Bird & Bird & Data Protection

White Paper for governments on the privacy implications of apps supporting the fight against the Covid-19 pandemic.

European countries have responded to the Covid-19 pandemic by bringing in unprecedented measures to limit people's movements in an effort to contain the outbreak. As governments are now planning how they are going to progressively loosen those restrictions, it is clear that contact tracing-apps should be part of their toolbox. Already rolled out in some countries (e.g. Singapore, China, Taiwan and South Korea), several EU countries have started working on the development of such apps. When EU governments imposed the lockdown in March 2020, very few commentators questioned how much this decision affected the universal right of free movement, everyone being so concerned by the need to do whatever was necessary to reduce the number of deaths. A month later, when the discussion is about alternative measures which should be implemented after the lockdown to avoid a new wave of the pandemic, one measure, the development of a contact tracing app, triggers many discussions about the possible infringement to privacy. In this discussion, very few commentators put in balance the right to privacy with other rights such as the right of free movement and the right to health, despite the fact that they are all fundamental rights.

The purpose of this white paper is to explain the need to put in balance these fundamental rights, to find a way to develop apps which are useful to fight against the pandemic for the benefit of us all and to focus the debate on the necessary safeguards for the rights and freedoms of individuals in compliance with data protection principles, instead of taking for granted that consent from individuals is the only way to go forward.

Thus as further explained in this white paper:

- the reflection on contact tracing apps led by governments responds to a fundamental Core Principle (**1**);
- when developing a contact tracing app, governments have the duty to balance the fundamental right to protection of personal data against other fundamental rights and freedoms, such as the freedom of movement and the right to engage in work (**2**);
- health data and geolocation data collected by contact tracing apps are subject to strict requirements under EU law, with specific provisions in case of serious threat to public health which can be used by governments (**3**);
- according to EU laws, governments have a choice between two options: voluntary use of the app (based on individual consent) or legislative measures for use of the app by all citizens (**4**);
- safeguards must be in place in any case and this white paper provides some preliminary suggestions (**5**).

1. The reflection on contact tracing apps led by governments responds to a fundamental Core Principle for all European countries

The reflection led by governments, consisting in evaluating if contact tracing apps can contribute to the fight against the Covid-19 pandemic responds **to a fundamental Core Principle for all European countries: the protection of public health**.

By way of examples: In **France**, this principle is set out by the preamble of the 1946 Constitution according to which the Nation guarantees for all the protection of health. In **Germany**, article 2 para 2 of the German Constitution establishes that every person shall have the right to life and physical integrity which includes that the German government is required to take protective measures to avoid impairment of these legally protected interests, namely public health. In **Italy**, article 32 of the Italian Constitution establishes that the Italian Republic protects the health as a fundamental right of the individual and an interest of the community. In **the Netherlands**, the Constitution stipulates in article 22(1) that the government must take measures to promote public health. In **Spain**, article 43 of the Spanish Constitution recognises the individuals' right to the protection of health and the authorities' obligation to manage and lead public health.

If governments do not consider the development of a contact tracing app now and if this tool then proves to be crucial to combat the dissemination of Covid-19, governments will have failed to meet their constitutional obligation to guarantee the protection of public health. **Therefore if an app is necessary to fight against the pandemic, governments have the duty to put in place such an app, or more precisely to put in place the app/technology/ies which combat best the virus in a manner in line with European law and national constitutions.**

2. Governments have the duty to balance the fundamental right to protection of personal data against other fundamental rights and freedoms

The fundamental right to protection of personal data does not *per se* prohibit the development of a contact tracing app and it is a duty for governments to balance it against other fundamental rights.

This does not result from a liberal interpretation of generic legal principles: this is what the GDPR[1] says. Its recital 4 makes clear that:

> "*the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*".

In the process of developing a contact tracing app, **governments must therefore balance the right to protection of personal data recognized by article 8 of the Charter of fundamental rights of the European Union against other freedoms and fundamental rights, in particular the freedom of movement[2] and the right to engage in work[3] which currently suffer unprecedented restrictions due to the lockdown**.

First, governments need to assess if the app needs to collect personal data to achieve its objective of protection of public health. **If anonymized data is sufficient, there is no need to balance the right to protection of personal data against other rights because no personal data is processed**.

However, **if a contact tracing app has limited effects when data is anonymized**, **the fundamental right to personal data does not prevent the use of personal data**. In this case, governments should put in balance the fundamental rights and freedoms provided by national constitutions and the EU Charter of fundamental rights, **the result of which is that personal data can be used – provided that strong safeguards are put in place, and individuals' consent is not the only way to ensure such safeguards** (see some suggestions of safeguards in Section 6 below).

It is important to note that the often-quoted statement "*the least privacy-intrusive technological solutions shall be used*" is – without qualifications – misleading. The statement is correct if there is a choice between two equally efficient means. However, if one technological solution is less efficient than another or only available at a later stage, a balancing exercise has to be undertaken.

3. Health data and geolocation data collected by contact tracing apps are subject to strict requirements under EU law, with specific provisions in case of threat to public health.

The following developments are based on the assumptions that (i) processing anonymized data is not sufficient to support the health system in ensuring a secure lifting of restrictions and (ii) processing geolocation data and health data is needed. The questions whether anonymized data is sufficient and

[1] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[2] Article 45 of the Charter of fundamental rights of the European Union.
[3] Article 15 of the Charter of fundamental rights of the European Union.

whether specific data (such as health data or geolocation data) is needed to best combat the virus are factual/medical and not to be determined by lawyers.

Legally, if needed, contact tracing apps may also use two categories of highly personal data (geolocation data and health data), the use of which is however subject to strict conditions under European Union legislation.

On the one hand, geolocation data is governed by Article 9 of the European ePrivacy Directive, which provides that it cannot be processed for any purpose other than the routing of communications, unless the data are anonymized, or prior consent is given, or another legal justification is available under applicable law. On the other hand, health data is specifically protected by Article 9 of the GDPR which requires consent or that other alternative justifications are available which are listed in Art 9 GDPR.

In both cases, prior consent is not the only way and derogations are possible in case of serious threats to public health (Art. 9 (2)(i) of the GDPR which permits processing that "*is necessary for reasons of public interest in the area of public health*"), or for the safeguarding of public security (Art. 15 (1) of the ePrivacy Directive), but subject to legislative measures safeguarding rights and freedoms. Such legislative measures may already exist under the existing laws of a country.

When evaluating the necessity, it needs to be considered whether contact tracing solutions that do not use GPS data but a Bluetooth solution based on randomic pseudonymization are available and equally help fighting the virus without collection of geolocation data. However, waiting for a solution not yet available or using a solution which is less suitable is not required. Therefore, the use of geolocation data may be justified.

4. Voluntary use or legislative measures safeguarding rights and freedoms: governments have a choice!

Governments can choose between two options:

- Option 1: put in place an app based on individuals' consent and which can be downloaded/deleted at any time (Voluntary use).
- Option 2: adopt legislative measures safeguarding rights and freedoms for the use of an app by all citizens (Legislative measures).

The choice between these options should be driven by the efficiency in combating the virus. Contact tracing apps will achieve their maximum efficiency if used by the largest possible share of the population.[4] Whether voluntary use or legislative measures is the best way to achieve this goal may vary depending on the country and its culture. But this is a political question. From a legal point of view, **governments have a choice!**

If option 1 (voluntary use) is chosen, the app should as a principle collect a consent which satisfies the conditions of validity set out by the GDPR, in particular the requirement of **free choice**. Under the GDPR, consent is not the only possible way for collecting and processing personal data, but when consent is used, then it should be freely given. This implies that refusal to consent to the use of the app should not expose the person to negative consequences, i.e. that each person should be able individually to accept or refuse without any unfavourable consequence on his situation.

This puts into question the practical interest of this individual approach in a context of a public health crisis. If refusing to use the application should not expose the person to any consequence in terms of restriction of movement, this means that a person who refuses to use the app could still benefit from the end of lockdown and freely circulate, at the risk of spreading the virus and endangering the lives of others. It needs to be evaluated whether this approach will concretely support the work of the health system to end the spread of Covid-19 and whether the population will find it worthwhile to use the contact tracing app. When public health and public safety are at stake in the context of a health crisis, and if an app is needed to collectively fight against the virus, can the use of such app depend on individual choice?

If option 2 is chosen, legislative measures properly reflecting individuals' rights and freedoms will need to be in place. Such legislative measures may already exist under the existing laws of a country, for example under section 22(1)(c) of the German Federal Data Protection Act**. This is not the case in all European countries. For instance if France choses option 2 (use of an app by all citizens), a new law will be required because the French Data Protection Act (*Loi Informatique et Libertés*) or other laws (e.g. surveillance laws or the recent law on the state**

[4] Epidemiologists seem to agree that at least 60% of the population need to use such an app to make it useful.

of health emergency) do not provide specific measures at this stage. Adopting a new law within a time period compatible with the emergency is possible.[5]

Whichever option is chosen, the application will have to incorporate strong safeguards and comply with the principles of the GDPR: proportionality, clear information provided to individuals, data minimization, purpose limitations and technical and organizational measures provisional nature of the crisis management mechanism, etc. We give some examples of safeguards in the next section.

5. Suggestions of safeguards

We do not know yet the exact purpose of the app, its characteristics and the technology used. What we have set out in the table below shall be considered as suggestions for governments' consideration, based on GDPR core principles. They will have to be adapted based on the project considered by each government (see next page).

[5] In France, the recent law on the state of health emergency has been adopted after only 4 days of parliamentary debates. This proves that a law can be adopted shortly. A legislative proposal on the creation of a contact tracing app has already been submitted by a group of members of Parliament on 7 April 2020. On 28 April 2020, the French Parliament is expected to debate on the rolling out of a contact tracing app.

	Suggestions of safeguards
Purpose limitation	Personal data must be collected for specified, explicit and legitimate purposes. In the context of the fight against the Covid-19, apps/associated data processing may pursue different legitimate purposes. Each purpose must be linked to fighting Covid-19. Currently the three following purposes are mainly discussed: • The **first purpose** is the **observation of collective practices** by tracking the movements of groups of people to identify risk areas. This purpose generally only requires the use of anonymized data. The relevant experts have already identified this as a core area. • The **second purpose** is the **tracing of contacts**. This involves tracing the movements of people who have tested positive, in order to inform the population living in high-risk areas and to be able to alert recent contacts who have come across a sick person. It has become consensus that this purpose requires the collection and processing of personal data since it cannot be achieved only with anonymous data. • The **third purpose** is to **control lockdown**, i.e. to monitor compliance with quarantines, as in Korea and Taiwan. It is the most privacy-intrusive. Contrary to the first and second purpose it is not obvious that this purpose is justified. There needs to be evidence or strong indications that this is really necessary and that the same or a similar result cannot be reached with less intrusive means. We are doubtful that this is legitimate as a first step, but also think it cannot be absolutely ruled out at this stage. In any case, this purpose would require the highest safeguards in a democracy. The purposes of the app will have to be clearly identified and individuals must receive clear and comprehensive information about such purposes.
Transparency	Information listed at article 13 and 14 of the GDPR should be provided to the users of the app e.g. via a privacy notice available at the time of the downloading of the app.
Data minimization / proportionality	Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes of the app. Among the different technologies which can be used to track people's movement (mobile cells, GPS, Bluetooth, bank or transport cards, video surveillance…), Bluetooth seems to be less privacy intrusive in relation to the contact tracing purpose. Therefore, if it is available and sufficiently efficient, using this technology would be privacy compliant since it is most in line with the data minimization principle. However, if the Bluetooth technology is not (yet) available or if it is substantially more efficient to use a combination of, for example, Bluetooth and geolocation, other technologies can be used. In any case, the government must be able to demonstrate the necessity and proportionality of the personal data collected with regard to the purposes pursued.

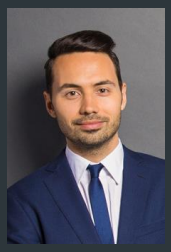
Accuracy	The app must ensure that the data collected is accurate. A process must be put in place which is as robust as possible: • to certify that when a person is declared Covid-19-positive, this information is accurate i.e. based on a test (as it triggers notifications to other people who have been exposed); • to identify the persons that have been in contact with the person declared Covid-19-positive. Mistakes on the identification of persons exposed to Covid-19 (false positives) should be limited as much as possible by the solution. There should be a possibility for users to report potential errors. The content of the notification sent to people exposed and in particular the instructions should be put under the control of health authorities to guarantee their appropriateness. Indeed, these instructions (e.g. quarantine, obligation to wear a mask, obligation to perform a test,...) may vary depending on the length and proximity of the contact of the person infected. A mechanism should be put in place for the exposed people to be able to obtain more information from a healthcare professional.
Limited retention	The app should last only for the time necessary to fight the Covid-19. This tool should be only temporary and should not remain in place after the crisis. All the personal data collected through the app will have to be suppressed once the crisis is resolved. This decision can be given to a group of independent experts. In addition some data shall be suppressed as soon as they are no longer useful i.e. the data collected to trace contacts shall be destroyed after a few weeks based on the opinion of experts on the duration of incubation of the virus.
Methods of storage	Two methods of data storage can be put in place: local data storage within individuals' smartphones, or centralised storage. Both can be put in place provided that adequate technical and organizational security measures are in place. Local data storage may be considered as more in line with the data minimization principle but centralised storage can be put in place if needed subject to appropriate security measures.
Design of the app / Technical requirements	Guarantees should be provided regarding the algorithms used by the contact tracing app. The fact that the source code of the app is open source is a guarantee of transparency for data subjects who can audit the code and verify that the app is used only for the purposes for which it was created.
Security	Robust technical and organizational measures must be in place. For instance, if data is sent to a central server, it must be transmitted over a secure channel. Encryption techniques may be implemented to secure data communications between the application and the server and between applications and to protect the information stored in the applications and on the server.

Specific measures for vulnerable data subjects	The government may take specific measures for minors and the impaired, less skilled or less educated parts of the population, older persons. For example, the information notice could be adapted for these vulnerable data subjects.
Sunset procedure and supervision	A procedure may be put in place to ensure that the mechanism is stopped and the data is deleted once the crisis is over. This procedure may set criteria to determine when the app is no longer needed and which authority (e.g. the public health authorities) must take this decision. The procedure may detail for instance how the collection of new data should be stopped (instructions to uninstall the application, automatic uninstallation, global deactivation of the application, etc.) and how the data already collected should be deleted from all databases. Some qualified members of the local DPA may be appointed to ensure that the safeguards are duly implemented and that the sunset procedure is activated when the relevant public authorities consider that the crisis is over.

Key contacts

Willy Mikalef
Senior Associate
Avocat – Paris Bar

Tel: +33142686349
willy.mikalef@twobirds.com



Ariane Mole
Partner
Avocat – Paris Bar

Tel: +33142686304
ariane.mole@twobirds.com

Ruth Boardman
Partner
Solicitor - Law Society of England & Wales

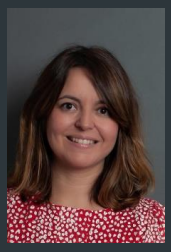
Tel: +442074156018
ruth.boardman@twobirds.com

Dr. Fabian Niemann
Partner
Attorney – German Bar

Tel: +4921120056000
fabian.niemann@twobirds.com

Lupe Sampedro
Partner
Attorney – Madrid Bar

Tel: +442079826502
lupe.sampedro@twobirds.com



Frederique Dupuis-Toubol
Partner
Avocat – Paris Bar

Tel: +442079826479
frederique.dupois-toubol@twobirds.com

Berend Van Der Eijk
Senior Associate
Attorney – The Netherlands Bar

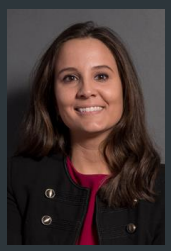
Tel: +31703538854
berend.vandereijk@twobirds.com

Debora Stella
Senior Associate
Attorney – Ordine di Pavia, Italy

Tel: +390230356029
debora.stella@twobirds.com

Ester Vidal
Associate
Attorney – Madrid Bar

Tel: +34917903232
ester.vidal@twobirds.com



twobirds.com

Abu Dhabi & Amsterdam & Beijing & Berlin & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw