NORTON ROSE FULBRIGHT

Contact tracing apps in Turkey

A new world for data privacy

As of January 21, 2021

The COVID-19 pandemic has seen governments across the world restricting civil liberties and movement to new levels. To aid the safe lifting of current public health restrictions, new technologies are being developed – contact tracing apps – and rolled out to automate labour intensive tasks critical to containing the spread of the virus. Our contact tracing survey summarises the principal regulatory and policy issues applicable to contact tracing across a range of key jurisdictions in real time.

Is technology being used by the government to monitor and control the spread of COVID-19 (e.g. contact tracing app, CCTV, cell phone location data, credit-card history)?

In collaboration with the Information Technologies and Communication Authority and all mobile phone operators, the Turkish Ministry of Health has launched a mobile contact tracing app called "Hayat Eve Sığar" (Life Fits Into Home) to monitor the movement of diagnosed COVID-19 patients and to warn users if they enter a high COVID-19 risk zone or if they had crossed paths with a diagnosed patient. Diagnosed COVID-19 patients are warned via text messages and automated calls in the event that they leave their place of isolation. A recently added feature to the app now allows users to scan barcodes at selected venues (e.g. participating shops, stores, etc.) to review detailed information such as the number of people who have recently visited that location.

What are considered to be the major privacy concerns in relation to the app in your jurisdiction (in relation to its use (a) by the government; and (b) by private sector organisations)?

The app is not being used by private sector organisations and to the best of our knowledge, there have been no surveys or polls to test public opinion on the app or any privacy concerns around it. However the major privacy concerns in relation to an app of this type would be the risk of a cyber attack and exfiltration of personal data (including sensitive health data) and whether established data processing principles would be duly complied with, including purpose limitation and time limitation.

App details

1. What is the name of app

Hayat Eve Sığar

2. Is the app voluntary?

No

While initial government guidance and news coverage indicated that the app's use by individuals diagnosed with COVID-19 was going to be mandatory, practical constraints (e.g. persons without access to necessary technology to use the app or persons who, despite having access, are nonetheless unwilling or unable to make use of the app) have limited the enforcement of such guidance. Obtaining HES codes (for details, please see the answer to question 3 below) for inter-city travels using mass transportation, however, is compulsory, and the app remains one of the most convenient ways to obtain said codes.

In addition to inter-city travels, HES codes have also become compulsory in a number of cities, including in Istanbul, in order to use mass transportation to travel within the city. Cities are able to enforce this rule by ensuring that smart "city cards," which are loaded with cash value or passes to pay public transportation fares, are paired with their users' unique HES codes.

Recently, some government buildings, including many in Istanbul (the country's most populous city) have been requiring HES codes from citizens wishing to enter.

3. Is there any suggestion that use of the app and a clean result may be necessary to enter workplaces or any commercial or public buildings (or is this explicitly or implicitly prohibited)?

Yes

A new COVID-19 measure has been introduced in Turkey for all domestic travel by plane, train or bus.

By checking the code on a platform provided by the Ministry of Health, the service provider - for example, an airline company - will check if a passenger is fit to travel. If the passenger has been exposed to the virus or has been in contact with any infected person, he/she will be denied access to boarding. Additionally, if a passenger who has been on a flight/train is subsequently diagnosed with COVID-19, other passengers on the same flight/train will be tracked via their HES code.

HES code can be obtained through the "Hayat Eve Sığar" app, or by sending a text message and providing the following information: the Turkish ID number; the last four digits of the serial number on the Turkish ID card; and the number of days for which the HES code should remain valid.

We note that different airline operators have different requirements as to the duration of the HES code validity.

4. What information is required to register for the app? Is the information collected considered excessive?

Yes

User's phone number is authenticated at the registration stage. User receives a text message with a code and authenticates his/her phone number using that code in the app.

According to the app's privacy notice, users can use a limited version of the app if they do not share a Turkish ID number, father's name and date of birth information (which are requested to authenticate the user's identity). If the user does not wish to provide his/her Turkish ID number, the user must nevertheless type in his/her age for the app to calculate COVID-19 risk exposure.

5. Is GPS or Bluetooth used?

Bluetooth

6. Is data stored on a centralised server?

Unsure

This information is not publicly available.

7. Does the identity of the infected user get captured centrally?

Yes

The Ministry of Health is informed of the identity of infected persons in any case after their diagnosis and therefore, has knowledge of the identity of the infected users.

8. Is the identity of the infected user disclosed to proximate users or public health authorities? Is it disclosed to anyone else?

Not disclosed to proximate users; but may be disclosed to the Ministry of Internal Affairs and law enforcement officers

If the infected user leaves his/her place of isolation and does not return despite the warning, his/her identity, contact information and location are shared with the Ministry of Internal Affairs and law enforcement officers alerted to protect public health and prevent the spread of COVID-19.

9. Is consent needed to share data with other users/ upload the data to a centralised system?

Yes

A user can track another user's location and risk exposure data if they consent to sharing such data. The invitation to share data is sent via the app.

10. Is the identity of the proximate users disclosed to public health authorities? Is it disclosed to anyone else?

Yes

The app will notify the users who have been in contact with an infected user. The Ministry of Health is the data controller and therefore has knowledge of the identity of the proximate users.

11. Does the app incorporate "privacy by design" and was a privacy risk assessment completed?

Unknown

This information is not publicly available.

12. How long will the data be kept for, are there clear lines around timing?

Unknown

The privacy notice does not clearly address these issues. According to the privacy notice, user data processing will be "limited to the pandemic combat period". According to the Presidency of the Republic of Turkey's Directorate of Communications' press release dated April 9, 2020, the data will be deleted once the pandemic risk is over.

13. Has data security been addressed expressly (e.g. encryption)?

Unknown

14. Are there clear limitations regarding who may have access to the data?

Yes

The Ministry of Health has access to the data as the data controller and can share it with the Ministry of Internal Affairs and law enforcement officers. Users can share data with other users if they wish to do so.

15. Are there clear limitations on the purposes for which the government may use the data?

Yes

According to the privacy notice, the purposes of data processing is "the protection of public health; preventative medicine; medical diagnosis; carrying out treatment and nursing services; planning and management of healthcare services and financing thereof". The privacy notice further specifically refers to the applicable personal data protection legislation which allows health data to be processed by persons or authorized institutions under confidentiality obligation without obtaining explicit consent from the data subject for the aforementioned purposes.

In case an infected user leaves his/her place of isolation, the Ministry of Health, as the data controller, may share such user's identity, contact information and location data with the Ministry of Internal Affairs and law enforcement officers for the purposes of public health protection and prevention of the spread of COVID-19.

16. Is the government of your country bound by privacy laws in respect of the contact tracing data?

Yes

As a general rule, the government is bound by Turkish personal data privacy laws. However, there are a small number of exceptions where privacy laws do not apply (e.g. where personal data is processed by legally authorized public authorities as part of preventive, protective and intelligence operations to safeguard public security and public order).

That said, the Ministry of Health nevertheless issued a privacy notice for the app and informed users regarding the data controller; purposes of data processing; grounds for, and recipients of, personal data transfer; grounds for, and method of, data collection; and the rights of the users under privacy laws.

17. Has the regulator commented/ provided guidance on the technology?

Yes

Turkish Data Protection Authority ("DPA") did not comment on the technology directly but in its public announcement dated April 9, 2020, the DPA mentioned that location data processing by public authorities due to the pandemic may fall under a statutory exception where data privacy laws do not apply:

"In cases where location data need to be used by relating to a natural person;

The provisions of Law does not apply in cases where personal data are processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorised and assigned by law to maintain national defence, national security, public security and order or economic security, pursuant to subparagraph (ç) of Article 28(1) of Law No. 6698.

Based on this, in cases that threaten public order and safety such as a pandemic, data processing measures by authorized public offices to ensure isolation of diagnosed individuals to naturalize any risk while they are still contagious, to determine crowded areas by processing the location data of the general public, and to develop preventative measures accordingly are all considered to fall within the scope of Article 28(1)(ç) of the [Data Privacy] Law.

In this context, there is no obstacle to the processing of location data by the competent institutions and organizations which fall under the scope of the mentioned article, in order to prevent the spread of the disease caused by COVID-19 that threatens public security and public order."

On the other hand, considering that grave harms may result during the processing of location data of persons, if such data are stolen by third parties, it should not be forgotten that relevant public authorities are to take all technical and administrative measures to ensure the safety of personal data and to erase and destroy said data, if and when the conditions necessitating the processing of data no longer exist.

18. Are there any private sector initiatives you are aware of to use/ integrate the app or the information from the app (e.g. to reflect the results back to workforces)?

Yes

Please see the answer to question 3 above.

Contacts

Ekin Inal
Partner, İnal Kama Attorney Partnership, associated with Norton Rose Fulbright in Turkey
Istanbul
Tel +90 212 386 1317
ekin.inal@inalkama.com

Chris Cwalina
Global Co-Head of Data Protection, Privacy and Cybersecurity
Washington DC
Tel +1 202 662 4691
chris.cwalina@nortonrosefulbright.com

Marcus Evans
Head of Data Protection, Privacy and Cybersecurity, Europe
London
Tel +44 20 7444 3959
marcus.evans@nortonrosefulbright.com

Ffion Flockhart
Global Co-Head of Data Protection, Privacy and Cybersecurity
London
Tel +44 20 7444 2545
ffion.flockhart@nortonrosefulbright.com

Anna Gamvros
Head of Data Protection, Privacy and Cybersecurity, Asia
Hong Kong SAR
Tel +852 3405 2428
anna.gamvros@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

Law around the world

nortonrosefulbright.com