approach meaning that a central server generates the crypto-identifiers assigned to users and then collects the crypto-identifiers of people who have been in "close" contact with another user (less than one meter for more than 15 minutes). The information about "contacts" is retained for 15 days.

If an individual tests positive for COVID-19, the lab that performed the tests will provide the user with a code that it can register on the app voluntarily and an instant message will be sent to any other user of the app whose smartphone has been in "close contact" with that individual's smartphone in the past two weeks. Message recipients will be advised to self-isolate, be tested and/or take other precautionary measures. The information about infection of a user is deleted immediately after the "contacts" have been notified.

The identity of the individual diagnosed with the virus will not be disclosed. It will not be possible either for a user to access the list of persons that he/she was in close contact with.

The Ministry of Health will act as data controller.

The use of the app will be voluntary. Based on the CNIL's recommendations, refusal or uninstalling of the app should not have any adverse consequences for the data subject in particular for access to tests and healthcare, but also for access to public transport, etc.

The app will be phased out six months after the end of the declaration of a health emergency.

The app was implemented by a vote of Parliament on 27 May 2020 and enacted by decree on 29 May 2020 . This decree notably specifies that data subjects cannot exercise the right of access or rectification nor the right to limitation of the processing (as we understand it this is due to the technical specifications of the app).

The CNIL had issued a preliminary opinion in April 2020. It issued a new opinion on 25 May, following live testing of the app.

The CNIL recognises that, as presented, the app complies with data protection by design. It made several recommendations in this new opinion, including: providing clear information to users, including on methods for erasing sensitive personal data; providing specific information for minors and parents; confirmation in the upcoming decree of a right to object and a right to erasure of pseudonymised data; and free access to the app's source code and server. It had also recommended that the efficiency of this app be monitored.

The CNIL also advised that the most appropriate basis for processing is Article 6(1)(e) GDPR processing necessary for the purpose of a task carried out in the public interest and, as regards health data, Article 9(2)(i) processing necessary for reasons of public interest in the area of public health.

Germany

What are the current/planned measures involving a contact tracing app?

The German Federal Government has conceived a decentralised model for the Corona App ("CA").

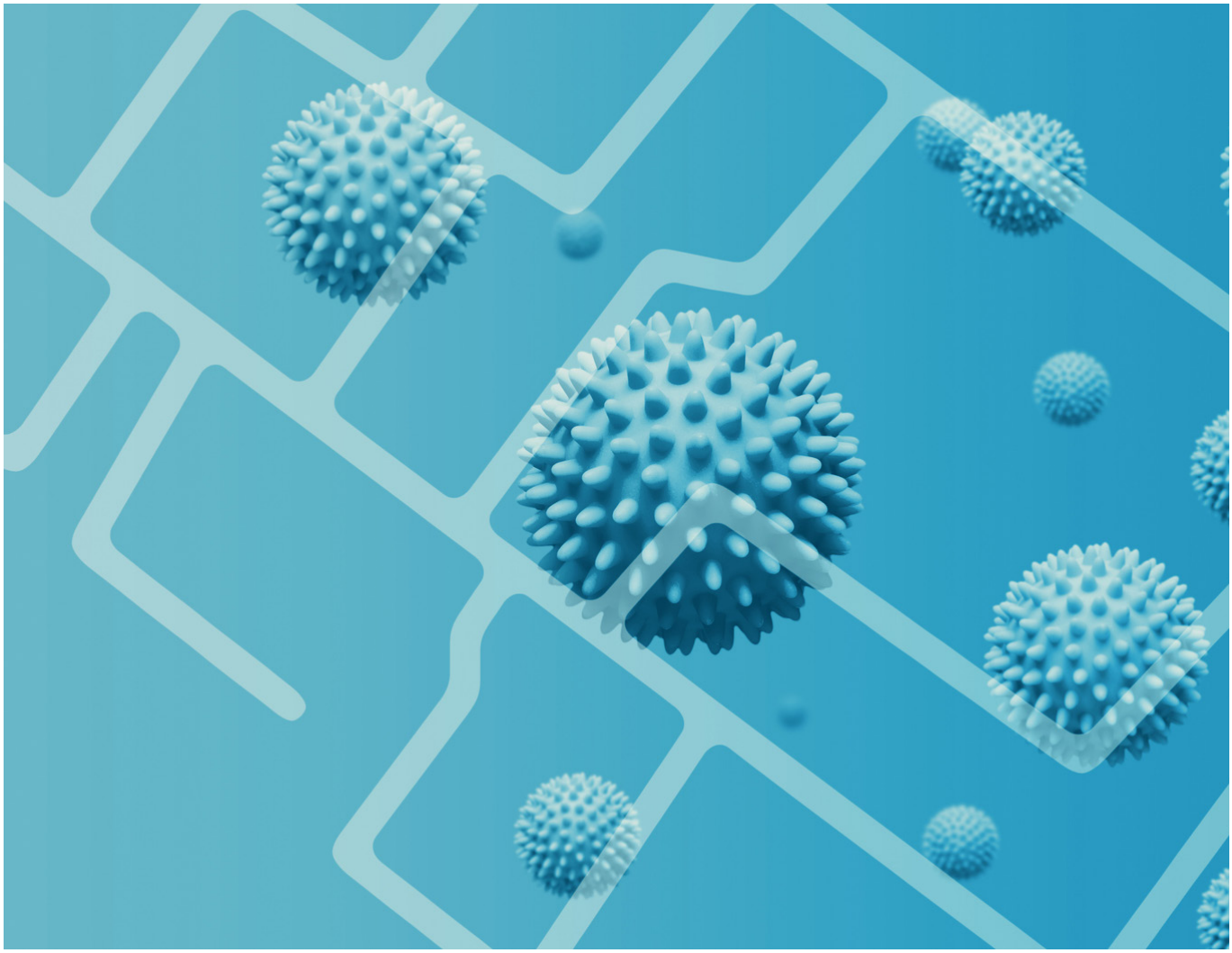
The Federal Government does not plan to process personal data, including location data.

Consent or opt-out? In order to keep the intervention in the right to informational self-determination and the integrity of the information technology systems as low as possible, the Federal Government plans to base the use of the CA on consent. Critics are calling for an opt-out solution to ensure that 40 to 50 million Germans use the CA. According to experts, this number is necessary to prevent the spread of the virus. Therefore, every smartphone user should receive a tracing CA on their mobile phone with the next smartphone update and anonymously decide whether they wish to participate, or deny permission for comprehensible reasons. Proponents of the consent solution argue that one must first check whether acceptance can be achieved with consent. If this is not the case, it should be possible to switch to an opt-out solution if necessary.

False events. Critics of the CA stress that there is a high risk of falsely registered events (false positives) that result in unjustly imposed isolation (for example, contact measurements through the wall between two apartments). To counter this, legal and factual controls are needed, such as recalling false infection reports, deleting wrongly registered contact events with an infected person and restrictions imposed because of data processing. None of the proposed systems provide for such a possibility so far.

Additional Data Donation App of the RKI. In addition to the CA, the Federal German scientific institution in the field of biomedicine, the Robert Koch Institute ("RKI") has developed an app that enables users to donate data; the so called 'data donation app' (*Datenspende-App*, "DAA"). The DAA is already available and is used for COVID-19 research purposes. Every DAA user is pseudonymised with a user ID. A Smart Watch transmits health data to the RKI. Anonymisation does not help, as it does not allow a correct assignment and interpretation of data. RKI stresses that the DAA is not a virus test, but only processes COVID-19-like symptoms, e.g. increased resting pulse as an indication of fever. The CA can be used with consent but currently not all providers are compatible with the CA, e.g. the CA does not work on Samsung and Huawei Smartphones.

The Federal Government's latest plan is to include RKI's DAA as an additional function into the Federal Government's CA.



Poland

What are the current/planned measures involving a contact tracing app?

"**Home Quarantine App**" is a mandatory app, developed by the Polish Ministry of Digital Affairs, to be downloaded and used by all of those placed under mandatory quarantine.

The mandatory 14-day quarantine applies to healthy individuals who have been in contact with patients who are infected or suspected of coronavirus infection. Everyone who enters Poland from abroad also falls thereunder.

The app is mandatory for all people placed under obligatory quarantine or epidemiological surveillance, as per article 7e.1 of the Act on Special Solutions toward Preventing, Counteracting and Combating COVID-19 and other Infectious Diseases and Related Crises.

The main purpose of the app is to facilitate and streamline compulsory quarantine at home. It was also intended as a tool to check whether quarantine rules are violated, for example whether the ban on leaving home is observed.

The app allows a person covered by the quarantine restrictions to confirm their location and to conduct a basic health self-assessment. It also grants them immediate access to the necessary quarantine information as well as contact details of the local social welfare institutions. The app has access to the GPS and the camera on the user's mobile phone.

A person placed under a mandatory quarantine (e.g. upon crossing the border), fills in a localisation form, indicating the location, where he/she declares to be quarantined along with his/her phone number. This data is then uploaded to the system and subsequently onto the application. Once the data is uploaded, the individual concerned receives a text message notifying them that they are obliged to download and use the application. Upon arrival at the quarantine location, the individual downloads and activates the app and uploads the so called "reference selfie".

From that moment on, the quarantined individual starts to receive throughout the day "tasks" to complete, such as e.g. taking a selfie in the quarantined location within a set period of time (e.g. 20 minutes) and confirming the location (the app does not track the location 24/7 but merely while completing the given task by the user). If the individual fails to complete the task within the set timeframe, the authorities will send the police to check if the individual remains at the declared quarantine location. However, the use of the app does not exclude the possibility of regular police check-ups being carried out in parallel.

The app uses geolocation (from the phone GPS) and facial recognition system. According to the privacy notice, the Ministry of Digital Affairs shall be the data controller. The controller will process the personal data, encompassing Citizen ID, name, surname, telephone number, declared location address, likeness, geolocation, end date of the quarantine for a period of six years.

This six year period (which is the standard statute of limitation for claims under the civil code, but seems rather excessive in this case), starts from the date the app is deactivated (i.e. after the lapse of 14 days of mandatory quarantine). The pictures however are said to be deleted immediately after the app is deactivated.

Those with sight impairments (the blind or visually impaired) are exempt from the obligation to use the Home Quarantine app. So too are the people who have made a statement to the competent services that they are not subscribers or users of the telecommunications network or do not have a mobile device enabling the installation of the application. The declaration is made under pain of criminal liability.

According to the Ministry of Digital Affairs, the app has been designated in accordance with the guidelines of the EDPB, the European Commission and in accordance with the EC's eHealth Network Toolbox.

For purposes of compliance with the GDPR, the General Sanitary Inspectorate is the data controller.

Telecommunication operator's obligation to provide end user's anonymised location data:

Since not everyone has a mobile device on which the above apps could be downloaded (i.e. the elderly) and not everyone who is under the mandatory quarantine downloads the Home Quarantine app, the Act on Special Solutions toward Preventing, Counteracting and Combating COVID-19 and other Infectious Diseases and Related Crises (in Art. 11 f) imposes obligations on the telecommunication operators.

These obligations are to provide the Minister of Digital Affairs, upon request, with anonymised location data, from the last 14 days, from the telecommunications device of an end user who is a COVID-19 sufferer or who is subject to quarantine.

The data should be used solely to counteract the spread of the COVID-19 pandemic; the difference is that as opposed to the Home Quarantine app – the Ministry of Digital Affairs can request that the telecommunications operator provide the location data of ANY citizen – even one who has not been placed under mandatory quarantine. Consent of the end user to processing and providing the data shall not be required. This obligation shall apply only during the state of epidemic hazard, the state of epidemic or the state of natural disaster, in order to counteract COVID-19.

ProteGO Safe App: on 21 April, the General Sanitary Inspectorate recommended on its website the use of the ProteGo Safe application, which allows it to control and curb the spread of the SARS-CoV-2 and COVID-19 disease.

The app is available for download here.

The application, which is voluntary, has been built by the open source community under the auspices of the Ministry of Digital Affairs (govTech Polska), and allows its users to:

- Self-monitor their health condition by filling in the so called "Risk Assessment Test" and the Health Diary (which can be easily provided to medical staff during a health check-up);
- Receive personalised recommendations as regards further steps to be taken, based on the answers given in the Risk Assessment Test;
- Receive notifications encouraging regular completion of Risk Assessment Survey and other preventative behaviours.

Upon the completion of the self-assessment, the app will check which of the three risk groups the user falls under:

- Low (observe expert recommendations and rules of hygiene, stay safe and monitor your health condition);
- Medium (stay at home, observe expert recommendations and rules of hygiene, stay safe and monitor your health condition); or
- High (immediately contact a health specialist).

In addition, the app has been recently supplemented with a module using Bluetooth technology, which allows it to collect information about the devices the user has encountered and inform about contact with persons infected with COVID-19, so it will be easier to track those who have potentially encountered the infected user.

This processed personal data is not disclosed to anyone in a form that would allow user identification. The Inspectorate shall not have access to the information and personal data uploaded onto the app and it shall not undertake any active measures in order to identify the user. It shall also refrain from analysing how the user is using the app. The data are saved only on the user's device and are not exported externally. No one else – other than the users themselves – shall have access to the data.

Information entered into the app, in connection with the COVID-19 infection self-assessment shall be anonymised and sent to the entity that provides that functionality, however, that entity shall not be able to identify the user either (as the data is being disclosed to third parties in a format that prevents user identification).

The personal data collected from the user shall not be processed for longer than the use of the application and no longer than it is absolutely necessary by the provisions of law. Once the user ceases to use the app, his personal data (such as user device ID, name, health data, gender, age, information regarding smoking addiction, and other data that the user voluntarily provides to the Health Diary) shall be deleted (erased) along with the app.

Slovakia

What are the current/planned measures involving a contact tracing app?

On 15 May, the Slovak National Council adopted a new amendment introducing two mobile applications (the "Amendment").

The first app is intended to monitor compliance with a mandatory quarantine (the "Quarantine App") and the second one should monitor infected persons' contacts with the other devices (the "Preventing App"). According to the Amendment's Explanatory Memorandum, the monitoring services are divided into two separate mobile apps due to both iOS' and Android's policies. The apps were developed for the Slovak Public Health Office.

The Quarantine App allows people returning to Slovakia from abroad to stay in a home quarantine rather than in dedicated quarantine premises. Use of the Quarantine App is entirely voluntary and any user monitored explicitly agrees to their location and their biometric data being exchanged. If a user disagrees, they will be isolated in the State's quarantine premises (various hotels, dormitories etc.).

Persons using the Quarantine App are obliged to:

- Install and use the Quarantine App and turn on the Quarantine App's notifications and automatic updates and checks;
- Allow access to location data in order to monitor their device's location;
- Allow facial recognition via their camera.
- Prevent any activities which may eventually lead to the Quarantine App's malfunction.

The Quarantine App will also have access to the photographs of each user's face, saved into the device during the quarantine. The photographs will not be sent to a third party or any public authorities, and will only be stored on the user's device.

The Quarantine App's functionalities are as follows:

- User's registration in order to monitor compliance with ordered quarantine;
- Monitoring user's compliance with ordered quarantine based on location data and health status monitoring; all data shall be deleted after 30 days;
- Notify the particular Regional Public Health Offices on the location of the home quarantine;
- Monitoring contacts with other devices that have installed the Preventing App, and subsequently notifying a user about possible contact with an infected person, if such infected person agreed to this, all related data shall be deleted in 30 days after origination;
- Providing general information regarding collection and displaying anonymous statistics and maps to persons who may be concerned.

The Public Health Office will not require any data from telecommunications operators, as it does not have the jurisdiction for such requests. Furthermore, any cooperation between the Public Health Office and telecommunications operators is strictly forbidden.

The Public Health Office shall only collect and process the following data obtained from the Quarantine App and Preventing App, in order to operate the Apps:

- User's name and surname, date of birth, e-mail address, telephone number, facial image and health status in connection with COVID-19;
- Unique identifiers generated via the Apps;
- The location of a home quarantine, as well as further information related to the ordered isolation;
- The location of the mobile device;
- Information regarding potential contact with other users, the intensity and duration of contact between other users via Bluetooth (the Preventing App).

The Public Health Office may also process the data for statistic or research purposes.

Use of both Apps will be monitored by the Public Health Office in order to identify whether their use is still necessary. The operation of the Apps and the processing of data will continue only until December 31, 2020, at the latest. All data shall be deleted after that except for any data stored for the purposes of admin or assessing the infringement of judicial proceedings.

Both apps are currently being tested, with further details, including rollout dates, expected to be announced.

Spain

What are the current/planned measures involving a contact tracing app?

In Spain, no contact tracing app has been developed yet. The Secretary of State for Digitization and Artificial Intelligence is assessing the Spanish position in light of how other European countries develop their respective contact tracing apps.

According to the Spanish Government, their app will be designated in accordance with the guidelines of the EDPB, based on a non-centralised system (Bluetooth), supported by the DP-3T initiative and for voluntary use. The data controller will be the Ministry of Health.

Both the Spanish Government and Spanish Data Protection Agency are waiting to see the first results from other contact tracing apps such as the one developed by the German Government. This is to inform their ability to give maximum protection to citizens without violating their right to privacy as outlined in Article 18 of the Spanish Constitution.

In addition, Autonomous Communities such as Catalonia are developing their own contact tracing app, although they are not yet available.

Under Ministerial Order SND / 297/2020 of March 27, the Ministry of Health ordered the development of two analysis tools:

"Asistencia COVID-19"

The objective of this app, which was developed by the Secretary of State for Digitization and Artificial Intelligence, is to decongest the health care telephones of the different Autonomous Communities.

The tool allows users to self-diagnose, access action recommendations and updated information, and receive reminders to periodically monitor health status.

The official application will allow for unified and homogeneous data, thereby contributing to the management of the epidemic at the national level.

The Spanish Government guarantees the general protection and security of the population data that is collected through its use.

Telefónica Digital Spain, SLU, will carry out the execution of activities that will allow the implementation and deployment of the app.

"DataCOVID-19"

This tool studies and applies citizens' mobility in relation to the COVID-19 crisis. This tool is focused on linking and combining data from mobile operators, in an aggregated and anonymised way, with the aim of analysing the mobility of people prior to and during confinement.

The data controller is the National Statistics Institute (Instituto Nacional de Estadística). The data processors will be the operators of mobile electronic communications, once an agreement is reached.

The National Statistics Institute, as data controller, authorises the operators to resort to other managers in the execution of the provisions.

UK

What are the current/planned measures involving a contact tracing app?

The NHSX, the digital transformation arm of the National Health Service ("NHS"), intends to make the contact tracing app voluntary in the UK. The app would rely on Bluetooth Low Energy signal. If an individual tests positive for COVID-19, the user can voluntarily provide that information to the NHS via the app and an instant message will be sent to anyone who has been in close contact with that individual, advising them to self-isolate, get tested and/or take other precautionary measures. The identity of the individual diagnosed with the virus will not be disclosed. The app is based on a centralised system where a central server is used for storage and processing. The Health Secretary has stated that the NHS will not store the health data for longer than necessary.

There have been reports of the government using aggregated and anonymised location data provided by telecom providers to manage the virus. The Information Commissioner's Office ("ICO")'s view on this was "*Generalised location data trend analysis is helping to tackle the coronavirus crisis. Where this data is properly anonymised and aggregated, it does not fall under data protection law because no individual is identified.*"

The ICO has been providing advice to the government about the application of data protection laws to the contact tracing app. The ICO's general stance is that: "*the data protection laws do not get in the way of innovative use of data in a public health emergency – as long as the principles of the law (transparency, fairness and proportionality) are applied. The same approach applies to the use of contact tracing applications*". The ICO recommends carrying out a data protection impact assessment for the contract tracing app prior to implementation, with regular reviews.

On 29 April 2020, a Joint Statement was issued by over 150 scientists and researchers in the UK in the field of information security and privacy urging the NHSX against centralised storage, which "would enable (via mission creep) a form of surveillance".

The app has not yet been launched, but is in the advanced stages of development. Tests of a pre-release version of the software went live on the Isle of Wight on 5 May 2020. The app was originally due to be rolled out nationwide in mid-May, but the government now says it will be ready in June.

Separately to the app rollout, on 28 May 2020, the NHS launched its Test and Trace service, involving 25,000 contact tracing staff making calls to those with coronavirus symptoms, to manually track the spread of COVID-19.

Contacts

EU

Rosa Barcelo
Partner, Brussels
Co-Chair Data Privacy & Cybersecurity Practice
T +322 627 1107
E rosa.barcelo@squirepb.com

Czech Republic

Petra Věžníková
Associate, Prague
T +420 221 662 242
E petra.veznikova@squirepb.com

France

Stephanie Faber
Of Counsel, Paris
T +33 1 5383 7400
E stephanie.faber@squirepb.com

Germany

Marina Langhofer
Associate, Berlin
T +49 30 72616 8137
E marina.langerhofer@squirepb.com

Poland

Magdalena Gad-Nowak
Senior Associate, Warsaw
T +48 22 395 5565
E magdalena.gad-nowak@squirepb.com

Slovakia

Silvia Belovičová
Partner, Bratislava
T +421 2 5930 3426
E silvia.belovicova@squirepb.com

Spain

Rosa Barcelo
Partner, Brussels

Irene Fernández
Junior, Madrid
T +34 91 426 4840
E irene.fernandez@squirepb.com

UK

Asel Ibraimova
Associate, London
T +44 207 655 1208
E asel.ibraimova@squirepb.com

Matthew Kirk
International Affairs Advisor, London
T +44 207 655 1389
E matthew.kirk@squirepb.com

SQUIRE PATTON BOGGS

squirepattonboggs.com