SNAPSHOT

The latest updates from the team at FTI Consulting

Giving you insight to what is on the political agenda

Is Europe ready to harness the power of apps in the fight against COVID-19

April 2020

Both the general and specialist media have been awash with coverage of the use of contact tracing apps to fight COVID-19. In this snapshot we set out the key questions around whether apps should be among the tools used to bring Europe out of lockdown. We provide an overview of the current EU position on regulating the way in which data is collected, who has access to it, and in particular the extent to which COVID-19 contact tracing apps can comply within the stringent privacy rules of the General Data Protection Regulation (**GDPR**), EU's umbrella data protection legislation.

Why are contact tracing apps seen as key tool in the COVID-19 fight?

A sound public health strategy to respond to COVID-19 requires a number of core elements:

- Curbing transmission, which in most countries has been done through social distancing;
- Isolation of infected persons, and shielding for those most at risk;
- Ensuring healthcare system capacity and resilience, mainly by mapping numbers of those affected and the availability of staff, medicines and medical materials; and
- Scientific research to cure the disease.

All these elements demand the use of data to support adherence to social distancing, to track infection spread, to assess availability of beds and care resources, and to fuel epidemiological studies and clinical trials. The demand for data has given rise to a range of smartphone apps with various functionalities. These have become as contact tracing apps. The most common are symptom checker functionalities that enable public health authorities to guide citizens on self-isolation, testing, seeking healthcare, and contact tracing as well as warning functionalities to identify those who have been in contact with an infected individual to inform them about self-quarantine and testing. In all cases data collected through the apps can be complemented with anonymised location data obtained from the telecom operators.

Petra Wilson, *Senior Advisor in the Healthcare Team at FTI Consulting Brussels and a member of the WHO Digital Health Technical Advisory Group;* ***Ana Jankov****, Director in the TMT Team at FTI Consulting Brussels*

Is anonymised location data the best way forward?

At the outset of the pandemic, the use of location data obtained from telecom operators was widely encouraged. One of the loudest proponents of the collection of location data was Thierry Breton, European Commissioner for Internal Market and Services, who urged telecom operators throughout the continent to share anonymised location data with governments and with the EU Commission.

This seemed like a quick fix at first, since anonymised data (i.e. data from which all personally identifiable information has been removed) is outside the realm of data protection legislation and its processing does not entail the bureaucracy

and safeguards mandatory for the processing of personal data[1].

However, there have been concerns that location data cannot be fully anonymised - the Dutch privacy regulator has claimed that full anonymisation is not possible, on the basis that knowing where someone lives or works and combining that data with the 'anonymised' location data, can be used in combination to link the datasets.

On a practical level, public health professionals have also raised concerns about the extent to which anonymised location data can help address the public health needs. While location data is useful for enforcing quarantine measures, and to some extent for predicting disease hotspots by mapping the concentration of people, anonymised location data is otherwise not useful for the substantial needs of the public health systems.

Can smartphone apps respect privacy?

If anonymised location data is not sufficient to meet public health needs, should Governments encourage the use of smartphone apps to collect non-anonymised personal data related to COVID-19?

If governments want to do this they will need to find adequate legal grounds in GDPR for this type of data collection. The European Commission[2] and the European Data Protection Board[3] have set out guidance which broadly state that apps could be used for reasons of public interest in the area of public health 'on the basis of EU or member state law which provides for adequate safeguard measures'[4]. In practice this means that EU Member States need to enact national (emergency) law. It is unlikely that any legislation at the EU level will be passed to serve as a basis for the processing of health data.

Alternatively, non-anonymised health data could be processed by health authorities on the basis of individuals' explicit consent. Although it is not technically difficult to obtain consent for the use of apps used to collect and transmit the data, the downside of consent is that it must be possible to withdraw consent at any time, which then forbids any further processing of that individual's data.

Member States will need to decide quickly which legal base they intend to use, since the advice of most data protection authorities is that starting to process health data on one basis (consent) and then switching to another basis (national emergency law, once enacted) would not be acceptable[5].

Can we get enough data to make apps useful?

For the data to be useful for public health purpose, a critical mass of users, i.e. at least 60% of a given population, need to use the app[6]. This demands that people trust in the app-facilitated data sharing system and are willing to use it. Given that mandatory app usage is very unlikely in Europe and that the first iteration of the Common EU Toolbox developed collaboratively by the e-Health Network, with the support of the European Commission, insists that the use of smartphone apps in the fight against COVID-19 must be voluntary. A number of tools are now being developed to promote the use of selected tech solutions with high privacy standards, platforms such as PEPP-PT[7], DP-3T[8] and the deployment of blockchain based solutions such as MiPASA[9] all of which have been developed in response to the COVID-19 crisis.

Can data generated through the apps be used for scientific research?

Personal health data is of great value for scientific research, aiming to eradicate the coronavirus and create a society more resilient to any future pandemic threats. Some of the questions science will aim to answer include what categories of population are especially prone to the infection, and what age groups are more likely to spread the virus (so-called 'super-spreaders').

However, using data collected for one purpose (contact tracing) for another purpose (scientific research) raises further GDPR issues. As a rule, personal data can only be processed for the purpose for which they had been initially collected. Processing for research purposes could therefore be included in the national (emergency) law, together with appropriate safeguards. In practice, however, it could well be the case that the processing for scientific purposes is not carried out under the auspices of the national health authority, which initially collected the data. It could be undertaken by a separate scientific institute, whose involvement is not known at the time that the national law was adopted. This would mean a change of the data controller, bringing with it more legal hurdles before data

[1] General Data Protection Regulation 2016/679 (GDPR), Recital 26
[2] See https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf
[3] See https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf
[4] GDPR, Art. 9(2)(i)
[5] As set out in the Opinion of the Article 29 Working Party Guidelines on consent under Regulation 2016/679, p. 23
[6] https://science.sciencemag.org/content/early/2020/04/09/science.abb6936
[7] See https://www.pepp-pt.org/
[8] See https://github.com/DP-3T/documents
[9] See https://mipasa.org/

could (if at all) be processed for research by universities and commercial enterprises.

Are we ready?

The experience of East Asia, and in particular South Korea, has demonstrated that contact tracing apps can play a huge role in monitoring the spread of infection and supporting infection control measures. Are we ready to follow that trend? While we don't have the element of compulsion to use apps seen in South Korea or their experience of living the 2015 MERS outbreak, we do have a well-developed, widely implemented and largely respected data protection regulation which can support the use of apps, and we also have a vibrant innovation community which is developing a wide range of privacy enhancing technologies to integrate into apps. As EU countries develop strategies of gradual transition out of strict lockdown, COVID-19 apps are therefore likely to play a key role, although perhaps not of the big-brother nature currently being portrayed in the popular press.

For all enquiries, please contact: BXLcorona@fticonsulting.com

FTI CONSULTING™

EXPERTS WITH IMPACT