Contact tracing apps in The Netherlands
A new world for data privacy
As of July 13, 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 Dutch Government is currently investigating whether a contact tracing app should be launched. In this context, the Dutch Government asked the public to submit proposals. Approximately 700 proposals were submitted. Subsequently, the Government selected seven apps that were further presented during an "appathon" held on 18 and 19 April. Following this "appathon", the Government decided that none of the apps met the requirements, inter alia under privacy legislation.

Therefore, the Government is working with various experts to develop an app. Currently, there are uncertainties surrounding the contact tracing app and it is even unclear whether the app will be launched at all (the app is currently being tested). The Government aims to decide mid-July whether to launch the app nationally. Nevertheless, some aspects of the framework have already been confirmed, which are indicted below.

Furthermore, the Government had published a draft bill which amends the Dutch Telecommunication Act (Telecommunicatiewet) and allows the National Institute for Health and Environment (Rijksinstituut voor Volksgezondheid en Milieu) (RIVM) to access telecommunication data (the aggregated location and traffic data of citizens) through the Dutch Central Bureau of Statistics (Centraal Bureau voor de Statistiek) for the purpose of controlling the spread of COVID-19. The Dutch Data Protection Authority (the DDPA) had reviewed the previous version of the draft bill and identified a number of areas that require improvement: (i) given that the bill was drafted with great urgency, its scope should be limited to the COVID-19 crisis alone (it allowed RIVM to access data for future epidemics as well); (ii) the purpose and necessity of the extended powers of the RIVM needed to be stated clearly; and (iii) no maximum retention period for the telecommunication data was included. The Government had considered the comments from the DDPA and published a revised draft bill on May 29, 2020. The DDPA is currently advising the Government on the draft bill, but it has already commented it does not agree with the draft bill in its current form. According to the DDPA, the data is not unconditionally anonymised, the purpose and necessary of the bill need to be stated more clearly and the safeguards proposed by the DDPA are insufficiently implemented into the new draft bill.

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)?

There are still unaddressed privacy concerns regarding the implementation of the contact tracing app. Although the DDPA did not yet provide any comments on the app that is currently being developed by the Government, it stated earlier regarding the use of contact tracing apps that it is unclear whether such apps are necessary and effective in combatting COVID-19. This clarity is required in order to justify the extensive intrusiveness that the contact tracing app will have on the fundamental right of privacy.

Furthermore, the purpose(s) of the app needs to be more clear, as well as the legal grounds to justify processing the data, including special categories of personal data (i.e. health data) regarding which more stringent requirements apply under the General Data Protection Regulation (GDPR). It needs to be more clear which (governmental) organisations will use the app and who the data controller is in respect of the personal data.
This is important as the data controller will be responsible for complying with the GDPR and will be the point of contact for data subjects in order to receive information on the data processing and to enforce their data subject rights under the GDPR. Given that the app is currently under development, it is unclear whether appropriate technical and organisational measures (e.g. pseudonymisation) will be implemented to ensure that the personal data is sufficiently protected. It should also be noted that there is a risk that the app will be used on an ongoing basis (i.e. after the crisis has ended). Pursuant to the GDPR, the app should in any case be a temporary measure.

**App details**

1. **What is the name of app**
   - CoronaMelder

2. **Is the app voluntary?**
   - Yes

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)?**
   - Unknown
   
   Given that use of the app will be voluntary, it is unlikely that the use of the app will be necessary to enter workplaces or any commercial or public buildings.

4. **What information is required to register for the app? Is the information collected considered excessive?**
   
   The Government indicates on its website that no personal data will need to be submitted in order to use the app and that the app does not collect any personal data itself. The app solely collects and shares anonymised codes that are updated frequently (every 15 minutes). It remains to be seen whether this is sufficient to avoid the processing of any personal data under the GDPR.

5. **Is GPS or Bluetooth used?**
   - Unknown
   
   The contact tracing app will make use of Bluetooth Low Energy.

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

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?**
   
   The Government indicates on its website that the identity of the infected user will not be disclosed to the proximate users (they will only receive a notification that they were in close proximity of an infected user, indicating solely the date on which the contact took place). Given that, according to the Government, the identity of users will not be captured (as no personal data will be processed), the identity will most likely also not be disclosed to others (such as public health authorities).

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

10. **Is the identity of the proximate users disclosed to public health authorities? Is it disclosed to anyone else?**
    
    Given that, according to the Government, the identity of users will not be captured (as no personal data will be processed), it is unlikely that public health authorities will receive the identity of the proximate users.

11. **Does the app incorporate "privacy by design" and was a privacy risk assessment completed?**
    
    Unknown
    
    This will be required under the GDPR. The Government indicates on its website that it will conduct a protection impact assessment (PIA) and discuss it with the Authority.

12. **How long will the data be kept for, are there clear lines around timing?**
    
    The data (i.e. anonymised codes of the user and the proximate users) will be stored in the app for 14 days. It is unknown how long the data will be stored in the centralised server.

13. **Has data security been addressed expressly (e.g. encryption)?**
    
    Unknown
    
    Although this is currently unknown, the Government does indicate that the app will need to comply with the applicable security and privacy standards. Experts in these areas are therefore closely involved in the development of the app.

14. **Are there clear limitations regarding who may have access to the data?**
    
    Unknown
15. Are there clear limitations on the purposes for which the government may use the data?

Unknown

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 DDPA is closely involved in the development of a potential contact tracing app. The DDPA commented on the seven apps that were further presented during the “appathon.” The DDPA investigated whether the apps met the requirements under GDPR. According to the DDPA, it was not provided with sufficient information to make this assessment and it therefore advised against implementing these apps. In its decision, the DDPA lists its main focus areas.

These include:

a. the necessity of the app,
b. the purpose of the app and the legal processing ground to justify the processing of the data,
c. the data processor and
d. the security of the app. Please also see our response above.

Going forward, the DDPA will continue to be involved in the development of the app. The DDPA has not yet commented on the app that is currently being developed by the Government.

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