EUROPEAN
COMMISSION

Brussels, 16.4.2020
C(2020) 2523 final

COMMUNICATION FROM THE COMMISSION

Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection

GUIDANCE ON APPS SUPPORTING THE FIGHT AGAINST COVID 19 PANDEMIC IN RELATION TO DATA PROTECTION

1 CONTEXT

The COVID-19 pandemic has created unprecedented challenge for the Union and the Member States, their healthcare systems, way of life, economic stability and values. Digital technologies and data have a valuable role to play in combating the COVID-19 crisis. Mobile applications typically installed on smartphones (apps) can support public health authorities at national and EU level in monitoring and containing the COVID-19 pandemic and are particularly relevant in the phase of lifting containment measures. They can provide direct guidance to citizens and support contact tracing efforts. In a number of countries, both within the EU and worldwide, national or regional authorities or developers have announced the launch of apps with different functionalities aimed at supporting the fight against the virus.

On 8 April 2020, the Commission adopted a Recommendation towards a common Union 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 (the "Recommendation")[1]. The purpose of the Recommendation is, inter alia, to develop a common European approach ("Toolbox") for the use of mobile applications, coordinated at EU level, for empowering citizens to take effective social distancing measures, and for warning, preventing and contact tracing to help limit the propagation of the COVID-19 disease. The Recommendation sets out the general principles which should guide the development of such a toolbox and it indicates that the Commission will publish further guidance, including on the personal data protection and privacy implications of the use of applications in this field.

With the Joint European Roadmap towards lifting COVID-19 containment measures, the Commission, in cooperation with the President of the European Council, set out a number of principles to guide the phase-out of the containment measures due to the COVID-19 outbreak. Mobile applications, including contact tracing functionalities, can play an important role in this context. Depending on the features of the apps and the extent to which the population uses them, they can have a significant impact on disease diagnosis, treatment and management of COVID-19 inside and outside the hospital setting. They are particularly relevant when containment measures are lifted and when the risk of infection grows as more and more people are in contact with each other. These applications can help to interrupt infection chains faster and more efficiently than general containment measures, and can reduce the risk of the virus spreading significantly. They should thus be an important element

[1] Recommendation C(2020) 2296 final of 8 April 2020 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.

in the exit strategy, complementing other measures like increased testing capacities[2]. An important prerequisite for the development, acceptance and up-take of such apps by individuals is trust. People must have the certainty that compliance with fundamental rights is ensured and that the apps will be used only for the specifically defined purposes, that they will not be used for mass surveillance, and that individuals will remain in control of their data. This is the foundation for the accuracy and effectiveness of such apps in containing the spread of the virus. It is therefore essential to identify solutions that are the least intrusive and fully comply with personal data protection and privacy requirements as set out in EU law. Moreover, the apps should be deactivated at the latest when the pandemic is declared to be under control. The apps should also include state- of- the- art information security protections.

This guidance takes into account the contribution from the European Data Protection Board (EDPB)[3] and discussions within the eHealth network. The EDPB plans to publish Guidelines in the upcoming days on geolocation and other tracing tools in the context of the COVID-19 out-break.

Scope of the guidance

In order to ensure a coherent approach across the EU and provide guidance to Member States and app developers, this document sets out features and requirements which apps should meet to ensure compliance with EU privacy and personal data protection legislation, in particular the General Data Protection Regulation[4] (GDPR) and the ePrivacy Directive[5]. This guidance does not address any further conditions, including limitations that Member States might have included in their national laws with regard to processing of data concerning health.

The guidance is not legally binding. It is without prejudice to the role of the Court of Justice of the EU, which is the only institution that can give authoritative interpretation of EU law.

The present guidance addresses only voluntary apps supporting the fight against COVID 19 pandemic (apps downloaded, installed and used on a voluntary basis by individuals) with one or several of the following functionalities:

- provide accurate information to individuals about the COVID-19 pandemic;
- provide questionnaires for self-assessment and for guidance to individuals (symptom checker functionality)[6];

[2] https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.

[6] If the apps provide information related to diagnosis, prevention, monitoring, prediction or prognosis, potential qualification as medical devices according to the medical devices regulatory framework should be assessed. As

- alert persons who have been in proximity for a certain duration to an infected person, in order to provide information such as whether to self-quarantine and where to get tested (contact tracing and warning functionality);

- provide a communication forum between patients and doctors in situation of self-isolation or where further diagnosis and treatment advice is provided (increased use of telemedicine).

Under the ePrivacy Directive, imposing the use of an app involving the confidentiality of communications rights set out in Article 5 is only possible through a law which is necessary, appropriate and proportionate in order to protect certain specific objectives. Given the high degree of intrusiveness of such an approach and the challenges involved, including in terms of putting in place appropriate safeguards, the Commission is of the view that a careful analysis is required before using this option. For these reasons, the Commission recommends the use of voluntary apps.

This guidance does not cover apps aimed at enforcing quarantine requirements (including those which are mandatory).

2 CONTRIBUTION OF APPS TO THE FIGHT AGAINST COVID-19

The symptom checker functionality is a tool for public health authorities to guide citizens on testing for COVID-19, to provide information on self-isolation, on how to avoid transmission to others and when to seek healthcare. It can also complement primary care surveillance and better inform what the transmission rates of COVID-19 are in the population.

Contact tracing and warning functionalities are tools to identify the persons that have been in contact with a person infected by COVID-19 and to inform him/her about appropriate next steps, such as self-quarantine, testing or providing advice on what to do in case of symptoms n. This functionality is therefore useful both for individuals and public health authorities. It can also play an important role in managing containment measures during de-escalation scenarios. Its impact can be boosted by a strategy supporting wider testing of persons showing mild symptoms.

Both functionalities may also be a relevant source of data for public health authorities and facilitate the transmission of such data to national epidemiological authorities and to the European Centre for Disease Prevention and Control (ECDC). This would help understand transmission patterns and, if combined with testing results, estimate the positive predictive value of respiratory symptoms in a given community and provide information on the level of virus circulation.

---

regards said framework, see Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p. 1) and Regulation (EU) 2017/745 of the European Parliament and the Council of 5 April 2017 on medical devices (OJ L 117, 5.5.2017, p. 1).

The degree of reliability of estimates is directly linked to the number and reliability of data transmitted.

Therefore, in combination with appropriate testing strategies, both symptoms checker and contact tracing functionalities can provide information on the level of virus circulation, and help to assess the impact of physical distancing and confinement measures. As set out in the Recommendation, in order to enable cross-border collaboration and to ensure contact detection between users of different apps (which is particularly important in cross border movements of citizens) interoperability between the IT solutions of different Member States should be ensured. Where an infected person is in contact with a user of an app of another Member State, cross-border transmission of personal data of that user to health authorities of its Member State should be possible to the extent strictly necessary. Work on this issue will take place as part of the toolbox announced by the Recommendation. Interoperability should be ensured both by means of technical requirements and by improving the communication and cooperation between national health authorities. A model of particular cooperation[7] could also be used as a governance model for contact tracing apps during the COVID-19 pandemic.

3 ELEMENTS FOR A TRUSTFUL AND ACCOUNTABLE USE OF APPS

The functionalities included in the apps can have different impact on a wide range of rights enshrined in the Charter of Fundamental Rights of the EU, such as human dignity, respect for private and family life, protection of personal data, the freedom of movement, non-discrimination, freedom to conduct a business, and freedom of assembly and of association. The interference with privacy and the right to protection of personal data may be particularly significant given that some of the functionalities are based on a data-intensive model.

The elements presented below aim to provide guidance on how to limit the intrusiveness of the app functionalities in order to ensure compliance with the EU personal data protection and privacy legislation.

3.1 National health authorities (or entities carrying out tasks in the public interest in the field of health) as data controller

The identification of who is deciding on the means and purposes of the data processing (the data controller) is crucial in order to establish who is responsible for compliance with the EU personal data protection rules, and in particular: who should provide information to the individuals who download the app about what is going to happen with their personal data (already existing or to be generated through the device, such as a smartphone, on which the app is being installed), what their rights will be, who will be responsible in the case of data breach, etc.

[7] Such cooperation already takes place as regards the project MyHealth@EU for exchange of patient summaries and ePrescriptions. See also art. 5(5) and recital 17 of Commission Implementing Decision 2019/1765.

Given the sensitivity of the personal data at hand and the purpose of data processing described below, the Commission is of the view that the apps should be designed in such a manner that the national health authorities (or entities carrying out task in the public interest in the field of health) are the controllers[8]. The controllers are responsible for the compliance with the GDPR (accountability principle). The scope of such access should be limited based on the principles described in section 3.5 below.

This will also contribute to higher trust among the population and therefore acceptance of the apps (and underlying infection transmission chains information systems) and will ensure that they fulfil the intended purpose of protecting public health. The underlying policies, requirements and controls should be aligned and implemented in a coordinated way by the responsible national health authorities.

3.2 Ensuring that the individual remains in control

A determining factor for individuals to trust the apps is demonstrating that they remain in control of their personal data. To ensure this, the Commission considers that in particular the following conditions should be met:

- the installation of the app on their device should be voluntary and without any negative consequences for the individual who decides not to download/use the app;
- different app functionalities (e.g. information, symptom checker, contact tracing and warning functionalities) should not be bundled so that the individual can provide his/her consent specifically for each functionality. This should not prevent the user from combining different app functionalities if this is offered as an option by the provider;
- if proximity data are used (data generated by the exchange of Bluetooth Low Energy (BLE) signals between devices within an epidemiologically relevant distance and during an epidemiologically relevant time), they should be stored on the individual's device. If those data are to be shared with health authorities, they should be shared only after confirmation that the person concerned is infected with the COVID-19 and on the condition that he/she chooses to do so;;
- health authorities should provide the individuals with all necessary information related to the processing of his or her personal data (in line with Articles 12 and 13 of the GDPR and Article 5 of the ePrivacy Directive);
- the individual should be able to exercise his/her rights under the GDPR (in particular, access, rectification; deletion). Any restriction of the rights under the GDPR and ePrivacy Directive should be in accordance with these acts and be necessary, proportionate and provided in the legislation;

[8] See recital 45 of the GDPR.

- the apps should be deactivated at the latest when the pandemic is declared to be under control; the deactivation should not depend on de-installation by the user.

3.3 Legal basis for processing

Installation of the apps and storing of information on the user's device

As noted above, under the ePrivacy Directive (Article 5), storing of information on the user's device or gaining access to the information already stored is allowed only if (i) the user has given consent or (ii) the storage and/or access is strictly necessary for the information society service (e.g. the app) explicitly requested (i.e. installed and activated) by the user.

The storage of information on the individual's device and getting access to the information already stored on this device is normally necessary for the apps to function. In addition, the contact tracing and warning functionality requires some other information (such as ephemeral, periodically changing alias user IDs of users of this functionality in proximity) to be stored on the user's device. Furthermore, this functionality may require the (infected, or likely infected) user to upload proximity data. Such an upload is not necessary for the functioning of the app as such. Therefore, the requirements of option (ii) mentioned in the previous paragraph are not met. That leaves consent (option (i) above) as the most appropriate ground for the relevant activities. This consent should be "freely given", "specific", "explicit" and "informed" within the meaning of the GDPR. It should be expressed through a clear affirmative action of the individual; this excludes tacit forms of consent (e.g. silence; inactivity).[9]

Legal basis for processing by national health authorities – Union or Member State law

National health authorities typically process personal data when there is a legal obligation laid down in EU or Member State law providing for such processing and meeting the conditions of Article 6(1)(c) and Article 9(2)(i) of the GDPR or when such processing is necessary for the performance of a task carried out to further the public interest recognised by EU or Member State law[10].

Any national law has to provide specific and suitable measures to safeguard the rights and freedoms of data subjects. As a general rule, the stronger the impact on the freedoms of the individuals, the stronger corresponding safeguards should be provided for in the relevant law.

EU and Member State laws that pre-exist to the COVID-19 outbreak and those which Member States are enacting specifically to fight the spread of epidemics may in principle, be used as a legal basis for processing of individuals' data if they provide for measures allowing for the monitoring of epidemics and if that law meets further requirements set out in Article 6 (3) GDPR.

[9] See the guidelines from the European Data Protection Board on consent: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
[10] Article 6(1)(e) GDPR.

Given the nature of the personal data concerned (in particular health data as special categories of personal data) as well as the circumstances of the current COVID-19 pandemic, relying on the law as the legal basis would contribute to legal certainty, since it would (i) prescribe in detail the processing of specific health data and clearly specify the purposes for the processing; (ii) spell out clearly who is the controller, i.e. the entity processing the data, and who, beside the controller, can have access to such data; (iii) exclude the possibility to process such data for different purposes than those listed in the legislation and (iv) provide for specific safeguards. In order not to undermine the public usefulness and acceptance of the apps the national legislator should pay particular attention that the solution chosen is as inclusive vis-a-vis citizens as possible.

Processing by health authorities on the basis of the legislation does not change the fact that the individuals remain free to install the app or not and to share their data with health authorities. No adverse consequences for the users should therefore occur whenever the app is uninstalled.

Contact tracing and warning apps provide for the warning of individuals. When this warning is provided directly by the app, the Commission draws attention to the prohibition of subjecting individuals to a decision based solely on automated processing which produces legal effect or similarly significantly affects him or her (Article 22 GDPR).

3.4 Data minimisation

The data produced via devices and already previously stored in those devices is protected as follows:

- As "personal data", i.e. any information relating to an identified or an identifiable natural person (Article 4(1) of the GDPR), it is protected under the GDPR. Health data benefit from additional protection (Article 9 of the GDPR).
- As "location data", i.e. data processed in an electronic communications network or by an electronic communication service, indicating the geographic position of the terminal equipment of the user, it is protected under the ePrivacy Directive (Art 5(1), 6 and 9)[11],
- Any information stored in and accessed from user's terminal equipment is protected under Article 5(3) of the ePrivacy Directive.

Non-personal data (such as irreversibly anonymised data) is not protected under the GDPR.

The Commission recalls that the principle of data minimisation requires that only personal data that is adequate, relevant and limited to what is necessary in relation to the purpose[12] may

[11] The Electronic Communications Code provides that services which are functionally equivalent to electronic communications services are also covered.
[12] Principle of data minimisation.

be processed. An assessment of the necessity to process the personal data and the relevance of such personal data should be carried out in the light of the purpose(s) pursued.

The Commission notes, for instance, that if the purpose of the functionality is symptom checking or telemedicine, these purposes do not require access to the contact list of the person owning the device.

Generating and processing less data limits the security risks. Therefore the compliance with data minimisation measures also provides for security safeguards.

- Information functionality:

An app with merely this functionality will not need to process any health data of individuals. It will merely provide them with information. In order to fulfil this purpose no information stored in and accessed from terminal equipment may be processed other than what is necessary to provide the information.

- Symptom checker and telemedicine functionalities:

If the app includes one or two of these functionalities, it will be processing personal health data. Therefore, a list of data which may be processed should be specified in the underlying legislation applicable to the health authorities.

In addition, the health authorities may need the phone numbers of the persons who used the symptom checker and uploaded the results. Information stored in and accessed from terminal equipment may be processed only insofar as it is necessary to enable the app to fulfil its purpose and allow it to function.

- Contact tracing and warning functionality:

A majority of COVID-19 infections occur through droplets that travel only over a limited distance. Identifying as quickly as possible persons who have been in proximity with an infected person is a key factor to interrupt the infection chain. The determining proximity is a function of the distance and duration of a contact and should be done from an epidemiologic point of view. The interruption of the infection chain is particularly relevant to avoid resurgence of infections in the crisis exit phase.

Proximity data could be necessary for this. For the metering of proximity and close contacts Bluetooth Low Energy (BLE) communications between devices appears more precise, and therefore more appropriate, than the use of geolocation data (GNSS/GPS, or cellular location data). BLE avoids the possibility of tracking (contrary to geolocation data). The Commission therefore recommends the use of BLE communications data (or data generated by equivalent technology) to determine proximity.

Location data is not necessary for the purpose of contact tracing functionalities, as their goal is not to follow the movements of individuals or to enforce prescriptions. In addition, the processing of location data in the context of contact tracing would be difficult to justify in

light of the principle of data minimisation and may create security and privacy issues. For this reason the Commission advises not to use location data in this context.

Irrespective of the technical means used to determine proximity, it does not appear necessary to store the exact time of the contact or the place (if available). However it might be useful to store the day of the contact to know whether the contact occurred when the person developed symptoms (or 48 hours before[13]) and to guide the follow up message with advice for instance on how long to self-quarantine.

Proximity data should only be generated and processed if there is an actual risk of infection (depending on the closeness and duration of the contact).

It should be noted that the necessity and proportionality of the collection of data will thus depend on factors such as the extent to which testing facilities are available in particular when measures such as confinement were already ordered. The warning of persons who have been in close contact with an infected person can be done in two ways:

Under the first approach, an alert is automatically delivered via the app to the close contacts when a user notifies the app – with the approval or confirmation by the health authority, for instance via a QR or TAN code – that he or she has tested positive (decentralised processing). The content of the alert message should preferably be determined by the health authority. Under the second approach the arbitrary temporary identifiers are stored on a backend server held by the health authority (backend server solution). Users cannot be directly identified through these data. Through the identifiers, users who have been in close contact with a positively tested user, receive an alert on their device. If the health authorities wish to contact the users who have been in close contact with an infected person also via phone or SMS, they need the consent of those users to provide their phone numbers.

3.5 Limiting the disclosure/access of data

- Information functionality:

No information stored in and accessed from terminal equipment can be shared with health authorities other than necessary to have the information functionality. Since this functionality provides only for the means of communication, health authorities will not get access to any other data.

- Symptom checker and telemedicine functionalities:

The symptom checker functionality can be useful for Member States to guide citizens about whether they should get tested, provide information about isolation and when and how to access healthcare in particular for risk groups. This functionality can also complement primary care surveillance and help understand what the infection rates of COVID-19 are in the population. Therefore, it may be decided that responsible health authorities and national

[13] The infected person is contagious 48 h before the onset of symptoms.

epidemiological authorities should get access to the information provided by the patient. ECDC could receive aggregated data from national authorities for epidemiological surveillance.

If the choice is made to allow for a contact with health officials rather than only through the app itself, then disclosing to national health authorities the telephone number of app users is also necessary.

- Contact tracing and warning functionality:
    - Data of the infected person

The apps generate pseudo-randomly ephemeral and periodically changing identifiers of the phones that are in contact with the user. One option is that the identifiers are stored on the device of the user (so called decentralised processing). Another option can provide that these arbitrary identifiers are stored on the server to which the health authorities have access (so called backend server solution). The decentralised solution is more in line with the minimisation principle. Health authorities should have access only to proximity data from the device of an infected person so that they are able to contact people at risk of infection.

These data will be available to the health authorities only after the infected person (after having been tested) proactively shares these data with them.

The infected person should not be informed about the identity of the persons with whom he/she has been in potentially epidemiologically relevant contact and who will be alerted.

    - Data of the persons who have been in (epidemiological) contact with the infected person

The identity of the infected person should not be disclosed to the persons with whom he/she has been in epidemiological contact. It is sufficient to communicate to them the fact that they have been in epidemiological contact with an infected person during the past 16 days. As noted above, data about the time and place of such contacts should not be stored. It is therefore neither necessary nor possible to communicate those data.

To trace epidemiological contacts of an e app user who is found to be infected, the national health authorities should be informed only about the identifier of the person with whom the infected person has been in epidemiological contact since 48 hours before the onset of symptoms until 14 days after the onset of symptoms, based on proximity and duration of the contact.

The ECDC could receive aggregated contact tracing data from national authorities for epidemiological surveillance on indicators defined in collaboration with Member States.

3.6 Providing for precise purposes of processing

The legal basis (Union or Member State law) should provide for the purpose of the processing. The purpose should be specific, so that there is no doubt what kind of personal data is necessary to process in order to achieve the desired objective and explicit. .

The precise purpose(s) will depend on the functionalities of the app. There may be several purposes for each functionality of an app. In order to provide the individuals with full control of their data, the Commission recommends not to bundle different functionalities. In any event, the individual should have the possibility to choose between different functionalities pursuing each a separate purpose.

The Commission advises against the use of the data gathered under the above conditions for other purposes than the fight against COVID-19. Should purposes like scientific research and statistics be necessary, they should be included in the original list of purposes and clearly communicated to users.

- Information functionality:

The purpose of this functionality is the provision of the information that is relevant from the point of view of the health authorities in the context of the crisis.

- Symptom-checker and telemedicine functionalities:

Symptom checker functionality can provide an indication of which proportion of the individuals reporting symptoms compatible with COVID-19 is actually infected (e.g. by swabbing and testing all or a random number of individuals with such symptoms, if there is capacity to do so). This identification of the purpose should make clear that the personal health data will be processed in order (i) to provide the individual with the possibility to self asses, on the basis of a set of questions asked, if he or she has developed symptoms of COVID-19, or (ii) to get medical advice if having developed the symptoms of COVID-19.

- Contact tracing and warning functionalities:

The mere indication of a purpose “prevention of further COVID-19 infections” is not specific enough. In this case, the Commission recommends to specify further the purpose(s) along the lines of: “retaining of the contacts of the persons who use the app and who may have been exposed to infection by COVID-19 in order to warn those persons who could have been potentially infected”.

3.7 Setting strict limits to data storage

The principle of storage limitation requires that personal data may not be kept for longer than necessary. Timelines should be based on medical relevance (depending on the purpose of the app: the incubation period, etc.) as well as realistic durations for administrative steps that may need to be taken.

- Information functionality:

If any data is collected while installing this functionality, it should be deleted immediately. There is no justification for keeping such data.

- Symptom checker and telemedicine functionalities:

Such data should be deleted by the health authorities after maximum one month (incubation period plus margin) or after the person was tested and the result is negative. Health authorities may retain data for longer periods for surveillance reporting and research provided it is in an anonymised form.

- Contact tracing and warning functionalities:

Proximity data should be deleted as soon as they are no longer necessary for the purpose of alerting individuals. This should be the case after maximum one month (incubation period plus margin) or after the person was tested and the result is negative. Health authorities may retain the proximity data for longer periods for surveillance reporting and research provided it is in an anonymised form.

The data should be stored on the user's device and only data that has been communicated by the users and is necessary to fulfil the purpose should be uploaded to the server available to the health authorities where this option is chosen (i.e. only upload the data to the server of "close contacts" of a person who tested positive of infection of COVID-19).

3.8 Ensuring the security of the data

The Commission recommends that the data should be stored on the terminal device of the individual in an encrypted form using state-of-the art cryptographic techniques. In the case that the data is stored in a central server, the access, including the administrative access, should be logged.

Proximity data should only be generated and stored on the terminal device of the individual in encrypted and pseudonymised format. In order to ensure that tracking by third parties –is excluded the activation of Bluetooth should be possible without having to activate other location services.

During the collection of proximity data via BLE it is preferable to create and store temporary user IDs that change regularly rather than storing the actual device ID. This measure provides additional protection against eavesdropping and tracking by hackers and therefore makes it more difficult to identify individuals.

The Commission recommends that the source code of the app should be made public and available for review.

Additional measures to secure the data processed can be envisaged notably with automatic deletion or anonymisation of the data after a certain point in time. In general, the degree of the security should match the amount and sensitivity of personal data processed.

All transmissions from the personal device to the national health authorities should be encrypted.

Where the national legalisation provides that the personal data gathered can also be processed for scientific research purposes, pseudonymisation should, in principle, be used.

3.9 Ensuring the accuracy of the data

Ensuring the accuracy of the personal data processed is not only a pre-requisite for the efficiency of the app but is also a requirement under the personal data protection legislation.

In this context, ensuring the accuracy of the information on whether a contact with an infected person (epidemiological distance and duration) has taken place is essential, to minimise the risk of having false positives. This should address scenarios when two users of the app are in contact in the street, in public transport or in a building. It is unlikely that the use of location data based on mobile phone networks is accurate enough for this.

It is therefore advisable to rely on technologies allowing a more precise assessment of the contact (such as Bluetooth).

3.10 Involving Data Protection Authorities

The Data Protection Authorities should be fully involved and consulted in the context of the development of the app and they should keep its deployment under review. Given that the processing of data in the context of the app will qualify as a processing on a large scale of special categories of data (health data), the Commission draws attention to Article 35 GDPR on data protection impact assessment.