INNOPAY

Analysis: how the EU sets out guiding principles on privacy and security for use in development of contact-tracing app

innopay.com

Comparing the Dutch Veilig Tegen Corona coalition's ten criteria against the EU Recommendation on a common toolbox for the use of technology and data to combat and exit from the COVID-19 crisis.

The development of contact-tracing applications ('apps') to combat COVID-19 is under close scrutiny. Veilig Tegen Corona (VTC), a coalition of concerned groups in the Netherlands, has published a list of ten key criteria such an app should meet. Meanwhile, on 8 April 2020, the European Commission issued its Recommendation to all Member States on creating a common European Union (EU) toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data.[1]

INNOPAY has compared the VTC's ten criteria against the EU Recommendation to analyse the extent to which the Recommendation addresses the valid concerns of the VTC coalition and other pressure groups.

Brussels, 8.4.2020
C(2020) 2296 final

COMMISSION RECOMMENDATION
of 8.4.2020

on a common Union toolbox for the use of technolygy and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data

[1] A European Recommendation is an instrument that does not possess any legal force but is negotiated and voted on by Member States and has political weight insofar as it is an instrument of indirect action aiming at preparation of legislation in Member States. It differs from a Directive only by the absence of obligatory power.

VTC's 10 criteria

- **1. ONE PURPOSE: GETTING COVID-19 UNDER CONTROL**
- **2. Based on scientific insight and proven effectiveness**
- **3. Proven reliability and based on expertise**
- **4. Usage of the application is temporary**
- **5. Not traceable to individuals**
- **6. Usage of as little data as possible**
- **7. No central storage of personal data**
- **8. Secure and abuse-resistant**
- **9. User-friendly and accessible**
- **10. Never enforced by governments or third parties**

1. One purpose: getting COVID-19 under control

This demand of the VTC coalition deals with the development and introduction of the contact-tracing app. It should have one single goal: getting the virus under control.

The Recommendation takes the same stance. Possessing of data of natural persons is subjected to Regulation (EU) 2016/679). Consideration 8 reminds us that in any case, the purposes and means of the data processing, what data are to be processed and by whom, should be clear and specific.[2] Besides that, the Recommendation describes the privacy and data protection aspects of the use of mobile applications. Particularly, one of the principles that must be observed is to "strictly limit the processing of personal data for the purposes of combating the COVID-19 crisis and ensure that the personal data are not used for any other purposes such as law enforcement or commercial purposes".[3] Furthermore, regarding the use of mobility data to inform measures and the exit strategy, it specifically indicates that "the second priority for the toolbox should be a common approach for the use of anonymised and aggregated mobility data necessary for: (1) modelling to map and predict the diffusion of the disease and the impact on needs in the health systems in Member States, such as, but not limited, to Intensive Care Units in Hospitals and Personal Protective Equipment; and (2) optimising the effectiveness of measures to contain the diffusion of the COVID-19 virus and to address its effects, including confinement (and de-confinement), and to obtain and use those data".[4] Finally, the Recommendation also expressly excludes sharing of the data with third parties.[5]

2. Based on scientific insight and proven effectiveness

Here the VTC coalition expresses the expectation that the contact-tracing app should be based on scientific results and be demonstrably effective.

Throughout the Recommendation, is it clear that this is paramount for the European Commission too. One of the principles of the toolbox is the preference to opt for the least intrusive yet most effective measures. Besides that, Member States are strongly encouraged to exchange best practices on the use of mobility data, share and compare modelling and predictions of the diffusion of the virus, and monitor the impact of measures to limit its diffusion.[6]

3. Proven reliability and based on expertise

This third point is an extension of the second one and states that the application should be developed based on expertise and its reliability should be proven.

The Recommendation states that the toolbox should be shared with the European Union's international partners to exchange best practices and help address the spread of the virus worldwide. The principles with regard to the mobile warning and prevention application should also take into account technical requirements concerning appropriate technologies to ensure secure and reliable device proximity, encryption, data security, storage of data on the mobile device, possible access by health authorities and data storage.[7]

[2] Article 6(1)(c) or (e) and Article 9(2)(i) of Regulation (EU) 2016/679).
[3] Article 16(1) Commission Recommendation (EU) 2020/4/8.
[4] Article 18 Commission Recommendation (EU) 2020/4/8.
[5] Article 20(6) Commission Recommendation (EU) 2020/4/8.
[6] Articles 16(2) and 19 Commission Recommendation (EU) 2020/4/8.
[7] Articles 12 and 16(3) Commission Recommendation (EU) 2020/4/8.

4. Usage of the application is temporary

The VTC collation calls for the app to be purely intended as a temporary solution.

This is expressly covered by the Recommendation insofar as the principles for the contact-tracing application cover the expiration of measures taken and the deletion of personal data obtained through these measures when the pandemic is declared to be under control at the latest, and that the deletion of data should in principle take place after a period of 90 days or when the pandemic is declared under control.[8]

5. Not traceable to individuals

In order to prevent potential stigmatisation and targeted abuse, the coalition argues that it should never be possible to trace information gained from any data gathered back to an individual.

The European Commission takes the same view; no fewer than six paragraphs of the Recommendation are devoted to this topic.[9] The Recommendation not only requires anonymity, but also adds to this demand by explicitly requiring safeguards to prevent de-anonymisation and avoid reidentification of individuals, including guarantees of adequate levels of data and IT security and assessment of reidentification risks when correlating the anonymised data with other data.

6. Usage of as little data as possible

The VTC demands that as little data as possible should be required from users.

The European Commission reflects on this aspect in the considerations. Existing EU law permits data collection only in narrowly defined circumstances or on the basis of consent of the user or subscriber. Only after having been provided with clear and comprehensive information to traffic and location data, the storing of information and the gaining of access to information stored in the terminal equipment, such as a mobile device, of a user or subscriber. The EU upholds the principle of data minimisation. This is set out in consideration 25, which stipulates that public health authorities and research institutions should process personal data only where adequate, relevant and limited to what is necessary, and should apply appropriate safeguards such as pseudonymisation, aggregation, encryption and decentralisation.[10]

7. No central storage of personal data

The VTC opposes the central storage of personal data.

This is not explicitly covered by the Recommendation. The European Commission upholds the principle of data minimisation, of course, and points out the requirements of integrated data protection and privacy-by-design principles, but this does not automatically translate into the prohibition of central storage of data.[11]

8. Secure and abuse-resistant

The VTC demands data security, including adequate measures against abuse.

Consideration 17 of the Recommendation pays attention to the protection of fundamental rights and respect for private and family life. Article 16(4) instigates the guiding principle of effective cybersecurity requirements to protect the availability, authenticity, integrity and confidentiality of data to be processed in the contact-tracing app.[12]

9. User-friendly and accessible

For effective use of the application, it is essential that the user base is as wide as possible, which is why this ninth point emphasises the importance of user-friendliness and accessibility.

The Recommendation agrees that transparency and clear and regular communication are paramount to ensure public trust and that the European e-Health systems and services should work with interoperable applications, to achieve a high level of trust and security, enhance continuity of care and ensure access to safe and high-quality healthcare. Transparency requirements on the privacy settings will help to address these considerations and ensure trust in the applications.[13]

[8] Articles 16(5) and 20(5) Commission Recommendation (EU) 2020/4/8.
[9] Articles 16(2)(6) and 20(1)(2)(3)(4) Commission Recommendation (EU) 2020/4/8.
[10] Consideration 25 and article 16(2) Commission Recommendation (EU) 2020/4/8; Directive 2002/58/EC of the European Parliament and Regulation 2016/679.
[11] Consideration 25 and article 8 Commission Recommendation (EU) 2020/4/8.
[12] Consideration 17 and article 16(4) Commission Recommendation (EU) 2020/4/8.
[13] Consideration 6, 30 and article 16(7) Commission Recommendation (EU) 2020/4/8.

10. Never enforced by governments or third parties

Lastly, VTC demands that the contact-tracing application cannot be thrust upon the population by governments or third parties.

This demand is partly covered by the Recommendation in the sense that the use of the application should always require consent and the protection of natural persons with regard to the processing of personal data and the free movement of such data. Besides that, the Recommendation contains a requirement to strictly limit the processing of personal data to the purposes of combating the COVID-19 crisis and to ensure that the personal data are not used for any other purposes such as law enforcement or commercial purposes.[14]

Concluding remarks

It can be concluded that the EU Recommendation addresses many of the concerns expressed by the coalition, since it already covers nine out of the ten criteria. The Recommendation therefore serves as an excellent starting point for app developers to ensure protection of fundamental rights and freedoms, particularly the rights to privacy and protection of personal data.

It is encouraging to see how quickly the European Commission has reacted to the various market tendencies and government activities to develop mobile applications based on the use of anonymised mobility data to combat COVID-19. It is of the utmost importance to critically monitor the actions of governments and institutions and to validate every step in developing and rolling out a contact-tracing app in the battle against COVID-19. The ability to fall back on established rules to protect fundamental rights within the EU will help to ensure the security of personal data, both now and in the future.

[14] Consideration 7 and article 10(1) Commission Recommendation (EU) 2020/4/8.

Authors

Mariane ter Veen, Jim de Wolf

INNOPAY

World Trade Center F-tower
Strawinskylaan 381
1077 XX AMSTERDAM
The Netherlands
T: +31 20 65 80 651

Taunustor 1
(TaunusTurm)
60310 Frankfurt a.M.
Germany
T: +49 (0) 69 50 50 60 4350

info@innopay.com
www.innopay.com

About INNOPAY

INNOPAY is an international consultancy firm specialised in digital transactions. We help companies anywhere in the world to harness the full potential of the digital transactions era.

We do this by delivering strategy, product development and implementation support in the domain of Digital Identity, Data Sharing, Open Banking, Payments and Digital CSR. Our services capture the entire strategic and operational spectrum of our client's business, the technology they deploy, and the way they respond to local and international regulations.

We have grown from strength to strength since our foundation in 2002 and operate from our offices in Amsterdam, Frankfurt and Berlin. Our head office is located in The Netherlands, where we have the #1 market position.

We are a founding member of Holland FinTech, a financial technology hub with links to the rest of Europe, the US, the Middle East and Asia. Our team consists of over 60 experienced domain experts who regularly advise a wide range of global organisations.