RESEARCH
LUXEMBOURG
COVID-19 Task Force

REPORT ON DIGITAL PROXIMITY TRACING IN THE CONTEXT OF THE COVID19 CRISIS

27.04.2020

WP05 Scientific Advisory Group

Damien Dietrich, Gabriele Lenzini, Philippe Valoggia, Guy Fagherazzi, Raquel Gomez Bravo, Jasmin Schulz, Dimitrii Pogorelov, Raffaella Vaccaroli

Executive Summary

European residents and businesses are facing significant restrictions on public life, social contact and economic activity in an attempt to contain the transmission of the SARS-CoV-2 virus and thus (1) prevent hospital overload and (2) protect citizens at risk for developing severe complications of the disease.

Although effective, this shutdown is not a long-term solution, and exit strategies are being planned and executed worldwide. Comprehensive testing and isolation of infected individuals and their contacts is the spearhead of the majority of these strategies. Identification and isolation of contacts are particularly important as up to 62% of new infections occur during the pre-symptomatic phase of the disease. In other words, any citizen who has been, consciously or not, in close contact with an infected patient, increases the likelihood of a new epidemic cluster, unless he decides to stay at home. A critical step to contain the epidemic is, therefore, to inform these individuals. Technically, this measure is called "contact tracing".

Traditionally, contact tracing is performed over the phone by health authorities: an agent asks a newly diagnosed patient for his contacts over the infectious period. This process has the advantage of being contextual but is time-consuming and may be inaccurate. Several governments are looking at information technology to overcome those limitations with a solution that automatically keeps track of the people getting in close proximity to one another. We talk, in that case, of digital proximity tracing. Digital proximity tracing refers to a set of technologies, usually running on smartphones, allowing for the identification and record of contacts. As compared to traditional contact tracing, these technologies have the potential to be (1) more exhaustive and precise (more contacts are recorded, and contact information are complete and accurate), and (2) faster, as contacts are immediately available and can be notified at once.

Digital proximity tracing can be based on geolocation or Bluetooth or a combination of both. Geolocation-based solutions can be inaccurate in indoors and are markedly impacting privacy, as opposed to Bluetooth-based solutions that are officially supported by the European Commission.

Based on the first available studies, the acceptability for Bluetooth-based solution amongst European citizen seems to be high. However, it is estimated (but need confirmation) that at least 60% of the population would need to use these solutions for them to be effective. A real-world evaluation of their impact is still missing and would vary based on the type of implementation.

The impact on privacy as well as the GDPR and legal compliance of Bluetooth-based solutions depends mainly on their mode of implementation. Several aspects are to be considered, the most important ones being (1) the implementation framework, (2) the implementation architecture, (3) the level of anonymity, (4) the consent management, (5) the data collection, processing and storage. In any case, participation based on free will is recommended.

Another aspect to be considered is its interoperability. Since the virus knows no border, a digital proximity tracing framework must work at least in neighbouring countries. The following document aims to introduce decision-makers to the thematic (Section 1), to a comprehensive state-of-the-art (Section 2), to practical recommendations for Luxembourg (Section 3) and options to move forward (Section 4).

1. Introduction

The coronavirus disease (COVID-19), having originated in Wuhan, Hubei province, China rapidly spread across the world, with the total number of infected individuals reaching 2’355’853 cases, as of April 20th 2020[1]. Although most of the patients exhibit mild symptoms encompassing fever, upper respiratory tract symptoms, dyspnea, and diarrhea[2], in severe cases the infection results in interstitial pneumonia, severe acute respiratory syndrome, multiple organ failure, and death[3]. In order to slow down the transmission of the infection and prevent overwhelming the health systems, more than 100 countries instituted either complete or partial lockdowns by the end of March 2020[4].

Albeit effective, not only do these restrictions on social life and economic activity put the economy at risk for a deep recession, but they also take their toll on the mental health of the population[5]. Hence, exit strategies are being evaluated by governments worldwide.

One of the most promising strategies, based on a recommendation by the WHO[6] and inspired by countries having successfully contained the spread of the infection[7], is to gradually lift the restrictions and switch to a massive screening and testing combined with targeted contact tracing and quarantine approach.

eHealth tools, such as mobile applications, can be instrumental in pursuing this policy by (1) empowering citizens with the timely delivery of up-to-date and accurate information, (2) streamlining access to healthcare facilities, (3) reinforcing the adherence to quarantine, (4) facilitating and speeding up contact back-tracing - which is of particular importance as up to 62% of infections occur during the pre-symptomatic period[8,9]-, (5) allowing the generation of data that can be used to manage the infection.

The European Union (EU) has recognised the potential benefits of mobile applications for the fight against COVID-19 in the European Commission recommendation document for member states[10], while providing guidelines for their implementation and usage.

Another element we deem crucial to consider in elaboration and implementation of eHealth strategies is the stance medical and scientific communities take on the matter. The German Academy of Science Leopoldina, in its statement from April 13th 2020, stated that traditional epidemiological methods of reporting and monitoring cases can be enhanced by innovative

[1] https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

[2] Guan, W.J.; Ni, Z.Y.; Hu, Y.; Liang, W.H.; Ou, C.Q.; He, J.X.; Liu, L.; Shan, H.; Lei, C.L.; Hui, D.S.C.; et al. Clinical Characteristics of Coronavirus Disease 2019 in China. N. Engl. J. Med. 2020.

[3] Chen, N.; Zhou, M.; Dong, X.; Qu, J.; Gong, F.; Han, Y.; Qiu, Y.;Wang, J.; Liu, Y.;Wei, Y.; et al. Epidemiological and clinical characteristics of 99 cases of 2019 novel coronavirus pneumonia in Wuhan, China: A descriptive study. Lancet 2020, 395, 507–513.

[4] https://www.bbc.com/news/world-52103747

[5] https://www.who.int/docs/default-source/coronaviruse/mental-health-considerations.pdf?sfvrsn=6d3578af_2

[6] https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---16-march-2020

[7] https://www.nature.com/articles/d41586-020-00938-0

[8] https://science.sciencemag.org/content/early/2020/03/30/science.abb6936

[9] https://www.ecdc.europa.eu/sites/default/files/documents/covid-19-rapid-risk-assessment-coronavirus-disease-2019-eighth-update-8-april-2020.pdf

[10] https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf

digital epidemiology approaches (such as smartphone apps), based on voluntary "data donations" and contact tracing[11]. The usage of such technologies empowers the citizens and enables them to make their personal contribution to fighting the pandemic. The Luxembourgish Association of Doctors and Medical Dentists (AMMD) in its open letter of appeal to the Minister of Health Paulette Lenert called for the launch of mobile applications allowing secure epidemiological back-tracing of spatial and temporal contact between individuals. They further emphasised that the same tool could facilitate paperless processing and completion of the due documents (sick leaves, prescriptions, …)[12].

Importantly, these eHealth tools have limitations as they rely on technology that can be diverted (e.g.: letting the phone at home to prevent contact tracing). Moreover, a certain part of the population may not be able to use them. Finally, all existing apps raise important privacy concerns that need to be addressed before their implementation. An acceptability study in France has suggested a strong support from the population, whereas 56% of respondents in Germany stated that they would use such an application voluntarily [13,14].

The present report focuses mainly on **proximity tracing** and aims to provide decision-makers with a summary of the state-of-the-art eHealth approaches and their role in combating the COVID-19 epidemic in Luxembourgish, European and global contexts (Section 2) as well as with important strategic considerations and recommendations (Section 3). In Section 4, options to move forward are presented.

[11] https://www.leopoldina.org/uploads/tx_leopublication/2020_04_13_Coronavirus-Pandemie-Die_Krise_nachhaltig_%C3%BCberwinden_final.pdf

[12] https://www.ammd.lu/actualites/article/2020/04/reprise-progressive-des-activites-medicales-et-medico-dentaires

[13] https://www.lemonde.fr/pixels/article/2020/04/01/coronavirus-les-francais-favorables-a-une-application-mobile-pour-combattre-la-pandemie-selon-un-sondage_6035233_4408996.html

[14] https://www.br.de/nachrichten/netzwelt/br24-umfrage-56-prozent-der-deutschen-wuerden-corona-app-nutzen,RveCeQh

2. State-of-the-art

2.1. Proximity tracing as a tool to support contact isolation

According to WHO, early tracing and close follow-up of those who have been in contact with a confirmed case of COVID-19 will help them to receive care and start self-isolating, preventing further transmission of the virus.

In the context of the COVID-19 pandemic, contact tracing is of particular importance as up to 62% of new infections occur during the pre-symptomatic phase[15,16]. In the absence of a vaccine and specific treatment, the only way to prevent these pre-symptomatic individuals from infecting other people - and thus to break the infection chains - is to quickly detect, test and isolate them, based on their contact history.

Traditionally, public health officials are interviewing newly diagnosed patients over the phone and asking who has been exposed to them during the infectious period. This process is time-consuming, prone to errors, and only covers part of all contacts because it relies on the recollections of the interviewees, who may fail to provide the exhaustive and accurate list of contacts or do not have this information. On the other hand, conventional tracing may have the advantage of collecting more granular data about the nature and the duration of the exposure. WHO urges the health authorities to locate every listed contact, inform them about their status, actions that will follow (triage, testing, quarantine, …) and advice on what to do, should a contact of a confirmed COVID-19 case develop symptoms. **Accordingly, contact tracing in the context of COVID-19 is both critical and resource-demanding.**

In view of these considerations, the interest in digital solutions to identify and record contacts has grown considerably. In this document, we will refer to this set of technologies as “proximity tracing”. Digital proximity tracing has several theoretical advantages over manual contact tracking: (1) comprehensiveness (every contact is automatically recorded if the bearer of a mobile device happened to be in close contact to a COVID -19 case) (2) decreased time to isolation (if a citizen is tested positive, a notification can be sent anonymously and without delay to all his contacts during the infectious period). However, as mentioned above, digital contact tracing is not contextual (context of contacts are not recorded). **All in all, digital proximity tracing seems complementary to and synergistic with manual contact tracing.**

One important requirement for digital proximity tracing to be effective is for it to reach the necessary penetration in the population. According to the EU Commission Report[17] (that refers to a statement from the Singaporean Ministry of Development and a study by Oxford University, also cited in the reference science paper[18]), **60 to 75% of the population would need to use the app**, which is close to the 70-80% of the population owning Bluetooth-

[15] https://science.sciencemag.org/content/early/2020/03/30/science.abb6936

[16] https://www.ecdc.europa.eu/sites/default/files/documents/covid-19-rapid-risk-assessment-coronavirus-disease-2019-eighth-update-8-april-2020.pdf

[17] https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf

[18] https://science.sciencemag.org/content/early/2020/03/30/science.abb6936

enabled phones. However, more studies are needed to better evaluate this number.

Although the potential of these solutions is supported by simulations and projections, the real-world assessment of their efficacy and effectiveness is still needed. Hopefully, such data may be provided soon by Asian countries. In particular, it would be worthwhile to evaluate the gain in exhaustiveness and mean time to isolation.

2.2. Technologies and initiatives in proximity tracing

Proximity-tracing can rely on:

- Bluetooth low-energy
- Geolocation, notably using GPS
- Data from telecommunication providers
- A combination of several of these modalities

Geolocation-based solutions for proximity tracing keep record of people's whereabouts by using GPS and cellphone cells. From geolocation data, contacts between people can be computed. This methodology has been successfully adopted in China and South Korea but is considered extremely invasive in European Countries.

Indeed, this set of technologies may be considered as unlawful and politically questionable in most liberal democracies as they potentially enable mass surveillance, which is opposed by several human right organisations and foundations (e.g. Electronic Frontier Foundation (EFF)[19] and Informatics Europe [20]). The EU itself, in a recent commission recommendation document [21] expresses concerns about the use of geolocation to tracking individuals:

"*measures taken in certain countries, such as the geolocation-based tracking of individuals, the use of technology to rate an individual's level of health risk and the centralisation of sensitive data, raise questions from the viewpoint of several fundamental rights and freedoms guaranteed in the EU legal order, including the right to privacy and the right to the protection of personal data*" (ibid, item (23)).

In addition to privacy and data protection concerns, geolocation data are notably imprecise indoors and lose precision if the GPS signal is obstructed (e.g. by buildings or underground). There is also no proof that GPS and cell tower location data can allow reliable calculation of whether two or more individuals have been within a distance from each other that is relevant for the virus transmission.

For all these reasons, there is a strong preference in the scientific community towards other solutions. The most widely debated ones use short-range proximity communication, mainly via Bluetooth, between smartphones.

[19] https://www.eff.org/deeplinks/2020/03/governments-havent-shown-location-surveillance-would-help-contain-covid-19

[20] https://www.informatics-europe.org/news/541-policy-recommendation-covid19.html

[21] C(2020) 2296 COMMISSION RECOMMENDATION of 8.4.2020 on 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 general concept is to let two phones record their contact based on the intensity of the Bluetooth signal and its duration. The definition of the contact is calibrated to match as much as possible the epidemiological definition of a close contact, that may result in the virus transmission. For most of the solutions available, a "close contact" is defined by being in the distance for droplet transmission (2 meters) for 15 minutes or more. However, this definition is still debated and can be tuned by the solution operator.

Bluetooth-based solutions have the following advantages:

- Best match the epidemiological definition of a close contact;
- Have the potential to maximise privacy: solutions can be implemented in a vast range of ways: from fully anonymised and decentralised to centralised and nominative (see Section 3.1, 3.2, 3.3)
- Hence, they have received the support from the European Commission

2.3. The European and Worldwide context

The European Commission has issued recommendations for member states as well as provided them with a toolbox. With regards to these documents, (1) the use of Bluetooth-based solutions are encouraged, as opposed to geolocation-based solutions, (2) the potential benefits of the application should be weighted against the impact on privacy and GDPR should be respected, (3) a national authority should coordinate the project, (4) the key importance of interoperability is emphasised.

The Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT [22]) is a non-profit organisation based in Switzerland, initiated by Technical University München and supported by the Botnar Foundation. They provide an open-source code and guidelines of implementation for Bluetooth-based proximity tracing, in line with recommendation of the European Union. Countries willing to participate in the initiative have to contract with an implementation partner that is member of PEPP-PT. France, Italy, Switzerland and Spain are foreseeing solutions based on PEPP-PT, or its decentralised implementation protocol (DP-3T). In the meantime, though the German government had been considering the implementation of the centralised implementation of the PEPP-PT model[23] (of which Fraunhofer HHI research institute and the Robert Koch Institute public health body were to become key players), amidst privacy concerns and warnings from the expert community[24], Health Minister Jens Spahn and Chancellor's chief of staff Helge Braun announced on 26th of April 2020 that Berlin would switch to backing a coronavirus-tracing app using technology supported by Google and Apple that compiles data in a decentralised and completely anonymous fashion[25].

[22] https://www.pepp-pt.org/

[23] https://www.spiegel.de/netzwelt/netzpolitik/corona-app-jens-spahn-soll-sich-fuer-umstrittenes-pepp-pt-modell-entschieden-haben-a-25bcd0ce-0150-4d5d-b308-67395b767e5a

[24] https://www.ccc.de/system/uploads/300/original/Offener_Brief_Corona_App_BMG.pdf

[25] https://www.welt.de/newsticker/dpa_nt/infoline_nt/brennpunkte_nt/article207513283/Corona-App-nun-doch-mit-dezentraler-Speicherung.html

Apple and Google are providing one of the alternative frameworks for implementation. They have partnered to provide worldwide an application programming interface that health authorities may use from mid-May onwards to implement and launch their nation-wide proximity tracing application. The concept is similar to PEPP-PT but is embedded directly in the operating system, which can markedly facilitate the operations and decrease the risk of flaws (in particular with respect to Bluetooth background activation). Another advantage lies in the worldwide interoperability and scalability. However, the trust in tech giants in the population is not guaranteed and may affect the penetration of the solution in the population. Moreover, the data processing behind these solutions would need to be carefully examined in order to avoid a negative impact on privacy.

Asian countries were the first strike by the pandemics and experienced similar challenges in the past 20 years. As previously discussed, China and South Korea have implemented apps that rely on geolocation, and their usage in a European setting seem incompatible with privacy preservation rules and culture. Singapore, however, has open-sourced its mobile application "Blue-Trace" that uses Bluetooth technology to help public health authorities to perform contact tracing. This mobile application works in a similar way that the Apple-Google solution. In the Singapore implementation, the usage of the app is pseudonymous. Upon the first use of the app, a citizen is asked to register using only his phone number (and confirm it by SMS challenge). The "key" linking a phone ID to a phone number is accessible only by the health authority. The contacts are stored directly on the phone in an anonymised way. In the event of a positive test, health authorities provide the patient with an activation code that is entered in the app. Following that action, contacts of the patients are anonymously notified that they have been in contact with a positive patient and should isolate. At the same time, health authorities are notified and able to decrypt the phone number of the contacts and call them to support isolation. Of note, this type of implementation in which health authorities have access to the phone number of contacts is supported by the sanitary inspection in Luxembourg, as it integrates with the traditional workflow and allows for synergy between manual and digital contact tracing.

April 26th 2020 saw the official launch of an Australian app COVIDSafe as an additional tool to keep communities safe from further spread of coronavirus through early notification of possible exposure[26]. As at 10:00 PM 27 April (local time), about two million Australians were reported to have downloaded the app[27]. The government stated that for it to reach maximum effectiveness, about 40% of the population would need to install it. The app-based on the one employed in Singapore - requests users to supply their age range, a mobile number, a postcode and a name or a pseudonym[28]. It also generates an encrypted code unique to the user that health authorities can use to contact them if the need arises. The COVIDSafe uses a Bluetooth wireless signal to exchange a "digital handshake" with another user when they come within 1.5m. The app then logs this contact and encrypts it. Users will be notified if a more than 15-minute long close contact with another user who tests positive took place. The data will be wiped after 21 days or upon de-installation of the app from the phone[29].

[26] https://www.pm.gov.au/media/covidsafe-new-app-slow-spread-coronavirus

[27] https://twitter.com/ScottMorrisonMP/status/1254704596175294464?s=20

[28] https://www.bbc.com/news/world-australia-52433340

[29] https://www.health.gov.au/resources/apps-and-tools/covidsafe-app

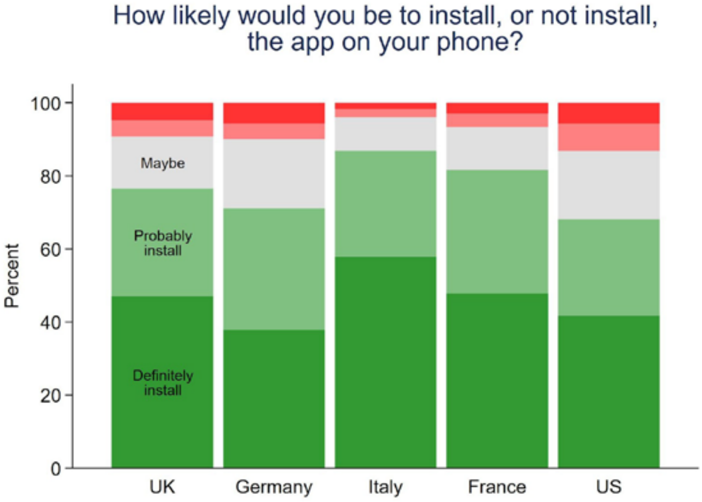
2.4. Acceptability of proximity tracing solutions

The COVID-19 crisis is a typical example of the impossibility of having one single global technological solution to a given problem. Acceptability of digital technologies has to be confronted systematically with cultural, moral, socio-political and religious backgrounds. With the priority given to a collective public health benefit and maintaining a local social order in this current emergency, digital measures may sometimes be found intrusive and can erode individual freedoms. Besides, even in countries like Luxembourg, a digital divide still persists today, and the digital approaches implemented could leave vulnerable populations behind. Digital solutions can be less frequently understood and used in people with a low health literacy level or specific subgroups such as minorities, older individuals, or those who live in rural or low-income areas.

Importantly, the effectiveness of any contact tracing app will depend on public support on first instance. Its acceptance will depend on whether the public perceives it as effective, accurate, privacy-protective and trustworthy, avoiding mass surveillance and strictly limited in time to the duration of this current situation. The app needs to be fit for this purpose, compliant with the current laws applicable and respecting values, rights and freedom of the EU.

In order to increase the acceptance, an integrated governance is needed based in a multidisciplinary approach (health, experts in data protection, authorities, academics, private sectors, …), to prepare and implement the measures.[30].

That being said, in neighbouring countries, a high percentage of acceptability has been observed (see Figure 1). For instance, a total of 8 out of 10 French citizens, for instance, would agree to download a contact tracing app that would use the Bluetooth Low Energy technology for proximity detection of nearby mobile phones. Along this high acceptance ratio, main fears concern data security, privacy and the use of such technology that persists after the crisis (avoiding the Big Brother effect).



[30] Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU toolbox for Member States.April, 14st 2020, Brussels. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

Figure 1: Acceptability for bluetooth-based proximity tracing in Western countries. Accessed from: https://osf.io/7vgq9/

2.5. GDPR and proximity tracing

Surveillance of the spread of the virus has become a major focus for health authorities. Digital technologies such as location-tracking and contact-tracing could contribute to contain the pandemic more quickly. But, those technologies raise significant concerns. In particular, they put at risk individual's privacy. The General Data Protection Regulation (GDPR) does not hinder the fight against COVID -19 outbreak. However, solutions that process personal data have to comply with the GPDR's provisions to be lawful.

"Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data, and in all cases, it should be recalled that any measure taken in this context must respect the general principles of law and must not be irreversible[31]".

To be compliant with GDPR, personal data processing activities have to comply with data protection principles set forth in Article 5(1).

- **Lawfulness, fairness and transparency**

Collecting and using personal data relies on an appropriate lawful basis. Even if the proximity-tracing app takes place on a voluntary basis, "it appears that the most relevant legal basis for the processing is the necessity for the performance of a task in public interest, i.e. Art. 6(1)(e) GDPR." It requires "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[32]."

To be fair, how the processing may affect individuals targeted by the app must be considered. "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[33]".

Transparency implies that all information related to the data processing is making available to individuals concerned.

- **Purpose limitation**

Personal data can only be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purpose[34]". It means that data collected by proximity-tracing solution must only be used to achieve the purpose of the processing operation. In addition, it must be of limited duration. Thus, once the COVID-19 crisis is over, proximity-tracing activity should not remain in use, and as a general rule, the data collected should be erased or anonymized[35].

[31] EDPB, Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020, https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[32] EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, OUT2020-0028, April, 14st 2020, Brussels

[33] EDPB, Guidelines 04/2020 on tue use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020.

[34] GDPR, Art. 5(1)(b)

[35] EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, OUT2020-0028, April, 14st 2020, Brussels

In addition, "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)[36]".

- **Data minimisation**

Personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed[37]". Thus, only data that are relevant to fulfil the purpose of the processing activity have to be collected. "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[38]". Thus, location tracking of individual users should be avoided.

"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.[39]"

- **Accuracy**

In comparison with manual proximity-tracing, automatic proximity-tracing will increase accuracy of data collected. Indeed, in manual proximity tracing, an individual is likely to either forget people he had been in contact with or not being able to identify whom he met.

"A mechanism should ensure that whenever a person is declared as COVID19-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".

- **Storage limitation**

Data collected have to be kept for no longer than it is necessary. In the context of proximity-tracing, retention period corresponds to COVID-19 maximal incubation period to which is added the necessary time for testing (1 month). After this delay, proximity- tracing data must be erased or anonymized[40].

- **Integrity and confidentiality**

Personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures[41]". This part will be discussed in the cybersecurity section

- **Accountability**

"To ensure accountability, the controller of any contact tracing application should be clearly defined[42]".

[36] EDPB, Guidelines 04/2020 on tue use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, GEN-2

[37] GDPR, Art. 5(1)(c)

[38] EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, OUT2020-0028, April, 14st 2020, Brussels

[39] EDPB, Guidelines 04/2020 on tue use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, DATA-5.

[40] EDPB, Guidelines 04/2020 on tue use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020

[41] GDPR, Art. 5(1)(f).

[42] EDPB, Guidelines 04/2020 on tue use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020.

Accountability provision focus on two main elements:

1) the need for a controller to take appropriate and effective measure to implement data protection principle;
2) the need to demonstrate upon request that appropriate and effective measures have been taken. It means that the controller is able to provide evidence of appropriateness and effectiveness of measures implemented.

Because contact-tracing application puts at risk individual's privacy, "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". Therefore, "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[43]."

In addition to compliance with data protection principles described above, it is necessary to guarantee individuals' rights. Under GDPR, individuals have the following rights: the right of access, the right to rectification, the right to erasure, the right to restriction of processing, right to object to processing, right to data portability, right to not be subject to automated decision making and profiling.

The rights available to individuals depend on the lawful basis of the processing. If lawful basis of proximity tracing is public interest[44], then the right to data portability is not available.

Due to COVID-19 outbreak context, some restriction to the right of rectification should be discussed given the importance of data accuracy in the context of COVID-19.

Importantly, if someone is informed of his/her proximity with a positive infected individual, the functional requirement that consists in "providing advice on next steps" should not 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[45]".

Finally, a data protection impact assessment (DPIA) must be carried out "before implementing such tool as the processing is considered likely high risk (health data, anticipated large-scale adoption, systematic monitoring, use of new technological solution)[46]". The EDPB strongly recommends the publication of DPIAs.

[43] EDPB, Guidelines 04/2020 on tue use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, GEN-4

[44] GDPR, art 6(1)(e).

[45] EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, OUT2020-0028, April, 14st 2020, Brussels.

[46] EDPB, Guidelines 04/2020 on tue use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020.

2.6. Cybersecurity and ethical considerations

Proximity tracing application is meant to run on smartphones. When a user, say Alice, goes out, the application broadcasts certain Bluetooth signals that will serve to "recognise" at a different level of anonymity Alice's phone; the phone receives similar signals from other people's phones close by that runs the application. Alice phone measures the strength of the received signals and determines whether there has been a close contact, enough to potentially transmit the virus. Alice's application keeps locally all those "close contact" signals, for a time that is usually aligned with the time for the symptoms to appear. It stores them in what we call a "close contact list", although it may not contain phone "contacts" as we usually think of them.

If, later on, Alice develops the symptoms and is found positive, the application allows, according to modalities that varies from one implementation to another, to get those close contacts registered on Alice phone to know that they have been potentially exposed.

All the available solutions differ because of the type and nature of the architecture that supports the applications, of the information carried by the signals that are shared and stored, and of the modalities in which Alice's close contacts, and Alice's as well, will be notified of being exposed to the virus. The architecture of the application which can be centralised (i.e., with a shared database of close contacts) or decentralised (i.e. with no such a thing but only lists stored in people phones). The close-contact lists can be anonymised (i.e. with no possibility to retrieve people's personal data, such as their phone numbers), pseudo-anonymised (i.e., with such a possibility), or nominative.

Depending on how proximity tracing application is designed and implemented, there are different risks and threats. Some are against personal data, others may be farther reached, as human rights.

About this latter, it is useful to reflect that the ethical consequences of an imprudent design, of a naive implementation, or of relaxed use of the proximity tracing technology can be quite severe. For instance, revealing to the public that one has been found positive and, e.g., responsible for having infected a lot of other peers while violating the quarantine, exposes the individual, a potentially vulnerable person, to stigmatisation e.g., to being referred as an anointer or a criminal. Social isolation and other repercussions, e.g., discrimination on the base of nationality or ethnicity, can potentially follow. Other significant human rights may also be endangered: people can experience loss of personal freedom and fear that freedom will never be restored.

On the other hand, it is undeniable that the potential utility of short-range proximity tracing application is promising: it enables to alert quickly and reliably whom might be infected because exposed to individuals tested positive; it promotes social awareness and cohesion by letting one's self-quarantine and seek for testing and assistance, fostering a communal effort to contain the epidemic and restore normality.

However, there are also limitations in what the technology can provide: viruses can be transmitted also via contact through infected objects, a sort of indirect and asynchronized proximity. Proximity tracing is oblivious about it. Proximity tracing also disregards whether users wear protections, which is a factor that instead delays the virus transmission; it may as well falsely report of two peers being in proximity when in fact, because of a wall, for example, there has been no such a close encounter. In short, proximity tracing as technology will have false positives, and false negatives and an accurate measure of how severe those measures are is missing and still matter of ongoing research.

Besides, proximity tracing is not an alternative to public health workers. As EFF states, proximity tracing "could not substantially help conduct COVID-19 contact tracing during a time like the present, when community transmission is so high that much of the general population is sheltering in place, and when there is not sufficient testing to track the virus. When there are so many undiagnosed infectious people in the population, a large portion of whom are asymptomatic, a proximity app will be unable to warn of most infection risks. Moreover, without rapid and widely available testing, even someone with symptoms cannot confirm to begin the notification process. And everyone is already being asked to avoid proximity to people outside their household "[47].

That said, it should not surprise that recently the literature has been generous in proposing quite a deal of different designs and of several implementations of the technology. From a data protection's perspective, the variety ranges from solutions which are privacy imprudent and invasive, to those which are computational theoretically privacy-preserving even against curious authorities.

Notably, on this matter a joint statement signed by "scientists and researchers from across the globe"[48] has been released to the media on April the 20th to advise that some "solutions" for contact tracing may result in systems which would allow unprecedented surveillance of society at large. The document reports that "we [scientists and researchers, ed.] urge all countries to rely only on systems that are subject to public scrutiny and that are privacy preserving **by design** (instead of there being an expectation that they will be managed by a trustworthy party), as a means to ensure that the citizen's data protection rights" . A list of design principles, we can say of desired security features, follows.

The successful adoption of a proximity tracing solution for a specific social goal, for instance, to relax the lockdown policy while avoiding falling back into an epidemic, depends on those security features but not only. The literature is generous in giving examples of theoretically strong protocols which people fail to use; and attacks can be successful not only because of some vulnerability in the security but because of a clever way to exploit ambiguities in graphical interfaces or because of tricks which take advantage of people's psychology and their interaction with the technology.

To facilitate a choice of an application that can fit better a certain social and political strategy to mitigate an epidemic, we compare different designs and implementations of proximity tracing; we discuss the related risks both from cybersecurity and an ethical standpoint. We

[47] https://www.eff.org/deeplinks/2020/03/governments-havent-shown-location-surveillance-would-help-contain-covid-19

[48] The original document is available here: https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view

highlight the threats. Where possible, we include a discussion about the presumption of compliance with specific principles of the GDPR.

Centralised vs non-centralised close contact list database. The choice is about whether to keep a central database of people's close-contact lists or not. The difference is that, in a centralised architecture, there is an authority in charge of the database; the database becomes a single point of failure in case of an attack or in case of a curious authority interested to know more than it should from the database. The risk for invasion of privacy varies depending on the information stored in the database e.g., on whether it is possible to retrieve the identities of people, their phone numbers, or on whether the database (called public reading list in this case) contains only anonymised seeds from the close-contact list of who has been found positive. In this latter case, users (i.e., their application) query regularly the database to deduce, them only, if they have been exposed.

A non-centralized, i.e., a decentralised, solution leaves instead to the application of the person tested positive the task of informing the phones in its close-contact lists in a peer-to-peer or peer-to-peers fashions. Here, the identity of the person found infected risk to be revealed to the peers, unless precautions are taken.

Anonymised vs pseudo-anonymised close-contact list. Here the choice is about the nature of the information shared and stored in the close-contact list. Choices in this matter are critical for privacy.

And app can share only fully anonymous random numbers generated in such a way that only the app which generated them can recognise them as its; no one else can associate those numbers with a phone or with the identity of its owner. In this case, the risk of re-identification is small, only relying on the robustness of the random generation functionality and on the anonymity of the communication protocols used to share them. Proving the integrity and the reliability of the data and their sources can be hard and advance cryptographic techniques have to be in place to achieve a high quality of data and privacy.

Alternatively, a pseudo-anonymisation list can be kept. This allows re-identification, i.e., to link the numbers exchanged during a close encounter with an identity, ultimately of the owner of the phone which has sent them. Implemented in a centralised architecture, the use of pseudonyms exposes people's identities. Even if protections can be in place, e.g., controlling access to the database, there are risks of abuses and, in case of data leakage, of exposure. It is today's news, RTL News reports [49], that "a data breach was found in the corona app Covid19 Alert. The app is one of the seven possible corona apps for the Netherlands and was presented this weekend to the Ministry of Health, Welfare and Sport." Covid19 Alert, the news says, keeps a database of users of the app.

Data collected / broadcasted (anonymised vs pseudo-anonymised). Even if the data shared to inform about a potential exposure are anonymised, an application can store other metadata, e.g., time and location, and associate them with the shared data collected during a close encounter. Such metadata that can later be potentially used to re-identify a phone.

[49] https://www.rtlnieuws.nl/tech/artikel/5095321/covid19-alert-datalek-crypto-digibyte-coronavirus-ministerie-app

This threat comes mainly from the application and can be minimised if the code is let open to public scrutiny.

Explicit vs implicit consensus of sharing. According to the GDPR, people should be informed of the consequences of using proximity tracing applications. Who has been positively tested may be asked to share the close-contact list to public health officials, and the decision can be let to him/her only; or it can be forced to do it (e.g., the application can share the data automatically). Proximity tracing application can keep all the close-contact information within the phone and protect them even in the case the phone is lost. The history of close contact can be regularly deleted when it became obsolete. All such choices will determine the level of intrusiveness that authorities have on the individuals and the risk of disclosing, outside, the identity of the persons found positive; ultimately, the choice of the consensus experience leads to a different degree of public trust or distrust into using the application.

It is important to emphasise that the current approach already makes a tradeoff between the privacy of a positively tested individual and the benefits to society.

Threats (adversaries). We comment briefly of the adversaries that can threaten a proximity tracing solution. Whenever the choice is in favour of a centralised architecture and with a database of pseudonyms, there is the risk of having a curious authority (as an entity, as a collective of individuals) taking advantage of it. The database will remain as a single point of privacy failure for the time of crisis and beyond. And it is exposed to attack from hackers interested to steal and exploit that sensitive information or to launch denial of service attacks or ransomware attacks, with extortion purposes. Hackers can also compromise the application e.g., in revealing the close-contact list, but this threat is not more serious than the usual risk of being infected by malware.

The references in footnotes were used for this discussion[50,51,52,53].

[50] PACT: Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing, Justin Chan1, Dean Foster, et al, arXiv:2004.03544v3 [cs.CR] 17 Apr 2020

[51] Decentralised Privacy-Preserving Proximity Tracing Version: 12th April 2020. Contact the first author for the latest version. Carmela Troncoso, et al., DP3T Distributed privacy-preserving contact tracing.

[52] Anonymous Collocation Discovery: Harnessing Privacy to Tame the Coronavirus
Ran Canetti, Ari Trachtenberg, Mayank Varia, arXiv:2003.13670v4 [cs.CY] 3 Apr 2020

[53] BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders Jason Bay, Joel Kek, Alvin Tan, Chai Sheng Hau, Lai Yongquan, Janice Tan, Tang Anh Quy Government Technology Agency Singapore

3. Considerations and recommendations for Luxembourg

3.1. Integration in the healthcare system, architecture choice (centralised vs decentralised, anonymous versus pseudonymous)

Health authorities are usually in charge of traditional contact tracing. In Luxembourg, that is the role of the sanitary inspection. Based on discussions with collaborators of the sanitary inspection, an outline of the process is presented here:

- Positive PCR lab results are sent daily with nominative contact information, by a data flux centralised by the national eHealth agency,
- Positive patients are contacted over the phone, their diagnosis is explained, as well as the quarantine and the follow-up procedure,
- Contacts of the positive individual during the infectious period are investigated over the phone,
- Contacts are contacted over the phone and isolated. Unfortunately, we were not able to ascertain if a test is currently recommended or not.

The sanitary inspection has expressed its preference towards a digital system integrated with its existing processes. In order to facilitate their work, they would like to have access to contacts' phone numbers of positive individuals, directly on their existing work interface. With that particular type of implementation, they could ensure the same level of quality for the isolation procedure while working more efficiently (decreased time) and effectively (better quality of contact tracing).

This type of implementation would necessitate a pseudonymised and partly centralised architecture. Unfortunately, we can't report here on the necessary staff to operate such a system, as we would need further inputs from the sanitary inspection.

A similar implementation, TraceTogether, has been chosen by Singapore's Government Technology Agency and implemented. BlueTrace, the privacy-preserving protocol that underpins TraceTogether, as well as OpenTrace, a reference implementation has been described in detail[54]. The CNIL, in France, has also commented on the legal base that withstands a similar solution, called StopCovid[55].

Germany, on the other hand, after having considered the same approach, seems to be decided for a decentralised one, like Switzerland. This can be explained because cases are declared 4 to 5 days to the central authority in Germany, preventing the implementation of an integrated system.

We will now consider 2 different options of implementation and how they could integrate in the already existing contact tracing and follow-up activities of health authorities:

- Partly centralised and pseudonymous

[54] https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf

[55] https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf

- Decentralised and anonymous

Based on the needs expressed by the sanitary inspection, a partly centralised and pseudonymous use-case could look like:

- The government advertises the application.
- A citizen downloads the app from the stores (Apple / Google) or via a QR code, and
- He reads a brief information document about the finality of the app, data processing and his rights +/- gives his consent for the usage of the app.
- Upon first connection, the citizen register using his phone number (verified by an SMS challenge).
- The association between a phone ID and a phone number is recorded on a server owned by the health authority with the highest cyber-security standards.
- The citizen goes on with his life, and contacts with other citizens are recorded **anonymously on the phone**.
- In the case the citizen is tested positive, the laboratory sends the positive test with the citizen's contact detail to the sanitary inspection, and the sanitary inspection call him back to support quarantine and start the follow-up (this process is already operational today).
- In addition, the sanitary inspection provides the newly diagnosed patient with a code that allow him to enter his "positive status" in the app.
- The app asks for permission to anonymously notify the contacts whom the app has recorded as being in proximity with the patient. If authorisation is given, notifications are sent.
- The app also asks for the authorisation to share contact history with the sanitary inspection.
- If yes, the sanitary inspection has the possibility to decrypt contact and retrieve phone numbers.
- They can then call back the contacts to inform them about what to do.

With the alternative (decentralised implementation), the use-case could be the following:

- The government advertises the application.
- A citizen downloads the app from the stores (Apple / Google) or via a QR code.
- He reads a brief information document about the finality of the app, data processing and his rights +/- give his consent.
- No registration is needed
- The citizen goes on with his life, and contacts with other citizens are recorded **anonymously on the phone**.
- In the case the citizen is tested positive, the laboratory sends the positive test with the citizen's contact detail to the sanitary inspection (already the case now), and the sanitary inspection calls him back to support quarantine and start the follow-up.
- In addition, the sanitary inspection provides the newly diagnosed patient with a code that allows him to enter his "positive status" in the app.
- The app then asks for the permission to notify contacts anonymously that they have been in contact with a positive individual and what to do.
- Contacts are anonymously notified that they have been in contact with a positive individual and are advised about what to do.

When comparing the two possible types of implementation, the pseudonymous and centralised mode allows for a clear integration of traditional and digital contact tracing processes. Accordingly, sanitary inspection teams could work more effectively and efficiently while ensuring the same level of quality for the isolation procedure. Also, false-positive generated by the app (for instance, contacts through a wall) could be identified, avoiding unneeded isolations of individuals. This implementation would be in line with the EDPB's recommendation that the isolation process should not be fully automated after proximity is detected by a digital system[56]. With regards to privacy and cyber-security, this solution presents a single point of failure. The probability this risk will realise can be minimised by applying high-standard cybersecurity guidelines. The maximal impact would be a list of contacts associated to phone numbers.

On the other hand, the decentralised and anonymous implementation would maximise the privacy and decrease the cybersecurity risk. Indeed, this solution presents no single point of failure, and so the maximal impact in case of a successful cyberattack would be a leak of anonymous contact of one individual. However, the effectiveness of such solutions is not proven, and amongst experts, there are serious concerns that they can effectively induce an isolation behaviour without an enforcement by health authorities, such as described above. Indeed, it would be easy to ignore an anonymous notification on a phone. Moreover, false positives could not be managed, inducing unnecessary isolations and, most probably, a lack of trust in the system.

Most importantly, in both cases, GDPR and legal compliance can be achieved (see section 2.5. and 3.6)

The following Table 1 summarises the pros and cons of each approach:

[56] EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, OUT2020-0028, April, 14st 2020, Brussels.

	Pros	Cons
Pseudonymized, partly centralized	Integrated and synergistic with the already existing traditional contact tracing and follow-up. Expert opinion suggests this implementation as more effective. False positives can be managed.	Pseudo-anonymity, especially if paired with data centralization, is vulnerable to privacy leakages. There is a single point of failure. A successful cyber-attack can expose sensitive information (contacts + phone numbers of positive individuals and their contacts). The probability of success of a cyber-attack depends on cyber-security measures in place.
Fully anonymised, decentralised	Offer better large-scale privacy protection, as there is no single point of security failure (and thus no potential leak of sensitive information).	Experts express serious doubts about the effectiveness in inducing isolation behaviors A cyber-attack, a malware, can still compromise a phone; the likelihood of this happening is that of a malware infection. It is not synergistic with the already existing manual tracing.

3.2. Modality of contact tracing, interoperability, openness of the code

Based on facts presented in Section 2.2, the group unanimously recommend the use of a solution based on Bluetooth low energy.

As stated by EDPB[57], the source code should be made publicly available for the widest possible scrutiny by the scientific community. In addition, by making the code source publicly available, it will contribute to increasing transparency towards users.

"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[58]."

The group unanimously recommend that the solution should be able to operate in a cross-border manner, especially with neighbouring countries. International coordination, at least at level of the Grand Region, is recommended.

3.3. Choice of the framework

The choice of the implementation framework is more prone to debate. We here summarise the pros and cons of potential implementation frameworks. DP-3T was the decentralised implementation protocol of PEPP-PT, now standing alone.

Framework	Pros	Cons
PEPP-PT (Of note, DP-3T was the decentralised implementation of PEPP-PT, now standing alone)	Inter-operability (supported by some European countries and the academic sector). Trusted (academic initiative) Flexibility Partner of APSI.lu / DIGITALEUROPE	Stability (recent division amongst founders) Sustainability, scalability, support (a decentralised academic initiative raises concern about the durability, scalability and support of the solution)
Apple / Google	Scalability and interoperability (Worldwide initiative, supported by some European countries) Sustainability, stability, support Flexibility	Trust (sensitive data operated by tech giants) Lack of penetration (the population may be sceptical and not use the app)
Blue Trace (Singapore)	Solution already implemented Feedback from users and health authorities available The implementation use-case matches the wish of the Luxembourgish sanitary inspection	Inter-operability (European countries support PEPP-PT so far)

[57] EDPB, 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

[58] EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, OUT2020-0028, April, 14st 2020, Brussels.

Other Asian framework (China, Taiwan, South-Korea)	Solution already implemented Feedback from users and health authorities available	**Based on Geolocation; too much concerns about privacy, likely to be unlawful.** Trust may be a concern (similar to Apple / Google)

3.4. Modality of consent collection

While the legal basis of the processing operation is "public interest", the installation of the app installation should be consent based[59]. Accordingly, users should be provided with complete and clear information on the intended utility of the application, data collection, processing and storage as well as participants' rights.

Based on recommendations from the EU Commission, consent should also specifically be sought before:

- installing and use the application (collect phone number details)
- sending anonymous notifications to contacts,
- sending information to the health authorities.

More generally, the information displayed should be intelligible, adapted to small screens and available at least in Luxemburgish, French, German, English and Portuguese.

3.5. Data collection, processing and storage

The data collection processing and storage will depend on the implementation variant that is chosen (see section 3.1, 3.2, 3.3).

The EDPB underlines that "the decentralised solution is more in line with the minimisation principle".

Moreover, 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, that is, as soon as there is no valid reason to retain it. In principle, the storage period should not exceed the maximal duration of the incubation period plus the time needed for a patient to be tested. The EDPB strongly supports 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.

In case a centralised component is used, and because of the nature of the information stored, the group recommends data storage in Luxembourg on state-owned servers with state-of-the-art cyber-security and business continuity.

[59] Common toolbox for Member States, SG-02

In order to conform to the GDPR, the patient should have the right to access and suppress his data at any time.

3.6. Legal frame in Luxembourg

As advised by the EDPB, proximity tracing application should be considered as "necessary for the performance of a task carried out in the public interest[60]". Declaration of such public interest is the responsibility of public authorities. Note, however, "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[61]".
"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 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[62]".

Appropriate communications activities should be carried out "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[63]".

In accordance with EDPB's guidelines on the use of location data and contact tracing, it is required to determine which public authority will be responsible for the processing operation - controller[64]. It is unlikely that controller processes data itself. Accordingly, a standard processor agreement with public and private organisations will process data on behalf of the controller - processor [65] - is required. In addition, the appointment of a Data Protection Officer, with adequate qualification qualifications, resources and power for exercising its supervisory function adequately, is required[66].

In addition, EDPB recommends making the application in an accountable way. It means that privacy measures put in place are appropriate, effective and documented[67]. It also states

[60] GDPR. Art. 5(1)(e)

[61] EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, OUT2020-0028, April, 14st 2020, Brussels.

[62] EDPB, 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.

[63] EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, OUT2020-0028, April, 14st 2020, Brussels.

[64] GDPR, Art. 4(7)

[65] GDPR, Art. 4(8)

[66] GDPR, Art. 37; Art.38; Art. 39

[67] GDPR, Art. 5(2)

that data processing shall be documented with a data protection impact assessment - DPIA[68]. Finally, it reminds that data protection by design and by default shall be implemented[69].

It is essential to consult with Commission Nationale pour la Protection des Données (CNPD) to ensure that personal data is processed lawfully, respecting the rights of the individuals, in accordance with data protection law.

According to legal experts Prof. E. Poillot, University of Luxembourg, specialists of users' profiling and Prof. G. Resta as well as V. Zeno Zencovich, University of Rome 3, both specialised in data protection (Prof. Resta sits in the Study Group on the legal and ethical implications of COVID-19, established within the Italian Higher Institute of Health), the application system such as described in Section 3.1 guarantees the respect of the social values and fundamental principles governing liberal democracies. They evaluated the system as GDPR compliant as it respects the fundamental data protection principles set forth in Article 5(1), lawfulness, fairness and transparency, purpose limitation, data minimisation, integrity and confidentiality, accuracy and accountability. Also, they have validated our concrete proposals regarding the processing of data to ensure a free and informed consent and concerning the key issue of storage limitation, suggesting that a maximum storage period of one month should be the principle. In the view of the legal experts, the system proposed also guarantees the respect of fundamental rights. The experts assessed the legality of the proposed application system with the existing national and EU regulations and also relying on the various recommendations already published by the European Union and the Council of Europe (Regulation (EU) 2016/679 (GDPR); Working Party Act 29, Guidelines on consent under Regulation 2016/679, WP259 rev.01 Directive (CE) 2002/58 on privacy and electronic communications; Conseil de l'Europe, Information Documents SG/Inf(2020)11, Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis A toolkit for member states, 07/04/20 ; Commission recommendation on 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 C(2020)2296 final of 8/04/20; Avis du Président du Comité Européen de la protection des données en date du 14 avril 2020, réf. OUT2020-0028 ; E Health Network: Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States Version 1.0 15.04.2020; Communication from the Commission Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection C(2020) 2523 final of 16 /04/20; European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak, 19/03/20).
They reach the conclusion that the system can be implemented as described and suggest the passing of a law in the forthcoming months, which would allow to clearly frame the use of the tracking application but would also send a clear signal of the importance granted by the government and the legislature to the respect of data protection principles and fundamental rights in the context of the current crisis context (see the legal opinion of the experts annexed to this document).

[68] GDPR, Art. 35

[69] GDPR, Art. 25

3.7. Additional functions

Proximity-tracing is only one amongst many functionalities of a mobile application that could support the exit from the lockdown. Based on the scoping review presented in the State-of-the-art Section, the EU recommendation, insights from stakeholders and a design thinking exercise realised by the scientific advisory group, the following features could be of interest (and lower risk):

- Access to up-to-date and verified information provided by the Ministry of Health.
- Symptom checker: guiding patients about what to do based on their symptoms and personal medical history.
- Research participation: having the possibility to be informed about available research initiatives and enrol, fill-in questionnaires and share health data.
- Dynamic consent management and settings: manage at any time the authorisations of the application, suppress data, dynamically manage consents for (1) the main use of the app, (2) participation to research.
- For the sanitary inspection, having the possibility to identify super-transmitters and contact them.

3.8. Acceptability

For all the reasons described in Section 2.4, a proximity tracing app for COVID-19 is expected to be received in very different ways by the population, or at least by some specific sub-groups. As acceptance and penetration are key for an optimal public health benefit, we highly recommend conducting a national survey among Luxembourgish residents prior to the launch of any digital solution. This will help to better understand the leverages and barriers in the population, as well as the different citizen profiles and their associated attitudes, perceptions and beliefs with respect to such digital solutions. It will help the government to adapt its strategy and maximise the likelihood of reaching the needed critical mass of users for efficiency. Such a survey will provide key figures to rely on at the time of the app launch and to adapt the wording and communication. The WP05 is ready to initiate or advise the government for such a study as soon as it needs it. A questionnaire has already been designed and can be shared with the government upon request for review/validation.

4. Options to move forward

We here propose several key questions to decide how to move forward (or not) with proximity tracing.

4.1. Is digital proximity tracing necessary?

As presented in section 2.1, digital proximity tracing seems complementary to and synergistic with manual contact tracing, particularly in the context of COVID19. However, one option could be to increase the staff of the sanitary inspection and stick to manual contact tracing. To evaluate the feasibility of this option, the following numbers would be needed:

- Number of workers dedicated to contact tracing at the sanitary inspection.
- Mean time to isolation after a positive test.
- Mean necessary time to perform a contact tracing.
- Numbers of people that could be hired.
- Necessary time for training new workers.

4.2. If yes, what strategic orientations should we take?

- Proximity tracing only versus other functionalities (see section 3.7)
- What architecture and implementation framework (see section 3.1., 3.2., 3.3)
- Integration with health authorities workflow or not (see section 3.1)

4.3. Beauty contest or other simplified tender procedure

If the government decides to move forward, the recommendations of this document and the strategic orientation chosen could serve as a basis for a simplified tender procedure, for instance a beauty contest.