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 Government has selected a contact-tracing app developed by a well-known software house. On 29 April the Italian Government issued a law decree setting out inter alia the rules governing the adoption of such app (Law Decree no. 28 of 30 April 2020, the Decree).

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 Data Privacy Authority considers that the Decree on the app complies with its previous comments on this topic and with EDPB guidelines.

Main privacy concerns lie in data minimization, data security, and actual prevention of use of such data for other purposes. The Decree addresses a wide-spread concern about ownership and localization, providing that the data controller shall be the Ministry of Health, and that data shall be stored in servers on the Italian territory.

Private sector apps to be used in the workplace will need to comply with strict Italian rules on remote monitoring of employees, as well.

<table>
<thead>
<tr>
<th>App details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What is the name of app</td>
</tr>
<tr>
<td>2. Is the app voluntary?</td>
</tr>
<tr>
<td>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)?</td>
</tr>
<tr>
<td>4. What information is required to register for the app? Is the information collected considered excessive?</td>
</tr>
</tbody>
</table>

The Decree prescribes that not using the app cannot lead to any adverse consequence, but no further details are provided.

Final details about the app are not available yet. The Decree sets the principle according to which the app shall process only the scope of data necessary to alert proximate users of contacts with infected users and easing the adoption of health assistance measures in their favour.
5. Is GPS or Bluetooth used?
   Bluetooth
   Use of localization data is prohibited under the Decree.

6. Is data stored on a centralised server?
   Yes

7. Does the identity of the infected user get captured centrally?
   Unknown
   Final details about the app are not available yet.

8. Is the identity of the infected user disclosed to proximate users or public health authorities?
   Is it disclosed to anyone else?
   Unknown
   Final details about the app are not available yet. It is envisaged that proximate users will be alerted of the fact of having had contact with an infected user, which in theory should not need disclosure of the infected user’s identity to other users. Data will be processed by public health authorities.

9. Is consent needed to share data with other users/ upload the data to a centralised system?
   Unknown
   Final details about the app are not available yet. Data will be processed by public health authorities.

10. Is the identity of the proximate users disclosed to public health authorities? Is it disclosed to anyone else?
    Unknown
    Media reports suggest that consent will be required, but this is not clearly stated in the Decree, which just confirms that installing the app shall be voluntary.

11. Does the app incorporate “privacy by design” and was a privacy risk assessment completed?
    No
    It is not known what kind of “privacy by design” analysis has been conducted in the development of the app. However, the Decree provides for a data processing impact assessment to be carried out.

12. How long will the data be kept for, are there clear lines around timing?
    End of year
    At the moment, data is intended to be retained until the end of the state of emergency and in any case not later than 31 December 2020.

13. Has data security been addressed expressly (e.g. encryption)?
    Yes
    In general terms, the Decree requires a ‘suitable level of security” to be adopted. Anonymization or (if not possible) pseudonymization is required.

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

15. Are there clear limitations on the purposes for which the government may use the data?
    Yes
    Data collected through the app can only be used for alerting persons that entered into close contact with persons that tested positive to coronavirus and protect their health (except for further use of aggregate or anonymised data for other purposes of public health, prevention, statistics or scientific research).

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

17. Has the regulator commented/ provided guidance on the technology?
    Yes
    The Italian Data Processing Authority has been heard in the Parliament and has issued an opinion on the Decree.

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
    Media reports suggest tests are being carried out by some Italian companies for using such an app at the workplace (e.g. in automotive manufacturing plants).
Contacts

Pietro Altomani
Senior Associate
Milan
Tel +39 03 86359 476
pietro.altomani@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
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