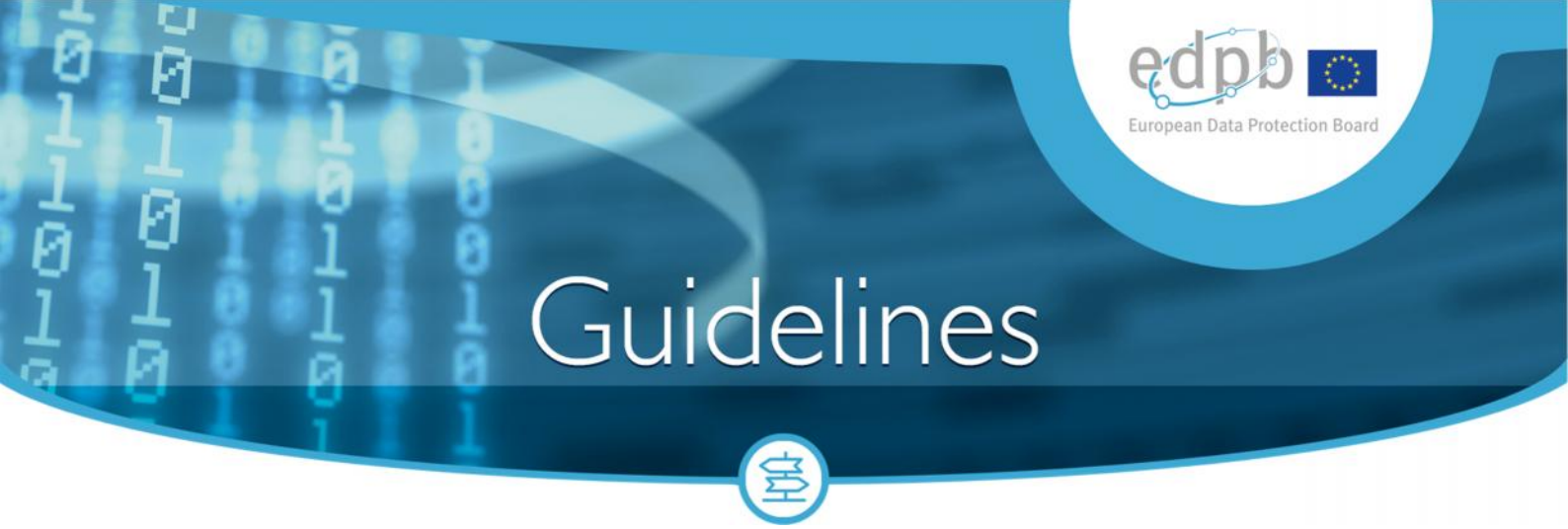

Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak

Adopted on 21 April 2020

adopted

Table of contents

The European Data Protection Board

Having regard to Article 70(1)(e) of the Regulation 2016/679/EU 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 (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES:

1 INTRODUCTION & CONTEXT

1 Governments and private actors are turning toward the use of data driven solutions as part of the response to the COVID-19 pandemic, raising numerous privacy concerns.

2 The EDPB underlines that the data protection legal framework was designed to be flexible and as such, is able to achieve both an efficient response in limiting the pandemic and protecting fundamental human rights and freedoms.

3 The EDPB firmly believes that, when processing of personal data is necessary for managing the COVID-19 pandemic, data protection is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby guarantee the effectiveness of these measures. Because the virus knows no borders, it seems preferable to develop a common European approach in response to the current crisis, or at least put in place an interoperable framework.

4 The EDPB generally considers that data and technology used to help fight COVID-19 should be used to empower, rather than to control, stigmatise, or repress individuals. Furthermore, while data and technology can be important tools, they have intrinsic limitations and can merely leverage the effectiveness of other public health measures. The general principles of effectiveness, necessity, and proportionality must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19.

5 These guidelines clarify the conditions and principles for the proportionate use of location data and contact tracing tools, for two specific purposes:

- using location data to support the response to the pandemic by modelling the spread of the virus so as to assess the overall effectiveness of confinement measures ;
- contact tracing, which aims to notify individuals of the fact that they have been in close proximity of someone who is eventually confirmed to be a carrier of the virus, in order to break the contamination chains as early as possible.

6 The efficiency of the contribution of contact tracing applications to the management of the pandemic depends on many factors (e.g., percentage of people who would need to install it; definition of a "contact" in terms of closeness and duration.). Moreover, such applications need to be part of a comprehensive public health strategy to fight the pandemic, including, inter alia, testing and subsequent manual contact tracing for the purpose of doubt removal. Their

1 References to "Member States" made throughout this document should be understood as references to "EEA Member States".

deployment should be accompanied by supporting measures to ensure that the information provided to the users is contextualized, and that alerts can be of use to the public health system. Otherwise, these applications might not reach their full impact.

7 The EDPB emphasises that the GDPR and Directive 2002/58/EC (the "ePrivacy Directive") both contain specific rules allowing for the use of anonymous or personal data to support public authorities and other actors at national and EU levels in monitoring and containing the spread of the SARS-CoV-2 virus[2].

8 In this regard, the EDPB has already taken position on the fact that the use of contact tracing applications should be voluntary and should not rely on tracing individual movements but rather on proximity information regarding users.[3]

[2] See the previous statement of the EDPB on the COVID 19 outbreak.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 USE OF LOCATION DATA

2.1 Sources of location data

9 There are two principal sources of location data available for modelling the spread of the virus and the overall effectiveness of confinement measures:

- location data collected by electronic communication service providers (such as mobile telecommunication operators) in the course of the provision of their service ; and
- location data collected by information society service providers' applications whose functionality requires the use of such data (e.g., navigation, transportation services, etc.).

10 The EDPB recalls that location data[4] collected from electronic communication providers may only be processed within the remits of articles 6 and 9 of the ePrivacy Directive. This means that these data can only be transmitted to authorities or other third parties if they have been anonymised by the provider or, for data indicating the geographic position of the terminal equipment of a user, which are not traffic data, with the prior consent of the users[5].

11 Regarding information, including location data, collected directly from the terminal equipment, art. 5(3) of the "ePrivacy" directive applies. Hence, the 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[6] or (ii) the storage and/or access is strictly necessary for the information society service explicitly requested by the user.

12 Derogations to the rights and obligations provided for in the "ePrivacy" Directive are however possible pursuant to Art. 15, when they constitute a necessary, appropriate and proportionate measure within a democratic society for certain objectives[7].

13 As for the re-use of location data collected by an information society service provider for modelling purposes (e.g., through the operating system or some previously installed application) additional conditions must be met. Indeed, when data have been collected in compliance with Art. 5(3) of the ePrivacy Directive, they can only be further processed with the additional consent of the data subject or on the basis of a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Art. 23 (1) GDPR.[8]

2.2 Focus on the use of anonymised location data

14 The EDPB emphasises that when it comes to using location data, preference should always be given to the processing of anonymised data rather than personal data.

15 Anonymisation refers to the use of a set of techniques in order to remove the ability to link the data with an identified or identifiable natural person against any "reasonable" effort. This "reasonability test" must take into account both objective aspects (time, technical means) and contextual elements that may vary case by case (rarity of a phenomenon including population density, nature and volume of data). If the data fails to pass this test, then it has not been anonymised and therefore remains in the scope of the GDPR.

16 Evaluating the robustness of anonymisation relies on three criteria: (i) singling-out (isolating an individual in a larger group based on the data); (ii) linkability (linking together two records

---

[4] See Art. 2(c) of the ePrivacy Directive.
[5] See Art 6 and 9 of the ePrivacy Directive.
[6] The notion of consent in the ePrivacy directive remains the notion of consent in the GDPR and must meet all the requirements of the consent as provided by art. 4(11) and 7 GDPR
[7] For the interpretation of article 15 of the "ePrivacy" Directive, see also, CJEU Judgment of 29 January 2008 in case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU.
[8] See section 1.5.3 of the guidelines 1/2020 on processing personal data in the context of connected vehicles.

concerning the same individual); and (iii) inference (deducing, with significant probability, unknown information about an individual).

17 The concept of anonymisation is prone to being misunderstood and is often mistaken for pseudonymisation. While anonymisation allows using the data without any restriction, pseudonymised data are still in the scope of the GDPR.

18 Many options for effective anonymisation exist[9], but with a caveat. Data cannot be anonymised on their own, meaning that only datasets as a whole may or may not be made anonymous. In this sense, any intervention on a single data pattern (by means of encryption, or any other mathematical transformations) can at best be considered a pseudonymisation.

19 Anonymisation processes and re-identification attacks are active fields of research. It is crucial for any controller implementing anonymisation solutions to monitor recent developments in this field, especially concerning location data (originating from telecom operators and/or information society services) which are known to be notoriously difficult to anonymise.

20 Indeed, a large body of research has shown[10] that *location data thought to be anonymised* may in fact not be. Mobility traces of individuals are inherently highly correlated and unique. Therefore, they can be vulnerable to re-identification attempts under certain circumstances.

21 A single data pattern tracing the location of an individual over a significant period of time cannot be fully anonymised. This assessment may still hold true if the precision of the recorded geographical coordinates is not sufficiently lowered, or if details of the track are removed and even if only the location of places where the data subject stays for substantial amounts of time are retained. This also holds for location data that is poorly aggregated.

22 To achieve anonymisation, location data must be carefully processed in order to meet the reasonability test. In this sense, such a processing includes considering location datasets as a whole, as well as processing data from a reasonably large set of individuals using available robust anonymisation techniques, provided that they are adequately and effectively implemented.

23 Lastly, given the complexity of anonymisation processes, transparency regarding the anonymisation methodology is highly encouraged.

[9] (de Montjoye et al., 2018) "On the privacy-conscientious use of mobile phone data"
[10] (de Montjoye et al., 2013) "Unique in the Crowd: The privacy bounds of human mobility" and (Pyrgelis et al., 2017) "Knock Knock, Who's There? Membership Inference on Aggregate Location Data"

3 CONTACT TRACING APPLICATIONS

3.1 General legal analysis

24 The systematic and large scale monitoring of location and/or contacts between natural persons is a grave intrusion into their privacy. It can only be legitimised by relying on a voluntary adoption by the users for each of the respective purposes. This would imply, in particular, that individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all.

25 To ensure accountability, the controller of any contact tracing application should be clearly defined. The EDPB considers that the national health authorities could be the controllers[11] for such application; other controllers may also be envisaged. In any cases, if the deployment of contact tracing apps involves different actors their roles and responsibilities must be clearly established from the outset and be explained to the users.

26 In addition, with regard to the principle of purpose limitation, the purposes must be specific enough to exclude further processing for purposes unrelated to the management of the COVID-19 health crisis (e.g., commercial or law enforcement purposes). Once the objective has been clearly defined, it will be necessary to ensure that the use of personal data is adequate, necessary and proportionate.

27 In the context of a contact tracing application, careful consideration should be given to the principle of data minimisation and data protection by design and by default:

- contact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used;
- as contact tracing applications can function without direct identification of individuals, appropriate measures should be put in place to prevent re-identification;
- the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary.

28 Regarding the lawfulness of the processing, the EDPB notes that contact tracing applications involve storage and/or access to information already stored in the terminal, which are subject to Art. 5(3) of the "ePrivacy" Directive. If those operations are strictly necessary in order for the provider of the application to provide the service explicitly requested by the user the processing would not require his/her consent. For operations that are not strictly necessary, the provider would need to seek the consent of the user.

29 Furthermore, the EDPB notes that the mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent. When public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest, i.e. Art. 6(1)(e) GDPR.

30 Article 6(3) GDPR clarifies that the basis for the processing referred to in article 6(1)(e) shall be laid down by Union or Members State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.[12]

31 The legal basis or legislative measure that provides the lawful basis for the use of contact tracing applications should, however, incorporate meaningful safeguards including a reference to the voluntary nature of the application. A clear specification of purpose and explicit

[11] See also European Commission "Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection" Brussels, 16.4.2020 C(2020) 2523 final.
[12] See Recital (41).

limitations concerning the further use of personal data should be included, as well as a clear identification of the controller(s) involved. The categories of data as well as the entities to (and purposes for which, the personal data may be disclosed) should also be identified. Depending on the level of interference, additional safeguards should be incorporated, taking into account the nature, scope and purposes of the processing. Finally, the EDPB also recommends including, as soon as practicable, the criteria to determine when the application shall be dismantled and which entity shall be responsible and accountable for making that determination.

32 However, if the data processing is based on another legal basis, such as consent (Art. 6(1)(a))[13] for example, the controller will have to ensure that the strict requirements for such legal basis to be valid are met.

33 Moreover, the use of an application to fight the COVID-19 pandemic might lead to the collection of health data (for example the status of an infected person). Processing of such data is allowed when such processing is necessary for reasons of public interest in the area of public health, meeting the conditions of art. 9(2)(i) GDPR[14] or for health care purposes as described in Art. 9(2)(h) GDPR[15]. Depending on the legal basis, it might also be based on explicit consent (Art. 9(2)(a) GDPR).

34 In accordance with the initial purpose, Article 9(2)(j) GDPR also allows for health data to be processed when necessary for scientific research purposes or statistical purposes.

35 The current health crisis should not be used as an opportunity to establish disproportionate data retention mandates. Storage limitation should consider the true needs and the medical relevance (this may include epidemiology-motivated considerations like the incubation period, etc.) and personal data should be kept only for the duration of the COVID-19 crisis. Afterwards, as a general rule, all personal data should be erased or anonymised.

36 It is the EDPB's understanding that such apps cannot replace, but only support, manual contact tracing performed by qualified public health personnel, who can sort out whether close contacts are likely to result in virus transmission or not (e.g., when interacting with someone protected by adequate equipment – cashiers, etc. -- or not). The EDPB underlines that procedures and processes including respective algorithms implemented by the contact tracing apps should work under the strict supervision of qualified personnel in order to limit the occurrence of any false positives and negatives. In particular, the task of providing advice on next steps should not be based solely on automated processing.

37 In order to ensure their fairness, accountability and, more broadly, their compliance with the law, algorithms must be auditable and should be regularly reviewed by independent experts. The application's source code should be made publicly available for the widest possible scrutiny.

38 False positives will always occur to a certain degree. As the identification of an infection risk probably can have a high impact on individuals, such as remaining in self isolation until tested negative, the ability to correct data and/or subsequent analysis results is a necessity. This, of course, should only apply to scenarios and implementations where data is processed and/or stored in a way where such correction is technically feasible and where the adverse effects mentioned above are likely to happen.

39 Finally the EDPB considers that a data protection impact assessment (DPIA) must be carried out before implementing such tool as the processing is considered likely high risk (health data,

[13] Controllers (especially public authorities) must pay special attention to the fact that consent should not be regarded as freely given if the individual has no genuine choice to refuse or withdraw its consent without detriment.
[14] The processing must be based on Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
[15] See Article 9(2)(h) GDPR

anticipated large-scale adoption, systematic monitoring, use of new technological solution)[16]. The EDPB strongly recommends the publication of DPIAs.

3.2 Recommendations and functional requirements

40 According to the principle of data minimization, among other measures of Data Protection by Design and by Default[17], the data processed should be reduced to the strict minimum. The application should not collect unrelated or not needed information, which may include civil status, communication identifiers, equipment directory items, messages, call logs, location data, device identifiers, etc.

41 Data broadcasted by applications must only include some unique and pseudonymous identifiers, generated by and specific to the application. Those identifiers must be renewed regularly, at a frequency compatible with the purpose of containing the spread of the virus, and sufficient to limit the risk of identification and of physical tracking of individuals.

42 Implementations for contact tracing can follow a centralized or a decentralized approach[18]. Both should be considered viable options, provided that adequate security measures are in place, each being accompanied by a set of advantages and disadvantages. Thus, the conceptual phase of app development should always include thorough consideration of both concepts carefully weighing up the respective effects on data protection /privacy and the possible impacts on individuals rights.

43 Any server involved in the contact tracing system must only collect the contact history or the pseudonymous identifiers of a user diagnosed as infected as the result of a proper assessment made by health authorities and of a voluntary action of the user. Alternately, the server must keep a list of pseudonymous identifiers of infected users or their contact history only for the time to inform potentially infected users of their exposure, and should not try to identify potentially infected users.

44 Putting in place a global contact tracing methodology including both applications and manual tracing may require additional information to be processed in some cases. In this context, this additional information should remain on the user terminal and only be processed when strictly necessary and with his prior and specific consent.

45 State-of-the-art cryptographic techniques must be implemented to secure the data stored in servers and applications, exchanges between applications and the remote server. Mutual authentication between the application and the server must also be performed.

46 The reporting of users as COVID-19 infected on the application must be subject to proper authorization, for example through a single-use code tied to a pseudonymous identity of the infected person and linked to a test station or health care professional. If confirmation cannot be obtained in a secure manner, no data processing should take place that presumes the validity of the user's status.

47 The controller, in collaboration with the public authorities, have to clearly and explicitly inform about the link to download the official national contact tracing app in order to mitigate the risk that individuals use a third-party app.

---

[16] See WP29 guidelines (adopted by the EDPB) on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.
[17] See EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default
[18] In general, the decentralised solution is more in line with the minimisation principle

4 CONCLUSION

48 The world is facing a significant public health crisis that requires strong responses, which will have an impact beyond this emergency. Automated data processing and digital technologies can be key components in the fight against COVID-19. However, one should be wary of the "ratchet effect". It is our responsibility to ensure that every measure taken in these extraordinary circumstances are necessary, limited in time, of minimal extent and subject to periodic and genuine review as well as to scientific evaluation.

49 The EDPB underlines that one should not have to choose between an efficient response to the current crisis and the protection of our fundamental rights: we can achieve both, and moreover data protection principles can play a very important role in the fight against the virus. European data protection law allows for the responsible use of personal data for health management purposes, while also ensuring that individual rights and freedoms are not eroded in the process.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

ANNEX -- CONTACT TRACING APPLICATIONS ANALYSIS GUIDE

0. Disclaimer

The following guidance is neither prescriptive nor exhaustive, and its sole purpose of this guide is to provide general guidance to designers and implementers of contact tracing applications. Other solutions than the ones described here can be used and can be lawful as long as they comply with the relevant legal framework (i.e. GDPR and the "ePrivacy" Directive).

It must also be noted that this guide is of a general nature. Consequently, the recommendations and obligations contained in this document must not be seen as exhaustive. Any assessment must be carried out on a case-by-case basis, and specific applications may require additional measures not included in this guide.

1. Summary

In many Member States stakeholders are considering the use of *contact tracing** applications to help the population discover whether they have been in contact with a person infected with SARS-Cov-2*.

The conditions under which such applications would contribute effectively to the management of the pandemic are not yet established. And these conditions would need to be established prior to any implementation of such an app. Yet, it is relevant to provide guidelines bringing relevant information to development teams upstream, so that the protection of personal data can be guaranteed from the early design stage.

It must be noted that this guide is of a general nature. Consequently, the recommendations and obligations contained in this document must not be seen as exhaustive. Any assessment must be carried out on a case-by-case basis, and specific applications may require additional measures not included in this guide. The purpose of this guide is to provide general guidance to designers and implementers of contact tracing applications.

Some criteria might go beyond the strict requirements stemming from the data protection framework. They aim at ensuring the highest level of transparency, in order to favour social acceptance of such contact tracing applications.

To this end, publishers of contact tracing applications should take into account the following criteria:

- The use of such an application must be strictly voluntary. It may not condition the access to any rights guaranteed by law. Individuals must have full control over their data at all times, and should be able to choose freely to use such an application.
- Contact tracing applications are likely to result in a high risk to the rights and freedoms of natural persons and to require a data protection impact assessment to be conducted prior to their deployment.
- Information on the proximity between users of the application can be obtained without locating them. This kind of application does not need, and, hence, should not involve the use of location data.

- When a user is diagnosed infected with the SARS-Cov-2 virus, only the persons with whom the user has been in close contact within the epidemiologically relevant retention period for contact tracing, should be informed.
- The operation of this type of application might require, depending on the architecture that is chosen, the use of a centralised server. In such a case and in accordance with the principles of data minimisation and data protection by design, the data processed by the centralised server should be limited to the bare minimum:
    - When a user is diagnosed as infected, information regarding its previous close contacts or the identifiers broadcasted by the user's application can be collected, only with the user's agreement. A verification method needs to be established that allows asserting that the person is indeed infected without identifying the user. Technically this could be achieved by alerting contacts only following the intervention of a healthcare professional, for example by using a special one-time code.
    - The information stored on the central server should neither allow the controller to identify users diagnosed as infected or having been in contact with those users, nor should it allow the inference of contact patterns not needed for the determination of relevant contacts.
- The operation of this type of application requires to broadcast data that is read by devices of other users and listening to these broadcasts:
    - It is sufficient to exchange pseudonymous identifiers between users' mobile equipment (computers, tablets, connected watches, etc.), for example by broadcasting them (e.g. via the Bluetooth Low Energy technology).
    - Identifiers must be generated using state-of-the-art cryptographic processes.
    - Identifiers must be renewed on a regular basis to reduce the risk of physical tracking and linkage attacks.
- This type of application must be secured to guarantee safe technical processes. In particular:
    - The application should not convey to the users information that allows them to infer the identity or the diagnosis of others. The central server must neither identify users, nor infer information about them.

Disclaimer: the above principles are related to the claimed purpose of *contact tracing* applications, and to this purpose only, which only aim to automatically inform people potentially exposed to the virus (without having to identify them).The operators of the application and its infrastructure may be controlled by the competent supervisory authority. Following all or part of these guidelines is not necessarily sufficient to ensure a full compliance to the data protection framework.

2. Definitions

Contact	For a contact tracing application, a contact is a user who has participated in an interaction with a user confirmed to be a carrier of the virus, and whose duration and distance induce a risk of significant exposure to the virus infection.

	Parameters for duration of exposure and distance between people must be estimated by the health authorities and can be set in the application.
Location data	It refers to all data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a publicly available electronic communications service (as defined in the e-Privacy Directive), as well as data from potential other sources, relating to: - the latitude, longitude or altitude of the terminal equipment; - the direction of travel of the user; or - the time the location information was recorded.
Interaction	In the context of the contact tracing application, an interaction is defined as the exchange of information between two devices located in close proximity to each other (in space and time), within the range of the communication technology used (e.g. Bluetooth). This definition excludes the location of the two users of the interaction.
Virus carrier	In this document, we consider virus carriers to be users who have been tested positive for the virus and who have received an official diagnosis from physicians or health centres.
Contact tracing	People who have been in close contact (according to criteria to be defined by epidemiologists) with an individual infected with the virus run a significant risk of also being infected and of infecting others in turn. Contact tracing is a disease control methodology that lists all people who have been in close proximity to a carrier of the virus so as to check whether they are at risk of infection and take the appropriate sanitary measures towards them.

3. General

GEN-1	The application must be a complementary tool to traditional contact tracing techniques (notably interviews with infected persons), i.e. be part of a wider public health program. It must be used only up until the point manual contact tracing techniques can manage alone the amount of new infections.
GEN-2	At the latest when ”return to normal” is decided by the competent public authorities, a procedure must be put in place to stop the collection of identifiers (global deactivation of the application, instructions to uninstall the application, automatic uninstallation, etc.) and to activate the deletion of all collected data from all databases (mobile applications and servers).

GEN-3	The source code of the application and of its backend must be open, and the technical specifications must be made public, so that any concerned party can audit the code, and where relevant - contribute to improving the code, correcting possible bugs and ensuring transparency in the processing of personal data.
GEN-4	The stages of deployment of the application must make it possible to progressively validate its effectiveness from a public health point of view. An evaluation protocol, specifying indicators allowing to measure the effectiveness of the application, must be defined upstream for this purpose.

4. Purposes

PUR-1	The application must pursue the sole purpose of contact tracing so that people potentially exposed to the SARS-Cov-2 virus can be alerted and taken care of. It must not be used for another purpose.
PUR-2	The application must not be diverted from its primary use for the purpose of monitoring compliance with quarantine or confinement measures and/or social distancing.
PUR-3	The application must not be used to draw conclusions on the location of the users based on their interaction and/or any other means.

5. Functional considerations

FUNC-1	The application must provide a functionality enabling users to be informed that they have been potentially exposed to the virus, this information being based on proximity to an infected user within a window of X days prior to the positive screening test (the X value being defined by the health authorities).
FUNC-2	The application should provide recommendations to users identified as having being potentially exposed to the virus. It should relay instructions regarding the measures they should follow, and they should allow the user to request advises. In such cases, a human intervention would be mandatory.
FUNC-3	The algorithm measuring the risk of infection by taking into account factors of distance and time and thus determining when a contact has to be recorded in the contact tracing list, must be securely tuneable to take into account the most recent knowledge on the spread of the virus.
FUNC-4	**Users must be informed in case they have been exposed to the virus**, or must regularly obtain information on whether or not they have been exposed to the virus, within the incubation period of the virus.
FUNC-5	The application should be interoperable with other applications developed across EU Member States, so that users travelling across different Member States can be efficiently notified.

6. Data

DATA-1	The application must be able to broadcast and receive data via proximity communication technologies like Bluetooth Low Energy so that contact tracing can be carried out.
DATA-2	This broadcast data must include cryptographically strong pseudo-random identifiers, generated by and specific to the application.
DATA-3	The risk of collision between pseudo-random identifiers should be sufficiently low.
DATA-4	Pseudo-random identifiers must be renewed regularly, at a frequency sufficient to limit the risk of re-identification, physical tracking or linkage of individuals, by anyone including central server operators, other application users or malicious third parties. These identifiers must be generated by the user's application, possibly based on a seed provided by the central server.
DATA-5	According to the data minimisation principle, the application must not collect data other than what is strictly necessary for the purpose of contact tracing
DATA-6	The application must not collect location data for the purpose of contact tracing. Location data can be processed for the sole purpose of allowing the application to interact with similar applications in other countries and should be limited in precision to what is strictly necessary for this sole purpose.
DATA-7	The application should not collect health data in addition to those that are strictly necessary for the purposes of the app, except on an optional basis and for the sole purpose of assisting in the decision making process of informing the user.
DATA-8	Users must be informed of all personal data that will be collected. This data should be collected only with the user authorization.

7. Technical properties

TECH-1	The application should available technologies such as use proximity communication technology (e.g. Bluetooth Low Energy) to detect users in the vicinity of the device running the application.
TECH-2	The application should keep the history of a user's contacts in the equipment, for a predefined limited period of time.
TECH-3	The application may rely on a central server to implement some of its functionalities.

TECH-4	The application must be based on an architecture relying as much as possible on users' devices.
TECH-5	At the initiative of users reported as infected by the virus and after confirmation of their status by an appropriately certified health professional, their contact history or their own identifiers should be transmitted to the central server.

8. Security

SEC-1	A mechanism must verify the status of users who report as SARS-CoV-2positive in the application, for example by providing a single-use code linked to a test station or health care professional. If confirmation cannot be obtained in a secure manner, data must not be processed.
SEC-2	The data sent to the central server must be transmitted over a secure channel. The use of notification services provided by OS platform providers should be carefully assessed, and should not lead to disclosing any data to third parties.
SEC-3	Requests must not be vulnerable to tampering by a malicious user
SEC-4	State-of-the-art cryptographic techniques must be implemented to secure exchanges between the application and the server and between applications and as a general rule to protect the information stored in the applications and on the server. Examples of techniques that can be used include for example : symmetric and asymmetric encryption, hash functions, private membership test, private set intersection, Bloom filters, private information retrieval, homomorphic encryption, etc.
SEC-5	The central server must not keep network connection identifiers (e.g., IP addresses) of any users including those who have been positively diagnosed and who transmitted their contacts history or their own identifiers.
SEC-6	In order to avoid impersonation or the creation of fake users, the server must authenticate the application.
SEC-7	The application must authenticate the central server.
SEC-8	The server functionalities should be protected from replay attacks.
SEC-9	The information transmitted by the central server must be signed in order to authenticate its origin and integrity.
SEC-10	Access to all data stored in the central server and not publicly available must be restricted to authorised persons only.
SEC-11	The device's permission manager at the operating system level must only request the permissions necessary to access and use when necessary the communication modules, to store the data in the terminal, and to exchange information with the central server.

9. Protection of personal data and privacy of natural persons

Reminder: the following guidelines concern an application whose sole purpose is contact tracing.

PRIV-1	Data exchanges must be respectful of the users' privacy (and notably respect the principle of data minimisation).
PRIV-2	The application must not allow users to be directly identified when using the application.
PRIV-3	The application must not allow users' movements to be traced.
PRIV-4	The use of the application should not allow users to learn anything about other users (and notably whether they are virus carriers or not).
PRIV-5	Trust in the central server must be limited. The management of the central server must follow clearly defined governance rules and include all necessary measures to ensure its security. The localization of the central server should allow an effective supervision by the competent supervisory authority.
PRIV-6	A Data Protection Impact Assessment must be carried out and should be made public.
PRIV-7	The application should only reveal to the user whether they have been exposed to the virus, and, if possible without revealing information about other users, the number of times and dates of exposure.
PRIV-8	The information conveyed by the application must not allow users to identify users carrying the virus, nor their movements.
PRIV-9	The information conveyed by the application must not allow health authorities to identify potentially exposed users without their agreement.
PRIV-10	Requests made by the applications to the central server must not reveal anything about the virus carrier.
PRIV-11	Requests made by the applications to the central server must not reveal any unnecessary information about the user, except, possibly, and only when necessary, for their pseudonymous identifiers and their contact list.
PRIV-12	Linkage attacks must not be possible.
PRIV-13	Users must be able to exercise their rights via the application.
PRIV-14	Deletion of the application must result in the deletion of all locally collected data.
PRIV-15	The application should only collect data transmitted by instances of the application or interoperable equivalent applications. No data relating to other applications and/or proximity communication devices shall be collected.
PRIV-16	In order to avoid re-identification by the central server, proxy servers should be implemented. The purpose of these *non-colluding servers is to* mix the identifiers of several users (both those of virus carriers and those sent by requesters) before sharing them with the central server, so as to prevent the central server from knowing the identifiers (such as IP addresses) of users.
PRIV-17	The application and the server must be carefully developed and configured in order not to collect any unnecessary data (e.g., no identifiers should be included

	in the server logs, etc.) and in order to avoid the use of any third party SDK collecting data for other purposes.

Most contact tracing applications currently being discussed follow basically two approaches when a user is declared infected: they can either send to a server the history of proximity contacts they have obtained through scanning, or they can send the list of their own identifiers that were broadcasted. The following principles are declined according to these two approaches. While these approaches are discussed here, that does not mean other approaches are not possible or even preferable, for example approaches that implement some form of E2E encryption or apply other security or privacy enhancing technologies.

9.1. Principles that apply only **when the application sends to the server a list of contacts:**

CON-1	The central server must collect the contact history of users reported as positive to COVID-19 as a result of voluntary action on their part.
CON-2	The central server must not maintain nor circulate a list of the pseudonymous identifiers of users carrying the virus.
CON-3	Contact history stored on the central server must be deleted once users are notified of their proximity with a positively diagnosed person.
CON-4	Except when the user detected as positive shares his contact history with the central server or when the user makes a request to the server to find out his potential exposure to the virus, no data must leave the user's equipment.
CON-5	Any identifier included in the local history must be deleted after X days from its collection (the X value being defined by the health authorities).
CON-6	Contact histories submitted by distinct users should not further be processed e.g. cross-correlated to build global proximity maps.
CON-7	Data in server logs must be minimised and must comply with data protection requirements

9.2. Principles that apply only when the application sends to a server a list of its own identifiers:

ID-1	The central server must collect the identifiers broadcast by the application of users reported as positive to COVID-19, as a result of voluntary action on their part.
ID-2	The central server must not maintain nor circulate the contact history of users carrying the virus.
ID-3	Identifiers stored on the central server must be deleted once they were distributed to the other applications.
ID-4	Except when the user detected as positive shares his identifiers with the central server, no data must leave the user's equipment or when the user makes a

	request to the server to find out his potential exposure to the virus, no data must leave the user's equipment.
ID-5	Data in server logs must be minimised and must comply with data protection requirements