European Data Protection Board

Olivier Micol

Brussels, 14 April 2020

Head of Unit European Commission
DG for Justice and Consumers
Unit C.3 – Data protection
Belgium

Ref: OUT2020-0028

Dear M. Micol,

Thank you very much for liaising and seeking the advice of the EDPB on the draft Guidance on apps supporting the fight against COVID-19 pandemic. Indeed, the EDPB has been keen to work fast on this issue by publishing a statement on March 19th and plans to issue additional guidance next week on tracing, scientific research and teleworking. Some National Supervisory Authorities are also developing guidelines at national level to advise their governments and telecoms operators on the best way to comply with data protection rules. The EDPB welcomes the Commission's initiative in developing a pan-European and coordinated approach, where mobile applications may become one of the proposed measures to empower individuals in the response to fight the pandemic. The EDPB has repeatedly stated that the implementation of data protection principles and the respect of fundamental rights and freedoms is not only a legal obligation, but also a requirement to reinforce the effectiveness of any data-based initiatives for combating the spread of the COVID-19 virus and for informing de-escalation strategies.

The EDPB is aware that no one-size-fits-all solution applies to the matter at stake, and that the available options require many factors to be considered, including the fact that individuals' health may be impacted. This is why envisaged technical solutions need to be examined in detail, on a case-by-case basis. In addition, the EDPB believes that it is a step in the right direction to highlight the essential need to consult with data protection authorities to ensure that personal data is processed lawfully, respecting the rights of the individuals, in accordance with data protection law.

The development of the apps should be made in an accountable way, documenting with a data protection impact assessment all the implemented privacy by design and privacy by default mechanisms, and the source code should be made publicly available for the widest possible scrutiny by the scientific community.

At this stage, and on the basis of the information provided by the Commission, the EDPB can only focus on the overall goal of the envisaged apps, to verify whether they are in line with data protection principles, and on the mechanisms provided for the exercise of the rights and freedoms of the population. Doing so, the EDPB believes that the Commission will draw elements for a further reflection in order to adjust, where needed, the choices represented in the document, or to explore

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

new technical options. In any case, the EDPB will investigate further this issue in its upcoming guidelines.

In this answer, the EDPB would like to address specifically the use of apps for the contact tracing and warning functionality, because this is where increased attention must be paid in order to minimise interferences with private life while still allowing data processing with the goal of preserving public health.

In the case where such applications would prove relevant in the implementation of some public health policy, they may only achieve their maximum efficiency if used by the largest possible share of the population, in a collective effort to fight the virus. Any functional heterogeneity, lack of interoperability or even individual difference in the use of the app may create negative externalities on others, resulting in a reduced sanitary effect. The EDPB strongly supports the Commission's proposal for a voluntary adoption of such apps, a choice that should be made by individuals as a token of collective responsibility. It should be pointed out that voluntary adoption is associated with individual trust, thus further illustrating the importance of data protection principles.

The EDPB notes that the mere fact that the use of the contact tracing takes place on a voluntary basis, does not mean that the processing of personal data by public authorities necessarily be based on the consent. When public authorities provide a service, based on a mandate assigned by and in line with requirements laid down in law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task for public interest. The enactment of national laws, promoting the voluntary use of the app without any negative consequence for the individuals not using it, could be a legal basis for the use of the apps. Such legislative interventions should accordingly not be intended as a means to push for compulsory adoption, and the individuals should be free to install and uninstall the app at will. These laws could be accompanied by appropriate communications activities at national level to promote such tools, with awareness-raising campaigns and assistance to minors, to the impaired, or to less skilled or educated parts of the population, in order to avoid scattered adoption, or blurred knowledge of the evolution of the epidemics and any potential health divide. Indeed, any lack of data, due to individuals' inattentive use of the app or even to battery fault of the device may seriously undermine the overall public usefulness of these instruments.

Contact tracing apps do not require location tracking of individuals users. Their goal is not to follow the movements of individuals or to enforce prescriptions. The main function of such apps is to discover events (contacts with positive persons), which are only likely and for the majority of users may not even happen, especially in the de-escalation phase. Collecting an individual's movements in the context of contact tracing apps would violate the principle of data minimisation. In addition, doing so would create major security and privacy risks.

Health authorities and scientists are well placed to identify what constitutes an event to be shared if, where and when it happens, under a strict necessity test as required by the law, and they should define some of the functional requirements of the app. Another debated issue is the storage of such events. Two main options are envisaged: local data storage within individuals' devices, or centralised

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

storage. The EDPB is of the opinion that both can be valid alternatives, provided that adequate security measures are in place, and that different entities may also be considered as controllers depending on the ultimate objective of the app (e.g. the controller and data processed may be different if the objective is to provide in-app information or to contact the person on the phone, for instance). In any case, the EDPB wants to underline that the decentralised solution is more in line with the minimisation principle.

Finally, these apps are not social platforms for spreading social alarm or giving rise to any sort of stigmatisation. In fact, they should be tools for empowering people to do their part. Quoting the draft Guidance, their sole objective is "*for public health authorities to identify the persons that have been in contact with a person infected by COVID-19 and ask him/her to self-quarantine, rapidly test them, as well as to provide advice on next steps, if relevant, including what to do if developing symptom*s". The quality of the processed data is of paramount importance in this effort. The steps that need to be taken "*to identify the persons that have been in contact with a person infected by COVID-19*" are not easy or straightforward. Informing a person, via an in-app notification, may be done in such a way that the application processes only random pseudonyms. In addition, a mechanism should ensure that whenever a person is declared as COVID-positive, the information entered in the app is correct, since this may trigger notifications to other people concerning the fact that they have been exposed. Such mechanism could be based, for instance, on a one-time code that can be scanned by the person when the result of a test is given to him/her. Every individual contact must be performed only by health authorities after assessing strong data evidence, with the least amount of inference. In addition, the role of the "*contact list of the person owning the device*", as envisaged in the Guidance, should be clarified by the Commission.

Algorithms used in contact tracing apps should work under the strict supervision of qualified personnel in order to limit the occurrence of any false positives and negatives, and by no means the task "*to provide advice on next steps*" should be fully automated. It is advisable that a call-back mechanism is put in place where the person is given a telephone number or a contact channel to get more information from a human agent. Also, in order to avoid stigmatisation, no potential identifying element of any other data subject should be part of this "*advice*", nor should the use of the app, or part of it (like dashboards, configuration settings etc.), allow the re-identification of any other persons, infected by COVID-19 or not. The EDPB strongly suggests not to store any directly identifying data in users' device and that such data be in any case deleted as soon as possible.

The EDPB strongly supports the concept in the Recommendations that once this crisis is over, such emergency system should not remain in use, and as a general rule, the collected data should be erased or anonymised.

Finally, the EDPB and its Members, in charge of advising and ensuring the correct application of the GDPR and the e-Privacy Directive, should be fully involved in the whole process of elaboration and implementation of these measures. The EDPB recalls that it intends to publish Guidelines in the upcoming days on geolocation and other tracing tools in the context of the COVID-19 out-break.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

In all circumstances, the EDPB remains available to provide further guidance to the EU institutions and to all stakeholders involved in the development and use of those mobile apps for the fight against COVID-19.

Yours sincerely,

Andrea Jelinek

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels