Contact tracing apps in Poland

A new world for data privacy

As of May 11, 2020

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)?

The Polish Government has launched two apps ("Kwarantanna domowa" app and "ProteGO Safe Safe" app).

The “Kwarantanna domowa” application is intended for people who are subject to 14-day mandatory house quarantine due to suspected COVID-19 exposure. The application uses geolocation and face recognition technology to ensure that relevant people are quarantined.

The “ProteGO Safe Safe” application is designed to allow users to monitor their level of risk of getting infected. The app facilitates self-assessment of the risk of COVID-19 infection and, if the user decides to do so, it allows the user to scan the environment for other smartphones on which the application is installed and saves the history of anonymous identifiers encountered.

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)?

“Kwarantana domowa” – It is unclear what methods have been used to protect personal data collected by the application and there may be a risk of data leakage. Due to concerns that the use of the “Kwarantanna domowa” application violates users’ rights to personal data protection, the Polish Ombudsman has asked the President of the Office for Personal Data Protection for an opinion on this matter.

“ProteGO Safe” – There are three main concerns indicated by Panoptykon, a Polish NGO:

- risk of de-anonymisation and reconstruction of the map of social links;
- threat to the safety of users (Bluetooth constantly on); and
- the risks associated with automatic decision making, which can have significant consequences for people using the application.
**App details**

1. **What is the name of app**
   
   **Kwarantanna domowa and ProteGO Safe**

2. **Is the app voluntary?**
   
   **Yes and No**
   
   The "Kwarantanna domowa" is mandatory. However, people with a visual impairment (blind or partially sighted) and those who have declared to the relevant service that they are not subscribers or users of the telecommunications network or do not have a mobile device to install this software are exempt from this obligation.

   The "ProteGO Safe" app is voluntary.

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)?**

   **No**

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

   **No**
   
   The "Kwarantanna domowa" collects the following data: citizen ID - technical identifier of citizen, first name, surname, phone number, declared residence address, photo, location of citizen and end date of quarantine.

   The "ProteGO Safe" can be used anonymously. However it is necessary to confirm the authenticity of the person who wants to send data from the device.

   In both cases, the scope of information collected by the application is not considered excessive.

5. **Is GPS or Bluetooth used?**

   "Kwarantanna domowa" uses GPS.

   "ProteGO Safe" uses Bluetooth.

6. **Is data stored on a centralised server?**

   **Yes**
   
   "Kwarantanna Domowa" app  
   Hybrid Solution - "ProteGO Safe" app

   **Kwarantanna domowa" – The data are stored on centralised servers.

   "ProteGO Safe" – The data is stored only on user devices and are not transmitted to any central server, but the key operations for the application take place on the central server.

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

   **No**

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

   **No**
   
   The identity of the quarantined person is disclosed to authorities in case of "Kwarantanna domowa", even though they have not been diagnosed with COVID-19.

   "ProteGO Safe” users will be informed if they have been in direct contact with person that has been diagnosed with COVID-19 (but without disclosing that person's identity).

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

   **No – “Kwarantanna Domowa”**

   **Yes – “ProteGO Safe”**

   "Kwarantanna domowa" – consent is not needed to upload data to a centralized system.

   "ProteGO Safe" – consent is needed to share data with other users.

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

    **No**

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

    **Unclear**

    There is no public information as to the degree of privacy risk assessment carried out.

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

    "Kwarantanna domowa” – The data will be kept for 6 years, except for images which are deleted when the user deactivates the account.

    "ProteGO Safe” – The Application deletes the data collected on the device after 2 weeks from the day it was saved in the Application or at any time upon request of the user.

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

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

Yes

“Kwarantanna domowa” – access to the data processed in the application and the system is provided to: Police Headquarters, Provincial Police Headquarters, voivodes, Central IT Centre (supports the application system), Take Task S.A. (company supporting the application from the technical side), Centre of Health Information Systems.

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

Yes

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

No

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

Yes

The Polish Government websites have provided information on both applications.

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)?

No
Contacts

Agnieszka Braciszewska  
Counsel  
Warsaw  
Tel +48 22 581 4900  
agnieszka.braciszewska@nortonrosefulbright.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  
fion.flockhart@nortonrosefulbright.com

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