EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS
60 YEARS 1960 - 2020

Council of Bars and Law Societies of Europe
The voice of European Lawyers
Rue Joseph II, 40/8 - B-1000 Brussels
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

CCBE Statement on Covid-19 contact tracing apps

15/05/2020

The Council of Bars and Law Societies of Europe (the CCBE) represents the bars and law societies of 45 countries, and through them more than 1 million European lawyers. The CCBE responds regularly on behalf of its members on policy issues which affect European citizens and lawyers.

With this statement the CCBE wishes to voice its concerns and set out a number of principles that need to be upheld when governments and private actors turn towards using contact tracing apps as a component in a wider programme of infection limitation and control of the Covid-19 pandemic.

The following statement is based on the findings set out in the CCBE considerations on the use of Covid-19 contact tracing apps, which is annexed below.

The CCBE acknowledges the imperative upon national governments to protect the health of their citizens and urgently to limit the spread of infection. It notes that national governments throughout Europe are introducing or proposing to introduce contact-tracing apps as a means of doing so, but also notes that the use of such apps is likely to constitute an infringement of fundamental rights, including the right to privacy and the right to limitation of the processing of personal data. Such infringements can be acceptable only if justified on the basis of proportionality.

The CCBE therefore asserts the following ***principles***:

1. No contact tracing system should be deployed otherwise than in accordance with the **rule of law**;
2. No contact tracing system should be *based upon* the collection by state authorities of mobile traffic data or other forms of geolocation data and no contact tracing app should *collect* such data other than in a manner which is fully justified on public health grounds, and which is open, transparent and with the explicit consent of the user;
3. The operation of any contact tracing app should **respect fundamental rights** and should be **proportionate**. In particular, it should be both in accordance with law, and demonstrably necessary in a democratic society to ensure the protection of public health;
4. The operation of such an app should respect the provisions of the **General data Protection Regulation** (GDPR), and, in particular, should operate in conformity with the principles of data processing specified in article 5 of the GDPR;
5. The basis upon which such an app operates and the manner in which it collects and stores data should be open and **transparent**;
6. There should be **no mandatory requirement** upon citizens to install or use such an app, nor should there be provided such inducements as might lead to a relative disadvantaging of those who have chosen not to install and use the app;
7. The operation of the app should be under the **control of the user** and its operation should be capable of being temporarily **paused** or the app **uninstalled** by the user at any time;
8. Appropriate steps should be taken to enable a facility for the user to exclude the collection of personal data where that data concerns the fact and circumstances of a meeting between a

citizen and a lawyer and where that meeting is or may be protected by **Legal Professional Privilege or professional secrecy**;

9. The data collected should be **processed by the relevant health authorities only**, and should not be available to any other body or agency;
10. The exercise of the liberty to cross a national or other border should not be contingent upon the downloading, possession or operation of a contact tracing app;
11. Appropriate provision should be made so as to ensure that the operation of the app and the storage and processing of personal data is **discontinued** and all databases containing personal data (including pseudonymised personal data) is **destroyed** when the emergency ends;
12. Insofar as the use or operation of the app may be governed or facilitated by emergency powers, the legislation authorising the emergency powers should contain an appropriate **sunset clause**.

In furtherance of these principles, the app should conform to the following ***minimum requirements:***

- The contact tracing system as a whole should respect the principle of **data minimisation**, and the collection and processing of personal data should be demonstrably justifiable for public health purposes;
- In particular, the **purpose** for which the data is collected and processed should relate exclusively to contact tracing for the purposes of control of infection within the framework of the Covid-19 pandemic and any mutation of the virus;
- The app should not cause the collection or processing of any data that is not required for the purposes of contact tracing;
- Before being launched the app should be the subject of a full **Data Protection Impact Assessment**;
- The source code of the program should be made available for **independent verification** as to its effectiveness and security, whether by an independent body or by publishing the source code;
- The app should be **continuously evaluated** for its effectiveness and compliance with fundamental rights and relevant data protection obligations and should be updated when required;
- The app should be able to be **uninstalled** at any time without leaving a trace;
- The app should be designed so as to enable users to choose whether or not to transmit data concerning their own infection;
- To that end, **access to the data** should not be available to other than the relevant public health authorities. Both technical and legal controls should ensure this limitation of purpose and of access;
- Personal data (including pseudonymised personal data) should be **retained for no longer than is required** for the purpose for which it was collected, with such data being deleted - preferably automatically - as soon as they are no longer needed for the purpose of control of the Covid-19 virus;
- It is ***recommended*** that, in developing contact tracing apps, national authorities seek, so far as is feasible, to ensure the interoperability of such apps with the apps used in other States, including neighbouring States.
- It is ***recommended*** that the relevant national data protection authority is given the opportunity to examine the software and administrative and other procedures associated with the app, to

verify proportionality and compliance with the data minimisation principles, before the app is made available to the public.

ANNEX: CCBE considerations on Covid-19 Contact Tracing Apps

ANNEX: CCBE considerations on Covid-19 Contact Tracing Apps

1. Introduction

As the realisation dawns around the world that Covid-19 is not likely to be eliminated any time soon, and as the economic damage caused by a near-total cessation of economic activity is becoming increasingly apparent, governments are looking for ways to resume some semblance of normal life, albeit talking, rather, of the "new normal".

From a public health perspective, there are several preconditions for the removal of severe lockdown measures, the most significant, for the present discussion, being: first, that the transmission rate has been brought significantly down; second, given the high transmissibility of the disease, there is put in place a robust contact tracing regime enabling those who have been in contact with an infected person to be traced and quarantined. For the last condition to be satisfied, there requires to be an extensive testing regime (so that it is actually known who may be infected) and a means of tracing contacts.

In relation to the testing regime, it is unlikely that universal testing of an entire population would ever be capable of implementation – not least because tests provide only a picture of the situation at the time of testing. The process of contact tracing is nothing new. It has been used in infectious disease outbreaks for well over a century, and most states, as part of the implementation of their respective public health policies, are able to implement manual processes of contact tracing facilities. These processes can be successful, but they are far from perfect – consider the example of an infected person taking a journey by public transport in a large city: not only will that person not be able to remember everyone with whom he came into contact, but, indeed, he will not even know who they were. For this reason, governments are contemplating the use of contact tracing apps, to automate the task of contact tracing, either in substitution for, or in conjunction with traditional manual means of contact tracing.

If it were sought by a state to make the use of contact tracing apps compulsory so as to (it might be argued) ensure that contact tracing is as widespread and effective as possible, then this presents an immediate, immense challenge to the fundamental right to privacy, and would struggle for public acceptance. Not the least of the problems would be how to compel the use of the app by a person who does not have (and, it may be, does not wish to have) a mobile telephone. On the other hand, a voluntary system would be likely to have a lower take-up, thereby limiting further the utility of the app, but, if "soft" encouragement is used to promote the use of apps, such as, for example, requiring the app to be active before entering certain premises, or using public transport, that has enormous consequences for civil liberties.

However, the debate about the use of apps should acknowledge that contact tracing apps can never be completely successful, first, because of the inherent weaknesses in any regime of contact tracing (as discussed above) and, second, can never be universal – not everyone has a mobile phone, or has a mobile phone equipped with Bluetooth, which they have with them, which has not run out of charge and is switched on.

These observations are made at the outset, as the debate over the use of apps is often conducted in black and white terms, based upon the easy, but false, assumption that contact tracing apps act as a panacea. It is widely acknowledged in public health circles that contact tracing apps, if used, should be used alongside, and assist, traditional manual methods of contact tracing.

That said, the perfect should not be the enemy of the merely good, and one can see from practical experience in Asia that apps can make a significant contribution to infection control. The question, rather, is whether paying the price in civil liberties and fundamental rights for the acquisition of that contribution is, in reality, a Faustian bargain.

2. Fundamental rights – The legal context

The collection of data by an App raises concerns both in respect of data protection law, and, more broadly, in relation to rights for respect for private and family life under the European Convention on Human Rights (ECHR) article 8 and under article 7 of the European Union Charter of Fundamental Rights and Freedoms as well as rights for the protection of personal data under article 8 of the European Union Charter.

So far as article 8 of the ECHR is concerned, the right is not absolute:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

In the present context, the use of an app, and conceivably, the compulsory use of an app, could be justifiable on the ground of protection of health, and, conceivably, in the interests of economic well-being (enabling the phased reintroduction of economic activity), so the question becomes one of proportionality. It will be recollected that there is a double test – not merely "necessary" but "necessary in a democratic society". Thus, it may be difficult to justify egregiously invasive measures such as those which had been adopted in China, but, as ever, the problem is one of where to draw the line.

Less obviously, ECHR article 6 might be engaged in certain cases. The fact that a particular person had consulted a particular lawyer at a particular time at a particular place is, itself, capable of protection under legal professional privilege (LPP) and professional secrecy. Insofar as an app might record data concerning such a fact, that could constitute an infringement of article 6 rights. However, the same proportionality issues could not be used to justify such surveillance as arise in connection with article 8 rights, since article 6 is unqualified. LPP/Professional secrecy trumps public health.

Under the General Data Protection Regulation (GDPR), the personal data collected would be special category personal data under article 9, which, under article 9(2) enjoys enhanced protection and may be processed only if (reading short):

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of 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;

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies."

Where the processing of special category personal is permitted under article 9(2), the processing also requires to fulfil the obligations under Article 6 of the GDPR as well as being consistent with the general principles of processing personal data as laid down in Article 5 of the GDPR.

In particular, Art. 5(1)(c) states that personal data shall be

"(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')."

In addition, Article 25 requires the implementation of data protection by design and default. This entails that only personal data which are necessary for each specific purpose of the processing should be processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

3. Finding the balance

As mentioned above, a balance requires to be found between, on the one hand, the positive effect on public health arising from the use of contact tracing apps, and, on the other hand, the degree of intrusion into fundamental rights arising from the use of such apps.

(a) Public health

In the discussions conducted in relation to this paper, one delegation referred to the problems associated with the use of an app where (as the consensus stands) the use of such an app is voluntary, all as discussed above. The delegation pointed out the real risk that an ineffective, or, at any rate, sub-optimally effective app could even be counter-productive as engendering a false sense of security, encouraging people to take unwarrantable risks. The delegation asked the question: "is it really necessary to create an app that has little chance of working, to allow the Government to show that it is doing something?"

The answer to that question as it is stated is self-evident, but the premise that an app has little chance of working may be unduly pessimistic, as such evidence as exists tends to support the view that, although not a complete solution, contact-tracing apps have a significant role to play as part of a wider contact-tracing and infection control regime.

(b) Centralisation of database?

A related issue is whether contact tracing apps should store personal data locally on the devices on which the app is loaded (a distributed model) or on a central database.

Some commentators, and at least one of the delegations contributing to this paper, expressed concern over the use of a centralised database, not least because a distributed app embodies privacy by design better than a centralised app is capable of doing. If one looks at European Governments, most are opting for the distributed data model, with France and the United Kingdom currently favouring a centralised database in England (though with the devolved governments in Scotland, Wales and Northern Ireland each respectively still considering their own solutions). Germany, which had also been developing a centralised database model, changed at a relatively late stage to a distributed model. When one comes to assess the balance of public health with fundamental rights, if all centralised and all distributed models produced substantially the same public health outcome, then it is arguable that the use of a distributed model would be more proportionate.

However, the reality is that there is potentially available a large diversity of apps, some decentralised and some using a centralised database, but each programmed in different ways, each with a range of

functionality, each deployed in a different manner and each subject to differing administrative regimes. As a result there is a diversity of public health outcomes from the use of contact tracing apps and it becomes difficult, at the level of generality, to assert that the adoption of one type of app will necessarily achieve a better balance between safeguarding public health and intrusion upon privacy than the adoption of another type of app.

Indeed, in its *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*[1] (adopted on 21 April 2020) the European Data Protection Board stated (at paragraph 42):

"Implementations for contact tracing can follow a centralised or a decentralised approach. 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."

In these circumstances, although anxious consideration might need to be given to the privacy and data protection compliance of a specific app, it is not really feasible to express a view, in the generality, on whether a centralised database or a decentralised model is preferable, beyond the self-evident observation that, with a centralised model, there is a heightened importance in ensuring the security of the central database, since not only would the hacking of the database constitute of itself a gross intrusion on privacy rights, but also, unless the public could be satisfied that rigorous security measures were in place, the mere risk of hacking might undermine public confidence and lead to a lower take up of the app. In any event, given that some governments are in fact adopting centralised models, the key consideration is to formulate an approach which sets out minimum standards to ensure proportionality, whatever model of app is adopted.

As the legal provisions set out above demonstrate, it is possible in appropriate circumstances to justify the use of a contact tracing app (whether centralised or distributed) consistently with ECHR article 8, provided that its use respects the requirement of proportionality. This might be achieved by strictly delimiting the purposes for which the data is gathered, prohibiting any other use, and, organisationally, ensuring that the data is stored specifically within the public health system. Such a regime could also potentially be GDPR compliant.

(c) The danger of Mission Creep

The creation of an extensive and unprecedented surveillance apparatus in order to fulfil a necessary public health aim presents an enticing temptation for a state to engage in mission creep – in the sphere of public health, extending the app to track influenza, or outbreaks of food poisoning, or to make the data available beyond the public health sphere, so as to enable surveillance by intelligence or law enforcement bodies, or, possibly in some states, to use the data to engage in wholesale interference with fundamental rights such as the right to free speech.

These concerns are not illusory. The example of the use made of surveillance data (with a system of "green and red flags") in China is well known, but a further example closer to home is the surveillance mechanism introduced in Israel[2]. There, surveillance is being used to track and trace virus infections – so far, so acceptable – but there are two extremely concerning aspects to this. The first is that, instead of an app, the state is using other and more insidious surveillance mechanisms, in particular, the gathering of mobile location data from mobile telephone operators and, second, though being, indeed, used for tracking Covid-19, the surveillance is being undertaken by the Shin Bet, the Israeli intelligence agency.

1 See https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

2 See https://www.bbc.co.uk/news/world-middle-east-52579475

It is essential to the creation of electronic means of contact tracing which are proportionate that their use is voluntary and that the apps do not, for their operation, require non-consensual access to location data obtained from mobile communications traffic data. This does not mean to say that an app should never be able to transfer location data, but if an app is to be capable of doing this, it must be done openly, transparently and with the consent of the user, who must be given the option to prevent the transferring of such data. The deployment of covert means more usually used by intelligence agencies can never be acceptable.

It is one short step from gathering location data (even if gathered in a proportionate manner) to using location data relating to a given IP address to enable the identification of individuals who have apparently breached quarantine regulations; and, if breach of quarantine regulations, why not other forms of unlawful activity?

This temptation for mission creep exists, and has been yielded to, within the European Union, for example, in Germany, in the State of Baden-Württemberg where the police has already been given access to health data held by the public health authorities in order to assist in the control of any violations of contact restrictions and to facilitate subsequent prosecutions[3].

This kind of potentially disproportionate interference with ECHR article 8 rights is not only concerning in itself, and in respect of where it might lead, but is also counter-productive in that it is likely to undermine the public trust which is so necessary to enable any contact tracing system to succeed in its public health objectives.

(d) Interoperability and cross-border travel

The present pattern of development of national apps is that different governments are tailoring different solutions to their different national circumstances. This gives rise to a possibility of a lack of interoperability between apps, and, in consequence, problems with cross-border travel by app users.

If a person crosses a border with an app which is not compatible with the app used in the country into which the user travels, then, in order to continue to have the benefits of an automatic notification system, he would require to load the app provided by the country into which he travels. This is something which the user might not trouble to do, especially for a short visit, and there would thus be created a gap in the coverage. This is unfortunate, and, in developing their apps, national governments may find it useful to seek, so far as possible, to ensure interoperability. However, interoperability may not always be possible to achieve, especially where the relevant data resides on a central database. If, in order to deal with this, national governments seek to agree that data should be able to be shared, then, for this to be proportionate, it is essential that this be justifiable on public health grounds and be done transparently and with the consent of the user.

Furthermore, it would clearly be unacceptable, as undermining the voluntary, consensual basis required to ensure proportionality, if, in crossing a border, it were made a mandatory requirement for a person to have, or to be required to download, an app which operates in the country into which he wishes to cross.

(e) Focussed concern

Against that background, it can be seen that there are two specific, focussed areas of concern:

(a) Whether the legal regime provides the necessary safeguards to give the assurance that use of a contact tracing app is proportionate and respects the data processing principles; and,

(b) What are the legal and organisational requirements required to ensure trust that privacy and data protection rights are being respected in a proportionate manner?

[3] See https://www.swr.de/swraktuell/baden-wuerttemberg/polizei-zugriff-corona-daten-100.html

4. Minimum safeguards

In considering the question of the minimum requirements governing the use of a contact tracing app in a manner which ensures adequate protection of both fundamental rights and data protection regulations, the CCBE is following a well-trodden path. Reference has already been made to the EDP *Guidelines* and it is worth also drawing to attention the comments of the IBA's Human Rights Institute (IBAHRI) on this subject in issue 3 of its *Freedom of Expression Bulletin* (5 May 2020)[4].

The IBAHRI specifically endorses a list compiled by Amnesty International, as follows:

1) Surveillance must be 'lawful, necessary and proportionate'.
2) Extensions of monitoring and surveillance must have sunset clauses.
3) The use of data would have to be limited to Covid-19 purposes.
4) Data security and anonymity would have to be protected and shown to be protected based on evidence.
5) Digital surveillance would have to avoid exacerbating discrimination and marginalisation.
6) Any sharing of data with third-parties would have to be defined in law.
7) There must be safeguards against abuse and procedures in place to protect the rights of citizens to respond to abuses.
8) 'Meaningful participation' by all 'relevant stakeholders' would be required, including public health experts and marginalised groups.

Although this checklist provides a useful starting point, any response made by the CCBE should be more pointed and should recognise the European context.

Against that background, further consideration might be better focussed by dealing with a series of questions which arise directly from the foregoing discussion.

4.1 Are contact tracing apps in principle acceptable in terms of civil liberties and data protection?

There is no question that the containment of the further spread of the corona virus is an outstandingly important common goal and is overwhelmingly in the public interest, both in terms of ensuring public health but also in terms of enabling, at the earliest juncture consistent with the protection of public health, the reversal of the restrictions which have been imposed on the fundamental rights of citizens. In this context, the use of technical means or the integration of technology-based processes can offer opportunities that form an essential component of a wider tracing and control strategy.

However, it is essential that fundamental rights and the rule of law are respected. Each proposed technical solution requires carefully to be assessed in respect of both its design and its implementation so as to ensure that it respects the need for proportionality. In particular, it should be both in accordance with law, and demonstrably necessary in a democratic society to ensure the protection of public health.

4.2 Should use of the App be compulsory?

It would be wholly disproportionate for the use of an app to be made compulsory. This would not only be an egregious derogation from fundamental rights, but would be impracticable, given that not all citizens will own or have available to them mobile telephones. Therefore, there should be no obligation to use tracing apps. It is unlikely to be possible to enforce such an obligation and monitor compliance with it without massively limiting the right to informational self-determination and the fundamental rights guaranteeing the confidentiality and integrity of information technology systems and personal

[4] See https://www.ibanet.org/Human_Rights_Institute/Freedom-of-Expression.aspx

data. Instead the use of such apps should be voluntary only. Even in times of crisis, restrictions on fundamental rights must not be allowed to go so far as *de facto* to abolish those rights.

4.3 What minimum requirements should be recommended to ensure adequate protection of fundamental rights?

- The purpose for which the data is collected and processed should relate exclusively to contact tracing for the purposes of control of infection from the Covid-19 virus and any mutation thereof.
- It must be ensured that the app does not cause the collection or processing of any data that is not required for the purposes of contact tracing.
- It is critical, in order to ensure public trust both so as to lead to as wide a take-up of the app as possible and to provide reassurance as to the privacy by design and medical effectiveness of the app, that the source code of the program be made available for independent verification as to its effectiveness and security. This might involve making the software available to an independent body, or it might involve publishing the source code.
- Before being launched the App should be the subject of a full Data Protection Impact Assessment.
- The app should thereafter be continuously evaluated for its effectiveness and compliance with data protection and fundamental rights obligations, and should be updated when required.
- Given that it is the free choice of the user to install the app, it follows that the user must be able to decide freely at any time whether to send a "push" message about his own infection. Such decision might be by default, but with an option on the part of the user to over-ride the default setting.
- The principle of data minimisation should be respected. In particular, data stored and sent concerning a user's infection, or exposure to others who may have been infected, should be demonstrably justified for public health reasons. How, precisely, data minimisation might be achieved may depend in part upon the architecture of the app, and, in particular whether the app depends upon distributed data or a centralised database.
- The data generated and processed by the use of the app and, in the case of a centralised model, stored and processed on the database must be processed solely for the purpose for which it was gathered, namely, contact tracing for the purposes of control of infection from the Covid-19 virus.
- To that end, access to the data should not be available to other than the relevant public health authorities. Both technical and legal controls should ensure this limitation of purpose and of access.
- Personal data (including pseudonymised personal data) should be retained for no longer than is required for the purpose for which it was collected. In particular, it must be ensured that such data are deleted - preferably automatically - as soon as they are no longer needed (for example, at the end of the incubation period with, it may be, a short temporal safety margin).
- Consideration should be given to allowing the relevant national data protection authority to examine the software and administrative and other procedures associated with the app, and to verify proportionality and compliance with the data minimisation principles before the app is made available to the public. Such a procedure would both allow independent verification of proportionality and, though the building of confidence in the public, encourage the uptake of the app.

4.4 Are there special considerations in respect of LPP/professional secrecy?

It will be recalled that the fact that there was a meeting between a person and his lawyer at a particular place and time is itself capable of constituting legally privileged information, so any contact tracing mechanism which stores or enables the recovery of that information potentially infringes LPP or professional secrecy. Such an intrusion may be capable of being justified on a proportionality test under ECHR article 8 (though, given the heightened protection accorded by the European Court of Human Rights to lawyer-client communication, this might be unlikely); but if the fact of the meeting relates to a criminal prosecution or a litigation, then such an intrusion will always constitute an infringement of article 6, which is, of course, an absolute right.

The problems with a compulsory app, or a system of collection of location data, such as that employed in Israel, is self-evident, but might be thought not to arise in connection with a voluntary app: neither a lawyer nor his client is forced to use the app and, if they have the app installed, they can always deactivate it before they meet. However, there is still a potential for an infringement of LPP/professional secrecy if the app is installed, but has no facility for temporary deactivation, or if the lawyer or client simply forgets to deactivate it. Even with a decentralised app, there is a potential risk to LPP/professional secrecy if re-identification and de-anonymisation of data enables a linkage between a client and his lawyer.

In these circumstances, and to ensure protection in respect of LPP/professional secrecy, as a minimum:

- any app should be engineered with a facility for temporary deactivation and
- lawyers and their clients should be vigilant to ensure that the app is deactivated before they meet.

4.5 What legal and regulatory mechanisms are required?

It is an essential prerequisite that the use of contact tracing apps should conform to the requirements of the rule of law. They should not be introduced and operated in an extra-legal manner. However, whether special legal or regulatory mechanisms are required to ensure compliance with the minimum requirements set out above may in part depend on the manner in which contact tracing technology is introduced in each country.

All European countries (excluding Belarus) are signatories to the European Convention on Human Rights, and there is already in existence in European countries a complex of primary legislation, regulations and jurisprudence governing the protection of privacy and the collection and processing of data, including (in the EEA, Switzerland and the UK) the GDPR. It is perfectly possible to create a contact app respecting the above minimum principles without the need for special legislation or regulation.

However, some countries may have chosen to facilitate the creation of contact tracing apps under special emergency powers, and, even in countries where there is no strict legal requirement to enact special legislation, there has been pressure from some quarters that, nonetheless, contact tracing apps should be subject to special legislation.

In that regard, any such special legislation, whether relating, narrowly, to contact tracing apps, or, more broadly setting out broad emergency powers should be acknowledged as being exceptional, and existing only to meet the present emergency, and should contain an appropriate sunset clause, a point made forcefully by the Organisation for Security and Co-operation in Europe[5].

Where the use of a contact tracing app is not subject to special legislation, it is more difficult to ensure that the data processing principles are not infringed by causing the app to continue and personal data to be retained beyond the end of the emergency, albeit that the legal order would not permit such continuation. In these circumstances, should an app be instituted otherwise than by means of special legislation or regulation, a sunset provision should be made explicit in the administrative arrangements

[5] See https://www.osce.org/odihr/449311

under which it is set up, and, in any event, the relevant data protection authorities, and civil society in general, should be vigilant in ensuring that the app is not continued in operation beyond the point at which its use ceases to be a proportionate interference with fundamental rights.

5. Conclusion

The foregoing discussion has been encapsulated in the CCBE Statement on Covid-19 contact tracing apps.